



Tenable OT Security 3.19 User Guide

Last Revised: November 20, 2024



Table of Contents

Welcome to Tenable OT Security	12
Getting Started with OT Security	13
OT Security Technologies	13
Solution Architecture	14
OT Security Platform Components	14
Network Components	15
OT Security Hardware Components	16
OT Security Hardware Appliance (ICP)	16
OT Security Sensor Components	17
Configurable Sensor	17
Rack Mount Sensor	19
Enterprise Manager	21
System Elements	22
Assets	22
Policies and Events	23
Policy-Based Detection	23
Anomaly Detection	24
Policy Categories	24
Groups	25
Events	26
OT Security License Components	26
Get Started with OT Security	28
Check Prerequisites	29



Install OT Security ICP	30
Use OT Security	31
Expand OT Security into Tenable One	31
Prerequisites	33
System Requirements	34
Access Requirements	38
Network Considerations	40
Firewall Considerations	40
OT Security Core Platform	40
OT Security Sensors	42
Active Query	43
OT Security Integrations	44
Identification and Details Query	44
Install OT Security ICP	45
Install OT Security ICP Hardware Appliance	46
Clean Install Tenable Core + Tenable OT Security on Tenable-Provided Hardware	47
Install OT Security ICP Virtual Appliance	54
Connect OT Security to the Network	56
Configure OT Security ICP	57
Set up Tenable Core	57
Install OT Security on Tenable Core	65
Configure OT Security Settings using Setup Wizard	67
Log into the OT Security Management Console	68
User Info	71



Device	73
System Time	76
Connect the Separate Management Port (Port Separation)	77
OT Security License Activation	78
Launch OT Security	91
Enable the OT Security System	92
Start Using OT Security	93
Install OT Security Sensor	96
Set up the Sensor	102
Set up a Rack Mount Sensor	102
Set up a Configurable Sensor	105
Connect the Sensor to the Network	108
Access the Sensor Setup Wizard	109
Restore Backup Using CLI	111
Management Console User Interface Elements	113
Main User Interface Elements	113
Navigate OT Security	116
Customize Tables	116
Export Data	121
Actions Menu	122
Dashboards	122
Risk Dashboard	123
Inventory Dashboard	124
Events and Policies Dashboard	125



Interacting with Dashboards	126
Compliance Dashboard	130
Generate an Executive Report	133
Events	134
Viewing Events	135
Viewing Event Details	138
Viewing Event Clusters	139
Resolve Events	140
Create Policy Exclusions	143
Download Individual Capture Files	148
Create FortiGate Policies	149
Policies	150
Policy Configuration	151
Groups	151
Severity Levels	152
Event Notifications	152
Policy Categories and Sub-Categories	153
Policy Types	154
Enable or Disable Policies	160
View Policies	163
View Policy Details	164
Create Policies	166
Create Unauthorized Write Policies	172
Other Actions on Policies	173



Edit Policies	173
Duplicate Policies	176
Delete Policies	178
Inventory	181
Viewing Assets	181
Asset Types	184
View Asset Details	193
Header Pane	194
Details Tab	195
Code Revisions	196
Version Selection Pane	196
Snapshot Details Pane	197
Version History Pane	197
Compare Snapshot Versions	198
Create a Snapshot	199
IP Trail	200
Attack Vectors	200
Generate Attack Vectors	201
Viewing Attack Vectors	204
Open Ports	204
Additional Actions in the Open Ports Tab	205
Vulnerabilities	206
Events	206
Network Map	209



Device Ports	210
Related Assets	210
Nested Asset Details	211
Edit Asset Details	212
Edit Asset Details through the UI	213
Edit Asset Details by Uploading a CSV	215
Hide Assets	218
Export Diagnostics	218
Perform Asset-Specific Tenable Nessus Scan	219
Perform Resync	220
Network Map	224
Asset Groupings	225
Applying Filters to the Map Display	228
Viewing Asset Details	229
Set a Network Baseline	230
Vulnerabilities	231
Vulnerabilities	231
Plugin Details	232
Edit Vulnerability Details	233
View Plugin Output	234
Managing Active Queries	237
Create Custom Queries	240
Add Restrictions	241
Edit Query Variation	242



Duplicate a Query Variation	243
Run a Query Variation	243
Download Query Log	244
Credentials	245
Add Credentials	245
Edit Credentials	247
Delete Credentials	248
WMI Accounts	248
Create Nessus Plugin Scans	248
Network	253
Network Summary	253
Set the Timeframe	257
Packet Captures	260
Packet Capture Parameters	260
Filter Packet Capture Display	261
Activate or Deactivate Packet Captures	262
Download Files	262
Conversations	263
Groups	264
View Groups	265
Asset Groups	266
Network Segments	272
Email Groups	276
Port Groups	278



Protocol Groups	281
Schedule Group	283
Tag Groups	289
Rule Groups	292
Actions on Groups	294
Local Settings	301
Sensors	304
View Sensors	304
Manually Approve Incoming Sensor Pairing Requests	305
Configure Active Queries	306
Update Sensors	307
System Configuration	309
Device	309
Port Configuration	312
Set Compliance Dashboard Preferences	312
Updates	314
Tenable Nessus Plugin Set Updates	314
IDS Engine Ruleset Updates	319
DFE Cloud Updates	323
Certificate	326
Pair ICP with Enterprise Manager	328
Disconnect ICP Pairing with Enterprise Manager	332
License	332
Environment Configuration	333



Monitored Networks	333
Add Assets Manually	335
Event Clusters	336
PCAP Player	338
Upload a PCAP File	338
Play a PCAP File	338
User Management	339
Local Users	340
View Local Users	340
Add Local Users	341
Additional Actions on User Accounts	342
User Groups	344
Viewing User Groups	345
Add User Groups	345
Additional Actions on User Groups	347
User Roles	349
Zones	359
Authentication Servers	362
Active Directory	362
LDAP	367
SAML	370
Integrations	372
Tenable Products	373
Tenable Security Center	373



Tenable Vulnerability Management	374
Tenable One	375
Palo Alto Networks – Next Generation Firewall	375
Aruba – ClearPass Policy Manager	375
Integrate with Tenable One	376
IoT Connectors	377
IoT Connectors Engine	378
Install IoT Connector Agent on Windows	381
Servers	383
SMTP Servers	383
Syslog Servers	385
FortiGate Firewalls	386
System Log	388
Appendix – SAML Integration for Microsoft Entra ID	389
Step 1 - Create the Tenable Application in Microsoft Entra ID	389
Step 2- Initial Configuration	390
Step 3 - Map Azure Users to Tenable Groups	396
Step 4 - Finalizing the Configuration in Azure	401
Step 5 - Activate the Integration	402
Signing in Using SSO	403
Revision History	405



Welcome to Tenable OT Security

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

OT Security offers comprehensive security tools and reports for IT security personnel and OT engineers. It provides visibility into converged IT/OT segments and ICS activity, and makes you aware of situations 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 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 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 patented technology, OT Security provides visibility into your infrastructure—not only at the network level, but down to the device level. It uses native communication protocols to 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 Industrial Control Systems (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.

Tip: The *Tenable OT Security User Guide* and user interface are available in [English](#), [Japanese](#), [German](#), [French](#), and [Simplified Chinese](#). To change the user interface language, see [Local Settings](#).

For additional information on Tenable OT Security, review the following customer education materials:

- [Tenable OT Security Introduction \(Tenable University\)](#)

Getting Started with OT Security

To get started with OT Security, follow the sequence of steps mentioned in [Get Started with OT Security](#).

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 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 allow list and/or block list 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 cataloged 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 (for example 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 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

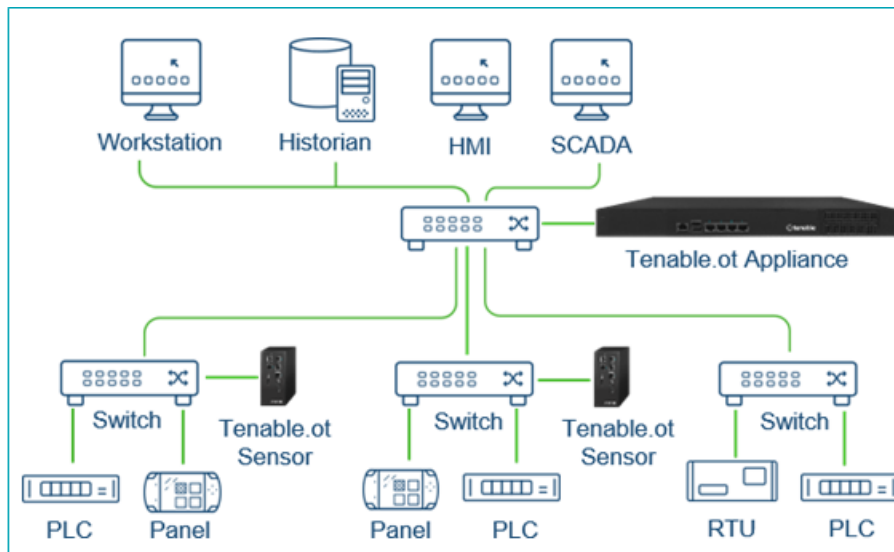
OT Security Platform Components

Note: In this document, the OT Security Appliance is referred to as ICP (Industrial Core Platform).

The OT Security solution is composed of these components:

- **ICP (OT Security Appliance)**– This component collects and analyzes the network traffic directly from the network (via a span port or network tap) and/or using a data feed from the Tenable OT Security Sensor (OT Security Sensor). The ICP appliance executes both the Network Detection and Active Query functions.
- **OT Security Sensors** – These are small devices deployed on network segments that are of interest, up to one sensor per managed switch. OT Security sensors provide full visibility into these network segments by capturing all the traffic, compressing the data and then communicating the information to the OT Security appliance. You can configure Sensors version 3.14 and later 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)** – You can create user accounts to control access to the OT Security Management Console. You can access the Management Console through a browser (Google Chrome) via a secure socket-layer authentication (HTTPS).

Note: You can only access OT Security user interface from 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**– Send OT Security Event logs to a SIEM using Syslog protocol.
- **SMTP Server** – OT Security sends event notifications by email to specific groups of employees via an SMTP server.
- **DNS Server** – Integrate DNS servers 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 integrations¹.

¹For 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](#).

OT Security Hardware Components

OT Security Hardware Appliance (ICP)



Component	Description
Power Indicator	Indicates when the OT Security appliance is turned on (Green) or off.
Console Port	For service or local access. Baud rate of 115200 bps with an 8N1 configuration.
USB Ports	For reimaging or upgrading the appliance in the offline mode.
Ethernet Ports	Four GbE ports used to connect to management and operational networks as follows: Port 1 – By default, this port is used for both Management (User Interface) and as the Active Query port (that communicates with the network assets). This port configuration could be changed (both during the setup and later in the Settings page) to include just the Queries. This is done in order to separate the management interface from the controllers' network. Port 2 – Mirror port - used as the destination of the mirroring session (SPAN). This port receives a copy of the network traffic. This port has no IP address.



Port 3 - if the port separation option is enabled, this port is used for management (user interface) only and can be connected to a network that is not part of the controller's network.

Port 4 - Reserved port, used by OT Security's Professional Services for remote or local support.

Note: All available network interfaces are configurable for OT Security ICP.

Rear Panel

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

Package Contents

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

OT Security Sensor Components

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
Power Indicator	Indicates when the sensor is turned on (Green) or off.
Console Port	For service or local access. <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;"> <p>Note: Baud rate of 115200 bps with an 8N1 configuration.</p> </div>
USB Ports	For reimaging or upgrading the appliance in the offline mode.



Ethernet Ports	<p>Five GbE ports used to connect to management and operational networks as follows:</p> <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>
-----------------------	---

Note: All available network interfaces are configurable for OT Security Sensors.

Package Contents

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

Rack Mount Sensor

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



Front Panel

Component	Description
Console Port*	For service or local access.
USB Ports	For reimaging or upgrading the appliance in the offline mode.
Ethernet Ports	<p>Four 1 GbE ports used to connect to management and operational networks as follows:</p> <p>Port 1 - Management port - used for managing the device.</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 - Not in use.</p> <p>Port 4 - Not in use.</p>

*Baud rate of 115200 bps with an 8N1 configuration.

Rear Panel

Power Button	Stand-by mode in red; Power-on mode in green.
Reset Button	Reboots the system without turning off the power.



Power Switch	ON/OFF switch. (Press and hold for a few seconds to turn the power off.)
Power Supply	AC power connector; 100 – 240 V AC

Package Contents

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

Enterprise Manager

You can deploy the OT Security EM as an appliance installed on site or on a Public or Private cloud server.

The following table shows the specifications for the various deployment methods.

Specification	On-Premises	Public Cloud
Hardware	Intel® Xeon™ D1548, 2.0 GHz 2 X 32GB DDR4, 2400 MHz Data: 2 x 2TB Fixed SATA3 HDD OS: 1 X 64 GB SSD	AWS
Form Factor	Dimensions: 438 x 44 x 321 mm Weight: 6 kg	N/A
Power	220W; Single PS Input AC 90V~264V	N/A



Cooling	CPU heatsink with fan duct 2 X cooling fans	N/A
Temperature	Operating: 0°C ~40°C/32°F ~104°F Storage: -20~70° C / -4°F ~158°F Humidity: 5% ~ 90%	N/A

System Elements

Assets

Assets are the hardware components in your network such as controllers, engineering stations, servers, and so on. 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** – Events 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 (for example, obsolete operating systems, usage of vulnerable protocols, vulnerable open ports, and so on.). 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 PLCs 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 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, OT Security generates an Event. OT Security logs the Event and sends notifications in accordance with the Policy Actions configured for the policy.

There are two types of policy events:

- **Policy-based Detection** – Triggers events when the precise conditions of the policy, as defined by a series of event descriptors, are met.
- **Anomaly Detection** – Triggers 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)** – 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**– An un-allowed communication protocol was used between two network assets or a communication took place between two assets that never communicated before.
- **Anomalous or unauthorized changes to the asset inventory** – A new asset was discovered or an asset stopped communicating in the network.
- **Anomalous or unauthorized changes in asset properties** – 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 (for example 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 (for example 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 cataloged 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 License Components

This topic breaks down the licensing process for Tenable OT Security as a standalone product. It also explains how assets are counted, lists add-on components you can purchase, explains how licenses are reclaimed, and describes what happens during license overages or expirations.

Tip: To update or reinitialize your license, see [OT Security License Workflow](#).

Licensing Tenable OT Security

You can purchase Tenable OT Security in subscription or perpetual/maintenance versions.

To license Tenable OT Security, you purchase licenses based on your organizational needs and environmental details. Tenable OT Security then assigns those licenses to your *assets*: all detected devices with IP addresses, one license for each IP address.

When your environment expands, so does your asset count, so you purchase more licenses to account for the change. Tenable licenses use progressive pricing, so the more you purchase, the lower the per-unit price. For prices, contact your Tenable representative.

How Assets are Counted

In Tenable OT Security, your license count is based on the number of unique IP addresses in your environment. Assets are licensed from the moment they are detected.



Note: Assets on internal networks behind live IP addresses do not count towards your license. For example, in a redundantly connected Programmable Logic Controller (PLC) chassis with two live IP addresses and 10 modules behind these, only the two live IP addresses count towards your license.

Tenable OT Security Components

You can customize Tenable OT Security for your use case by adding components. Some components are add-ons that you purchase.

Included with Purchase	Add-on Component
<ul style="list-style-type: none">• Virtual Core Appliance.• Tenable Security Center.	<ul style="list-style-type: none">• Tenable OT Security Enterprise Manager.• Tenable OT Security Configurable Sensor.• Tenable OT Security Certified Configurable Sensor.• Tenable OT Security Certified Core Platform.• Tenable OT Security Core Platform.• Tenable OT Security XL Core Platform.

Reclaiming Licenses

When you purchase licenses, your total license count is static for the length of your contract unless you purchase more licenses. However, Tenable OT Security reclaims licenses in real time as your asset count changes.

Tenable OT Security reclaims the following assets:

- Hidden assets
- Assets that have been offline for more than 30 days
- Assets you remove or hide in the user interface

Exceeding the License Limit

In Tenable OT Security, you can only use your allocated number of licenses unless you purchase more licenses.

When you exceed your license limit:



- Non-administrators can no longer access Tenable OT Security.
- A message that your license has been exceeded appears in the user interface.
- You can no longer restore assets from the Tenable OT Security Settings.
- You can no longer update vulnerability plugins or IDS Signatures (Feed updates).

Note: When you exceed your license limit, Tenable OT Security can still detect and add new assets.

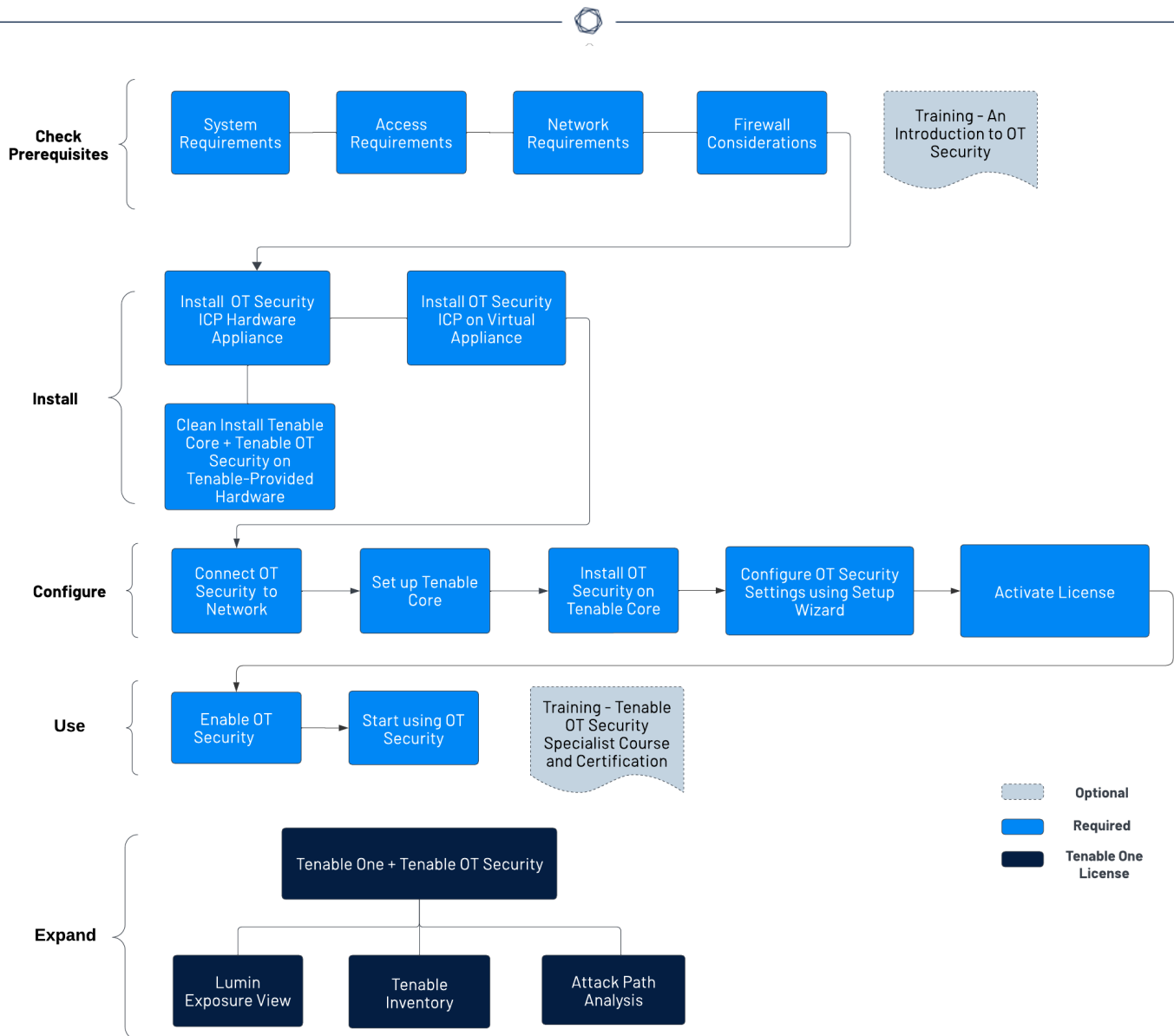
Expired Licenses

The Tenable OT Security licenses you purchase are valid for the length of your contract. 30 days before your license expires, a warning appears in the user interface. During this renewal period, work with your Tenable representative to add or remove products or change your license count.

After your license expires, Tenable OT Security is disabled and you cannot use it.

Get Started with OT Security

Use the following getting started sequence to install and start using OT Security.



Check Prerequisites

- [Prerequisites](#) – Review the system, hardware, virtual, and license requirements for OT Security.
 - [System Requirements](#) – Review the requirements to install and run Tenable Core + OT Security.
 - [Access Requirements](#) – Review the internet and port requirements to run Tenable Core + OT Security.



- [Network Considerations](#) – Review the network interfaces to connect OT Security.
- [Firewall Considerations](#) – Review the ports that must be open for OT Security to function correctly.
- [Introduction to Tenable OT Security](#) – Go through the training material for an understanding of OT Security.

Install OT Security ICP

OT Security is an application running on top of the Tenable Core operating system, and it is subject to the base requirements of Tenable Core. Use the following guidelines to install and configure Tenable Core + OT Security.

To install OT Security:

1. [Install OT Security ICP](#)

- [Install OT Security ICP Hardware Appliance](#) – Set up OT Security as a hardware appliance.

Note: Tenable-provided Tenable Core hardware comes with Tenable Core+ OT Security pre-installed. If you are installing an older or dated appliance, you might opt for a clean install. For more information, see [Clean Install Tenable Core + Tenable OT Security on Tenable-Provided Hardware](#).

- [Install OT Security ICP Virtual Appliance](#)– Deploy Tenable Core + OT Security as a virtual machine using the pre-configured `.ova` file containing the standard virtual machine configuration, or customize your appliance using the installation `.iso` file.

2. [Connect OT Security to the Network](#)– Connect OT Security hardware and virtual appliance to the network.

3. [Configure OT Security ICP](#)

- a. [Set up Tenable Core](#) – Configure Tenable Core via CLI or the user interface.
- b. [Install OT Security on Tenable Core](#) – Manually complete the installation of Tenable OT Security in Tenable Core.



- c. [Configure OT Security Settings using Setup Wizard](#) – Use the setup wizard to configure basic settings in OT Security.
 - [Log in](#) to the OT Security console and configure the [User Info](#), [Device](#), [System Time](#), and [Port Separation](#) settings.
4. [Activate OT Security License](#) – Activate your license after you complete the OT Security installation.

Use OT Security

[Launch OT Security](#)

1. [Enable](#) OT Security – Enable OT Security after you activate your license.
2. [Start using OT Security](#) – Configure your monitored networks, port separation, users, groups, authentication servers, and so on to start using OT Security.

Tip: To gain hands-on experience and to obtain Tenable OT Security Specialist Certification, take the [Tenable OT Security Specialist Course](#).

Expand OT Security into Tenable One

Note: This requires a Tenable One license. For more information about trying Tenable One, see [Tenable One](#).

Integrate OT Security with Tenable One and leverage the following features:

- In [Lumin Exposure View](#), reveal converged risk levels and uncover hidden weaknesses across the IT-OT boundary. You can continuously monitor and track potential vulnerabilities with enhanced OT data:
 - Review the **Global** [exposure card](#) to understand your holistic score. Click **Per Exposure** to understand what factors are driving your score, and by how much.
 - Review the **Operational Technologies** [exposure card](#).



- [Configure the exposure view settings](#) to set customized card target, and to configure your **Remediation SLA** and **SLA Efficiency** based on your company policy.
- [Create a custom exposure card](#) based on business context, and include the new tag you created in Tenable Inventory.
- In [Tenable Inventory](#), enrich asset discovery with OT-specific insights, such as firmware versions, vendors, models & operational states. Access OT intelligence that standard IT security tools cannot provide:
 - Review your OT assets to understand the strategic nature of the interface. This should help set your expectations on what features to use within Tenable Inventory, and when.
 - Review the [Tenable Queries](#) that you can use, edit, and bookmark.
 - Familiarize yourself with the [Global Search query builder](#) and its objects and properties. Bookmark custom queries for later use.

Tip: To get a quick view of what properties are available:

- In the query builder, type *has*. A list of suggested asset properties appears.
- Customize the list by adding a column. A list of available columns/properties appears.

- Drill down into the [asset details](#) page to view asset properties and all associated context views.
- [Create a new dynamic tag](#) for your OT assets, where:
 - Operator = **Host System Type**
 - Value = **PLC**
- (Optional) [Create a tag](#) that combines different asset classes.
- In [Attack Path Analysis](#), expose vulnerable network paths that could disrupt key operations like production lines or data centers. You can track OT communication paths and unauthorized changes:
 - View the [Attack Path Analysis Dashboard](#) for a high-level view of your vulnerable assets such as the number of attack paths leading to these critical assets, the number of open findings and their severity, a matrix to view paths with different source node exposure



score and ACR target value combinations, and a list of trending attack paths.

- Review the **Top Attack Path Matrix** and click the **Top Attack Paths** tile to view more information about your “Crown Jewels”, or assets with an ACR of 7 or above.

You can adjust these if needed to ensure you’re viewing the most critical attack path data and findings.

- On the [Findings](#) page, view all attack techniques that exist in one or more attack paths that lead to one or more critical assets by pairing your data with advanced graph analytics and the MITRE ATT&CK® Framework to create Findings, which allow you to understand and act on the unknowns that enable and amplify threat impact on your assets and information.
- On the [Mitre Att&ck Heatmap](#), select the **ICS** heatmap option to focus on ICS (Industrial Control Systems) tactics and techniques.
- On the [Discover](#) page, generate attack path queries to view your assets as part of potential attack paths:
 - [Generate an Attack Path using a Built-in Query](#)
 - [Generate an Asset Query using the Asset Query Builder](#)
 - [Generate an Attack Path Query using the Attack Path Query Builder](#)

Then, you can view and interact with the [Attack Path Query](#) and [Asset Query](#) data via the query result list and the [interactive graph](#).

Prerequisites

Objective: Ensure you have everything you need for a successful ICP installation.

Tenable OT Security is an application running on top of the Tenable Core operating system, and it is subject to the base requirements of Tenable Core.

Tenable Core + Tenable OT Security is available for deployment both on hardware and as a virtual machine appliance. A virtual machine deployment must meet the minimal requirements as mentioned in [Hardware Requirements](#).



Hardware Requirements

Multiple sizes of dedicated Tenable Core + Tenable OT Security hardware appliances are available (purchased separately). For hardware specifications, see [Tenable OT Security Physical Hardware Sheet](#).

The Tenable Core operating system and the Tenable OT Security application are pre-installed on all available hardware appliances.

You can also install Tenable Core + Tenable OT Security on custom hardware that meets the requirements. For instructions, contact Tenable Support or your Customer Success Manager.

For information about the requirements for Tenable Core + Tenable OT Security, see the following:

- [System Requirements](#)
- [Access Requirements](#)

Virtual Appliance Requirements

Tenable Core + Tenable OT Security can be deployed in the following ways:

- Using the `.ova` file – This file is ready to deploy and includes all the standard and supported virtual machine configuration.
- Using the `.iso` file – This is a general-purpose installation disk image. Deploy this on a properly configured virtual machine, which meets the requirements.

License Requirements

For general information about licensing for OT Security, see [OT Security License Components](#).

For the licensing workflow, see [OT Security License Activation](#).

System Requirements

To install and run Tenable Core + OT Security or Tenable OT Security Sensor, your application and system must meet the following requirements.

Note: Tenable Support does not assist with issues related to your host operating system, even if you encounter them during installation or deployment.



Environment		Tenable Core File Format	More Information
Virtual Machine	VMware	.ova file	Install OT Security ICP Virtual Appliance
Hardware	Tenable-provided hardware	.iso image	Install Tenable Core on Hardware Note: Tenable Core + OT Security requires Tenable-provided hardware. For more information, contact your Tenable representative.

Note: While you could use the packages to run Tenable Core in other environments, Tenable does not provide documentation for those procedures.

Note: Tenable does not recommend deploying multiple applications on a single instance of Tenable Core. If you want to deploy several applications on Tenable Core, deploy a unique instance for each application.

Tenable Core + OT Security ships with the latest version of OT Security included.

You can install OT Security on a hypervisor¹ or directly on user-supplied hardware running Tenable Core.

Note: Tenable strongly discourages running Tenable Core + OT Security in an environment shared with other Tenable applications. For example, installing two products on the same virtual machine, or in the same Tenable Core system.

Storage Requirements

Tenable recommends installing OT Security on direct-attached storage (DAS) devices, preferably solid-state drives (SSD), for best performance. Tenable strongly encourages the use of solid-state storage (SSS) that have a high drive-writes-per-day (DWPD) rating to ensure longevity.

Tenable does not support installing OT Security on network-attached storage (NAS) devices. Storage area networks (SAN) with a storage latency of 10 milliseconds or less, or Tenable hardware appliances, are a good alternative in such cases.

¹Hypervisor must be officially supported by VMWare and known to work under Hyper-V, KVM.



Disk Space Requirements

Enterprise networks can vary in performance, capacity, protocols, and overall activity. Resource requirements to consider for deployments include raw network speed, the size of the network to monitor, and the configuration of the application. Processors, memory, and network card selection rely heavily on these deployment configurations. Disk space requirements vary depending on usage based on the amount of data, and length of time you store data on the system.

OT Security needs to perform full packet captures of monitored traffic, and the size of the policy event data stored by OT Security depends on the number of devices and the type of environment.

You can calculate storage requirements per day (GB/day) by multiplying the traffic rate (Mbps) * 2.7 - based on a compression factor of 0.25.

In an example with two sensors receiving 23 Mbps SPAN traffic each, the storage requirements per day (GB/day) is calculated as $(23*2)*2.7=124$ GB of space per day for traffic storage.

Note: If compliance or security requirements require that you store up to 30 days of traffic, then you need a PCAP (Packet Capture) storage drive of 3.75 TB to accommodate this requirement. Once the stored traffic data reaches the maximum size, OT Security overwrites the oldest PCAP data and replaces it with new traffic.

ICP System Requirement Guidelines (Virtual or Tenable Core)

Maximum SPAN/TAP Throughput (Mbps)	CPU Cores ¹	Memory (DDR4)	Storage Requirements	Network Interfaces
50 Mbps or less	4	16 GB RAM	128 GB	Minimum 4 x 1 Gbps
50-150 Mbps	16	32 GB RAM	512 GB	Minimum 4 x 1 Gbps
150-300 Mbps	32	64 GB RAM	1 TB	Minimum 4 x 1 Gbps
300 Mbps to 1 GB	32-64	128 GB RAM or more	2 TB or more	Minimum 4 x 1 Gbps



Disk Partition Requirements

OT Security uses the following mounted partitions:

Partition	Content
/	operating system
/opt	application and database files
/var/pcap	packet captures (full packet capture, event, query)

The standard process places these partitions on the same disk. Tenable recommends moving these to partitions on separate disks to increase throughput. OT Security is a disk-intensive application and using disks with high read/write speeds, such as SSDs, results in the best performance. Tenable recommends using an SSD with high DWPD ratings on customer-supplied hardware installations when using the packet capture feature in OT Security.

Tip: Deploying OT Security on a hardware platform configured with a redundant array of independent disks (RAID 0) can dramatically boost performance.

Tip: Tenable does not require RAID disks for even our largest customers. However, in one instance, response times for queries with a faster RAID disk for a customer with more than one million managed vulnerabilities decreased from a few seconds to less than a second.

Network Interface Requirements

You must have four network interfaces present on your device before installing OT Security. Tenable recommends the use of gigabit interfaces. The VMWare OVA creates these interfaces automatically. Create these interfaces manually when you install the ISO on your own hardware.

Note: Tenable does not provide SR-IOV support for the use of 10 G network cards and does not guarantee 10 G speeds with the use of 10 G network cards.

NIC Requirements



nic0 (192.168.1.5) and **nic3** (192.168.3.3) have static IP addresses when you install Tenable Core + OT Security in a hardware or virtual environment. Other network interface controllers (NICs) use DHCP.

nic3 (192.168.3.3) has a static IP address when you deploy Tenable Core + OT Security on VMware. Other NICs use DHCP. Confirm that the Tenable Core **nic1** MAC address matches the NIC MAC address in your VMware passive scanning configuration. Modify your VMware configuration to match your Tenable Core MAC address if necessary.

For more information, see [Manually Configure a Static IP Address](#), [Manage System Networking](#) and the *VMware Documentation*.

¹CPU Cores reference PHYSICAL cores, assumes server-class CPU (Xeon, Opteron).

Access Requirements

Your deployment must meet the following requirements.

- [Internet Requirements](#)
- [Port Requirements](#)

Internet Requirements

You must have internet access to download Tenable Core files and perform online installs.

After you transfer a file to your machine, internet access requirements to deploy or update Tenable Core vary depending on your environment.

Note: You must reach `appliance.cloud.tenable.com` to install from the online ISOs (and to get online updates) and `sensor.cloud.tenable.com` to pick up scan jobs.

Environment		Tenable Core Format	Internet Requirement
Virtual Machine	VMware	.ova file	Does not require internet access to deploy or update Tenable Core.



Hardware	.iso image	Requires internet access to install or update Tenable Core.
----------	------------	---

Tip: You do not need access to the internet when you install updates to via an offline .iso file. For more information, see [Update Tenable Core Offline](#).

Port Requirements

Your Tenable Core deployment requires access to specific ports for inbound and outbound traffic. Tenable Security Center also requires application-specific port access. For more information, see [Port Requirements](#) in the *Tenable Security Center User Guide*. OT Security also requires application-specific port access. For more information, see [Firewall Considerations](#).

Inbound Traffic

Allow inbound traffic to the following ports:

Note: Inbound traffic refers to traffic from users configuring Tenable Core.

Port	Traffic
TCP 22	Inbound SSH connections.
TCP 443	Inbound communications to the OT Security interface.
TCP 8000	Inbound HTTPS communications to the Tenable Core interface.

Outbound Traffic

Allow outbound traffic to the following ports:

Port	Traffic
TCP 22	Outbound SSH connections, including remote storage connections.
TCP 443	Outbound communications to the <code>appliance.cloud.tenable.com</code> and <code>sensor.cloud.tenable.com</code> servers for system updates.
UDP 53	Outbound DNS communications for OT Security and Tenable Core.



Network Considerations

The OT Security appliance (both physical and virtual) must reach these network interfaces:

Management and Active Query Interface

- An interface configured with an IP address that allows network reachability to manage and configure the appliance.
- Allows the appliance to reach assets on the network for active querying (recommended, but optional).
- Allows you to split between two separate network interfaces. See [Connect the Separate Management Port \(for Port Separation Option\)](#).

Monitoring Interface

- Passively monitors and collects traffic for analysis.
- Must be connected to a Mirroring, Switch Port Analyzer (SPAN), or Remote Switch Port Analyzer (RSPAN) destination interface of a switch.
- (Optional) Uses sensors and Encapsulated Remote SPAN (ERSPAN) configuration to monitor traffic that cannot mirror directly into the appliance interface.

Firewall Considerations

In setting up your OT Security system, it is important to map out the open ports to allow the Tenable system to operate correctly. The following tables indicate the ports to reserve for use with the OT Security ICP and OT Security Sensors as well as those needed for running Active Queries and for integration with Tenable Vulnerability Management and Tenable Security Center.

Note: For information about the list of Tenable websites and domains that you must allow through the firewall, see the [Knowledge Base article](#).

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 and TCP 28304	OT Sensor	Sensor authentication, pairing, and receiving sensor information.
Outbound	TCP 443 and TCP 28305	OT Security EM	ICP and EM pairing
Inbound	TCP 8000	Web interface for Tenable Core	Browser access to Tenable Core
Inbound	TCP 28304	ICP/ OT Security	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 443	cloud.tenable.com	Sends data for integration
Outbound*	Various Industrial protocols	PLCs/controllers	Active query
Outbound*	TCP 25 or 587	Email server for alerts	SMTP (alert emails, reports)
Outbound*	UDP 514	Syslog server	Sends policy event alerts and syslog messages
Outbound*	UDP 53	DNS server	Name Resolution
Outbound*	UDP 123	NTP server	Time service
Outbound*	TCP 389 or 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 *.nessus.org	Automatic Plugin, Application, and OS Updates**
Outbound	TCP 10146 (secure port)	IoT Connector	Connects ICP to IoT connector agent

*Optional services

**Offline procedure available

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
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
Outbound	TCP 28303	ICP/ OT Security Sends communication from	Unauthenticated / passive only sensor connection



		sensor, receives on ICP/ OT Security	
Outbound	TCP 443 and TCP 28304	ICP/ OT Security Sends communication from sensor, receives on ICP/ OT Security	Authenticated / secure tunnel between sensor and ICP

*Optional services

Active Query

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

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	UDP/TCP 44818	OT Devices	CIP protocol
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



Note: The ports used by the devices vary depending on the vendor and product line. For a list of relevant ports and protocols needed to ensure active queries are successful, see [Identification and Details Query](#).

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

Identification and Details Query

You can use the following ports for Identification and Details queries:

Note: You may need to open the ports on the firewall for OT Security or its sensors to reach the relevant port for your assets.

Port	Port Name
21	FTP
80	HTTP
102	Step-7 / S7+
111	Emerson OVATION
135	WMI
161	SNMP
443	HTTPS
502	MODBUS / MMS



1911	Niagara FOX
2001	Profibus
2222	PCCC_AB-ETH
2404	IEC 60870-5
3500	Bachmann
4000	Emerson ROC
4911	Niagara FOX TLS
5002	Mitsubishi MELSEC
5007	Mitsubishi MELSEC
5432	PSQL / SEL
18245	S RTP
20000	DNP3
20256	PCOM
44818	EthernetIP / CIP
47808	BACNET (udp)
48898	ADS
55553	Honeywell CEE
55565	Honeywell FTE

Install OT Security ICP

Objective: Get the OT Security ICP installed and ready for use.

Before you Begin

- See [Prerequisites](#).

Follow these steps as required to install and connect OT Security ICP to the network:



- [Install OT Security ICP Hardware Appliance](#)

Note: Tenable-provided Tenable Core hardware comes with Tenable Core+ OT Security pre-installed. If you are installing an older or dated appliance, you might opt for a clean install. For more information, see [Clean Install Tenable Core + Tenable OT Security on Tenable-Provided Hardware](#).

- [Install OT Security ICP Virtual Appliance](#)

Next Step

- [Connect OT Security to the Network](#)

Install OT Security ICP Hardware Appliance

You can either mount the OT Security appliance on a rack or simply place it on top of a flat surface such as a desktop.

Tip: Tenable recommends that you complete the basic configuration and setup described in [Set up Tenable Core](#) and [OT Security setup wizard](#) at the comfort of your desk, before moving the appliance to a rack or any other remote location.

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 supplied AC power supply cable to the power supply port in the rear panel and plug this 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 and flat surface (such as a desktop).

Note:

- Make sure that the tabletop is flat and dry.
- Make sure that the cooling fan air intake (at the back panel) and the air ventilation holes (on the top panel) are not obstructed.
- If you place a unit 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.

2. Plug in the supplied AC power supply cable to the power supply port in the rear panel and plug this cable to the AC power supply (mains).

For more information about connectivity, see [Network Considerations](#).

What to do next

[Connect OT Security to the Network](#)

Clean Install Tenable Core + Tenable OT Security on Tenable-Provided Hardware

Tenable Core + OT Security are pre-installed out-of-the-box on official Tenable-provided hardware. In some cases, a clean-install (also referred to as re-flashing) is recommended.

Note: If you have recently received a new appliance, you can skip this procedure.

Before you Begin

Make sure you have the following:

- An application to format and create bootable USB flash drives, such as Rufus.
- A serial cable.
- A serial terminal application, such as PuTTY.
- A USB drive ~8 GB+.

To install Tenable Core + OT Security ISO file:



1. Download the latest Offline ISO file from [Tenable Downloads](#).

Tenable Core + Tenable.ot (OL8)					
Tenable-Core-OL8-Tenable.ot-20240315.ova	Tenable Core Tenable.ot VMware Image	2.75 GB	Mar 15, 2024	Checksum	
	OVA Specifications: <ul style="list-style-type: none">◦ CPU: 4◦ Memory: 16384 MB◦ Disk: 205 GB◦ Includes Tenable.ot 3.18.51				
Tenable-Core-OL8-Tenable.ot-20240404.iso	Tenable Core Tenable.ot Installation ISO	958 MB	Apr 4, 2024	Checksum	
	<ul style="list-style-type: none">◦ Requires an internet connection◦ Installs the latest version of Tenable.ot and the latest system packages				
Tenable-Core-OL8-Tenable.ot-offline-20240404.iso	Tenable Core Tenable.ot Self-Contained Installation ISO	3.32 GB	Apr 4, 2024	Checksum	
	<ul style="list-style-type: none">◦ Includes Tenable.ot 3.18.51				

2. Plug the USB drive into a PC and flash the ISO onto the flash drive in DD mode.

Rufus 4.4.2103 (Portable)

Drive Properties

Device
NO_LABEL (Disk 1) [16 GB]

Boot selection
Tenable-Core-OL8-Tenable.ot-offline-20240315.iso SELECT

Persistent partition size
0 (No persistence)

Partition scheme: MBR
Target system: BIOS or UEFI

^ Hide advanced drive properties

- List USB Hard Drives
- Add fixes for old BIOSes (extra partition, align, etc.)
- Use Rufus MBR with BIOS ID: 0x80 (Default)

Format Options

Volume label
TenableCore Install ISO

File system: FAT32 (Default)
Cluster size: 8192 bytes (Default)

^ Hide advanced format options

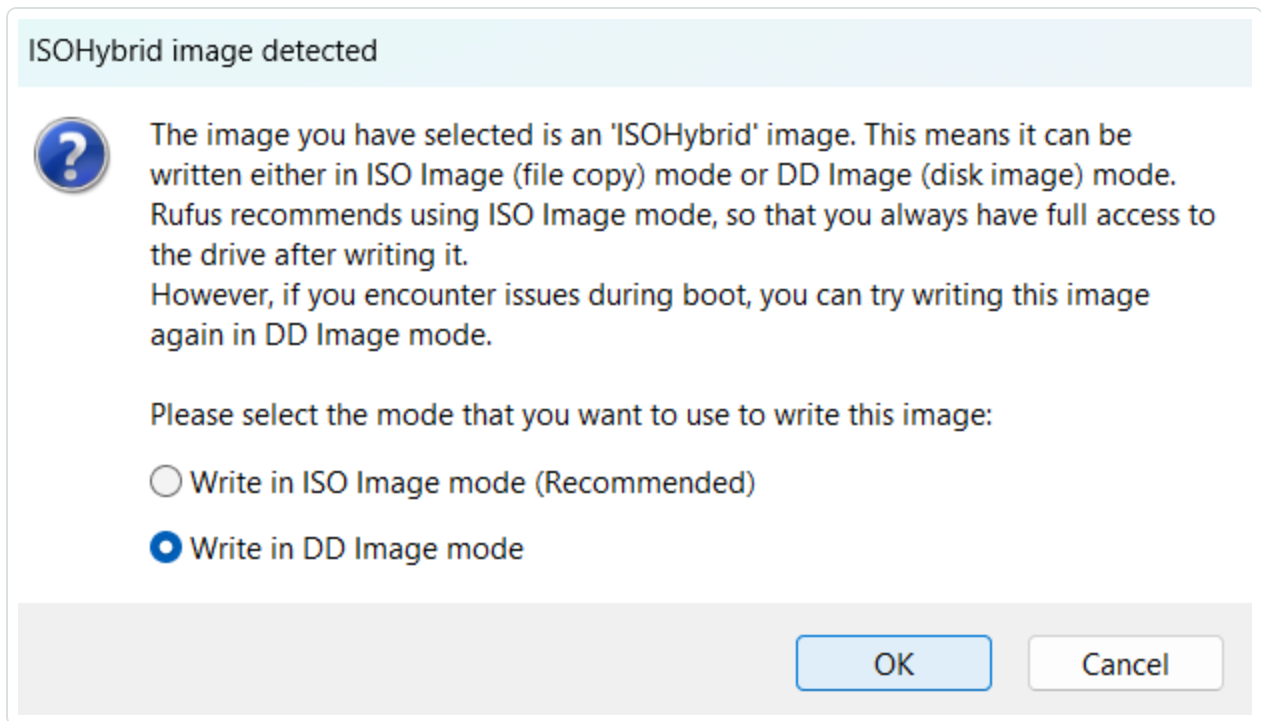
- Quick format
- Create extended label and icon files
- Check device for bad blocks: 1 pass

Status

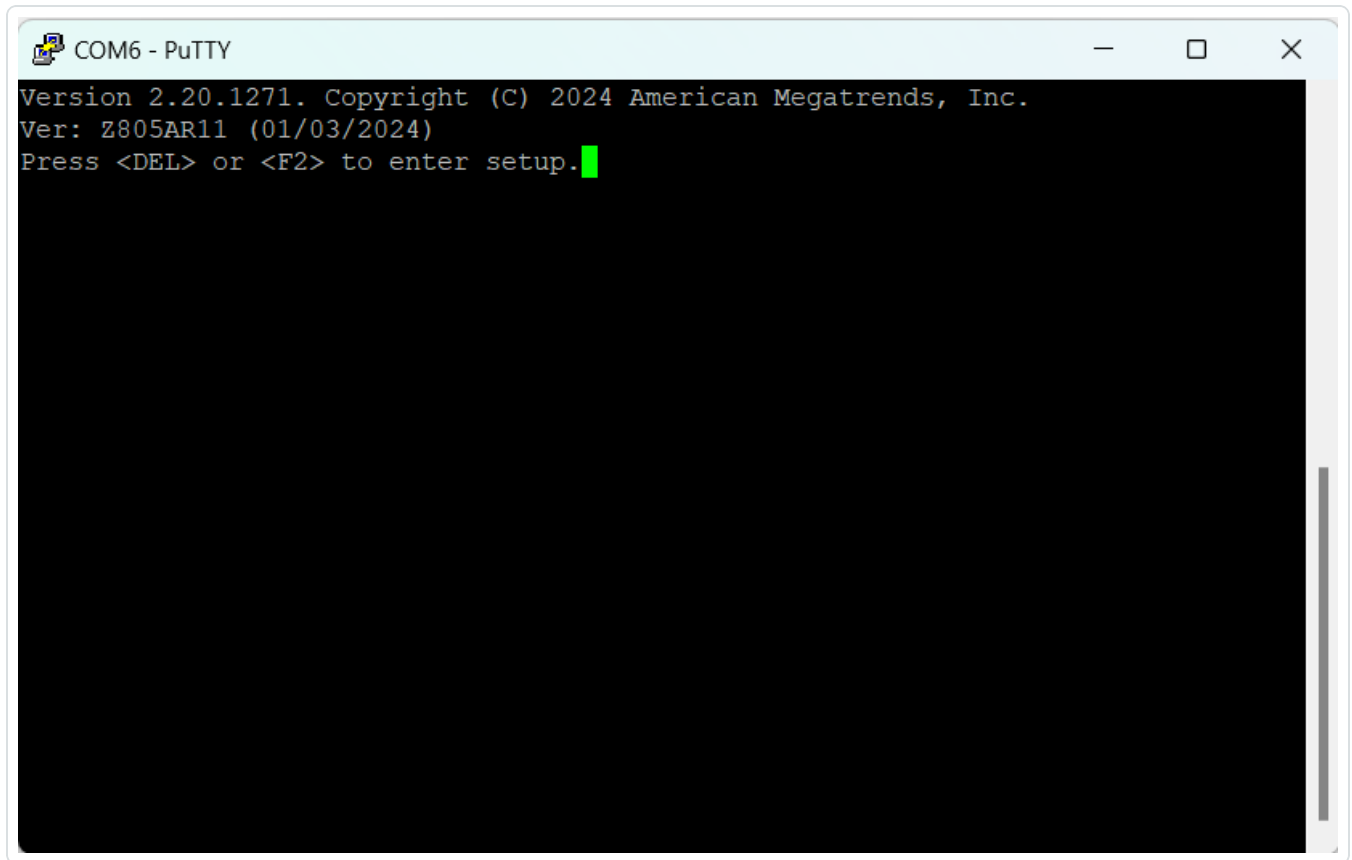
READY

START CLOSE

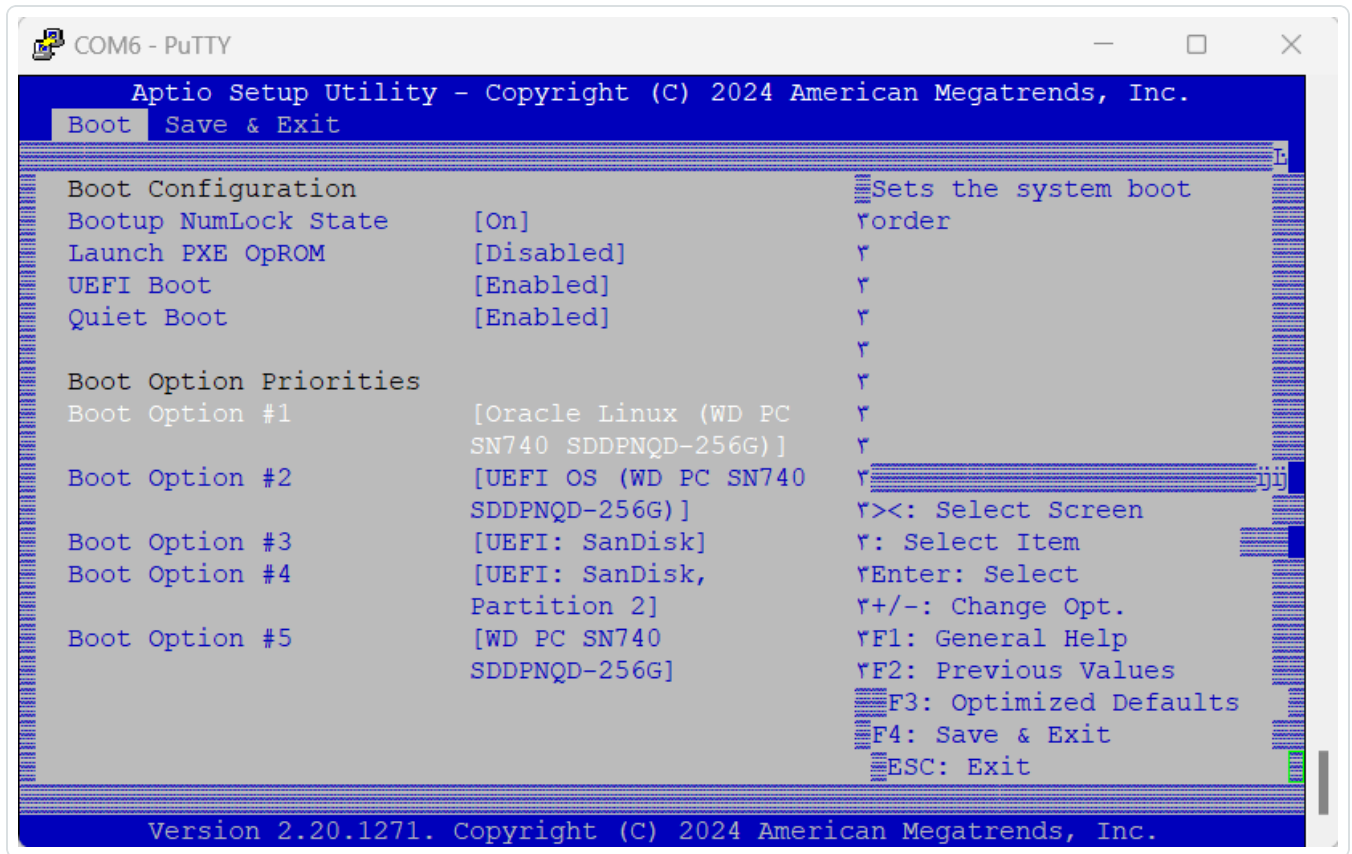
Using image: Tenable-Core-OL8-Tenable.ot-offline-20240315.iso



3. When finished, plug the USB drive into a USB port on the OT Security appliance.
4. Connect to the appliance via the Console Serial interface (Baud rate of 115200 bps with an 8N1 configuration), and power it on.

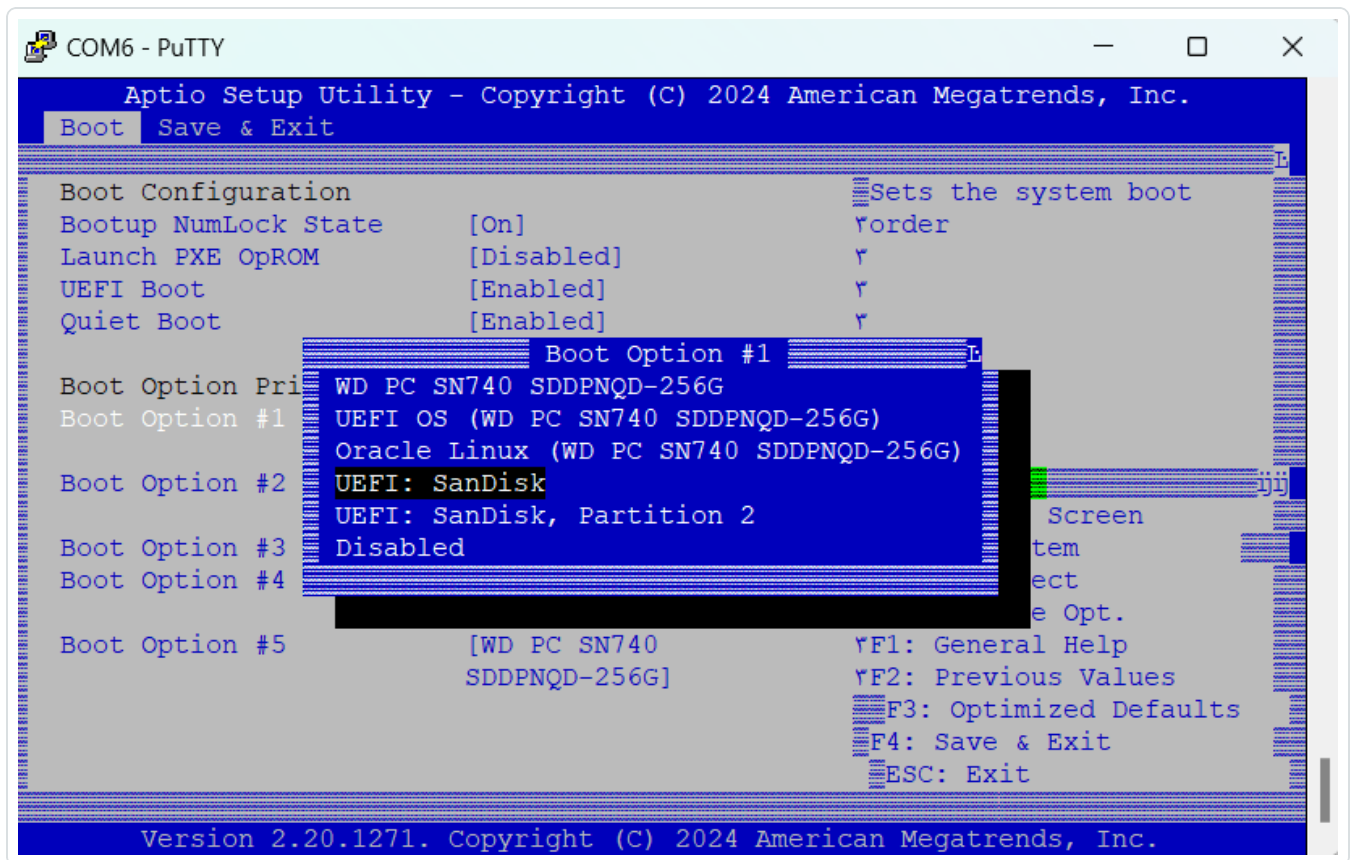


5. When prompted, press to enter the setup.
6. In the system setup, use the arrow keys to navigate to the **Boot** section.



7. Select **Boot Option #1**, and change it to your USB drive.

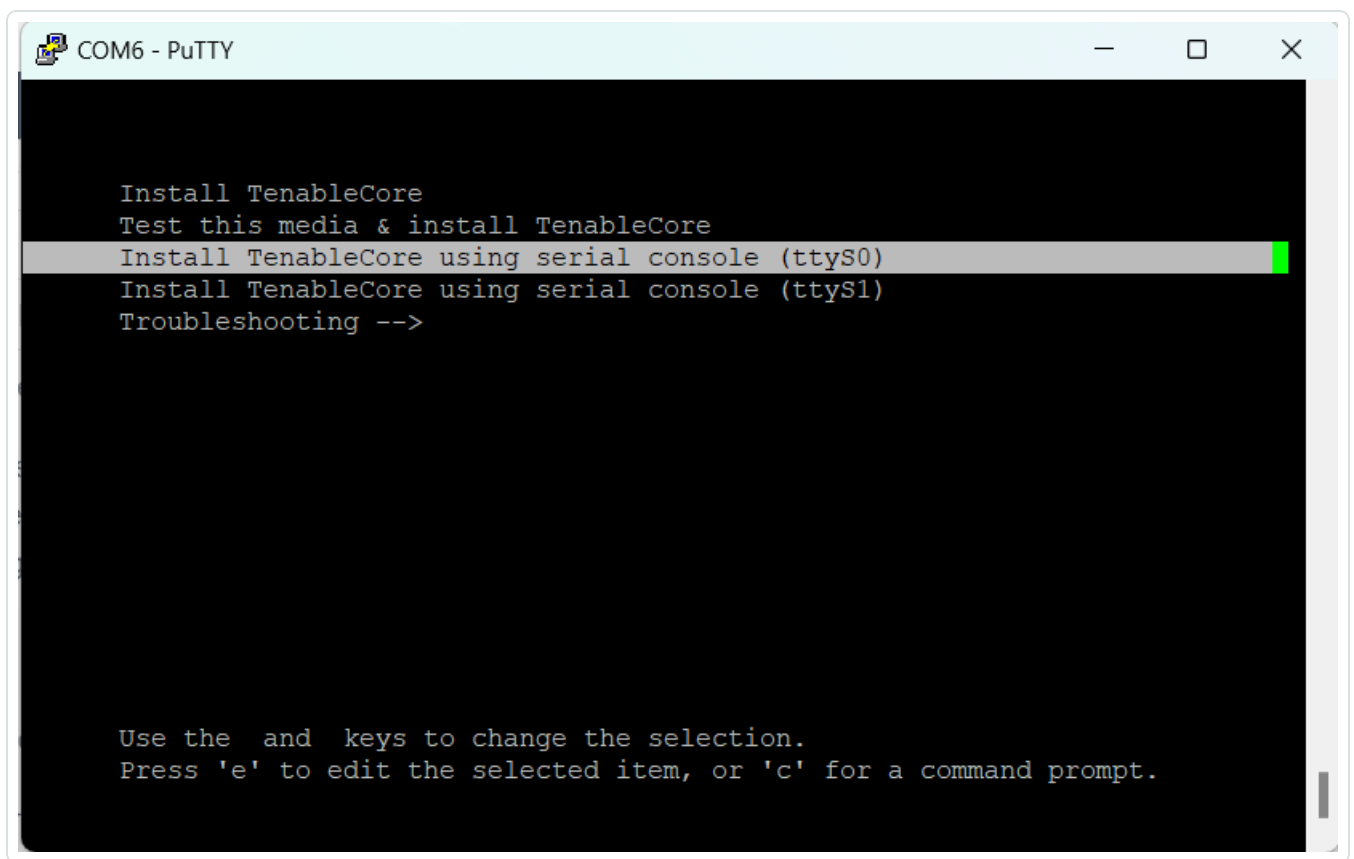
Note: Use the Unified Extensible Firmware Interface (UEFI) option.



Note: You can use “One-shot boot” on appliances that support the feature.

8. In the **Save & Exit** section, select **Save Changes and Reset**.
9. After the appliance restarts, and at the prompt, select **Install TenableCore using serial console (ttyS0)**. This ensures that the installation output is pushed into the serial console connection of the appliance.

Note: If your hardware supports a monitor output (VGA, HDMI, and so on), you can select the **Install TenableCore** option. In this case, the output of the installation appears on your connected monitor.



Allow the appliance to finish the installation. The system might reboot multiple times. The installation is complete when a login prompt appears. The system might shut down after the installation completes, by design on some appliances.

Note: The system might perform a few installation procedures even after the login prompt appears. Tenable recommends that you wait a few minutes before starting the Tenable Core setup wizard.

10. Unplug the USB drive only after the installation is complete.

What to do next

[Connect OT Security to the Network](#)

Install OT Security ICP Virtual Appliance

To deploy Tenable Core + OT Security as a VMware virtual machine, you must download the Tenable Core + OT Security .ova file and deploy it on a hypervisor.



Note: If deploying the .iso file instead of the pre-configured .ova:

- Follow the [system requirements](#) for Tenable Core + OT Security.
- When prompted to choose a setup method, select **Install Tenable Core**. See [Clean Install Tenable Core + Tenable OT Security](#).
- Follow and monitor the installation process using the installation user interface via the virtual machine console. The installation process is fully automated and so do not interact with the system until the installation is fully complete.

Before you begin:

- Confirm your environment supports your intended use of the instance, as described in [System Requirements](#).
- Confirm your internet and port access supports your intended use of the instance, as described in [Access Requirements](#).

To deploy Tenable Core + OT Security as a VMware virtual machine:

1. Download the Tenable Core + OT Security .ova file from the [Tenable Downloads](#) page.
2. Open your VMware virtual machine in the hypervisor.
3. Import the Tenable Core + OT Security VMware .ova file from your computer to your virtual machine. For information about how to import a .ova file to your virtual machine, see the [VMware documentation](#).
4. In the setup prompt, configure the virtual machine to meet your organization's storage needs and requirements, and those described in [OT Security System Requirements](#).
5. Launch your Tenable Core + OT Security instance.

The virtual machine boot process appears in a terminal window. The boot process may take several minutes to complete.

Note: The system might perform a few last installation procedures even after the login prompt appears. Tenable recommends that you wait a few minutes before starting the Tenable Core setup wizard.



Note: If you want to increase your disk space to accommodate your organization's data storage needs, see [Disk Management](#).

What to do next

[Connect OT Security to the Network](#)

Connect OT Security to the Network

You can use OT Security for both Network Monitoring and Active Query. For more information, see [Network Considerations](#).

- **Network Monitoring** – Connect the unit to a mirroring port on the network switch connected to the appropriate controllers/PLCs.
- **Active Query** – Connect the unit to a regular port that has an IP address on the network switch connected to the appropriate controllers/PLCs.

In the default configuration, the Active Query and the Management Console use the same port on the unit (Port 1). However, after the initial setup, you can separate the Management port from the Active Query port, by configuring management on Port 3. After this configuration, you can connect Port 3 on the unit to a regular port on the switch to perform the management as described in [Connect the Separate Management Port \(Port Separation\)](#).

For the initial setup, 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:

On a hardware appliance:

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.

On a virtual appliance:



If you deployed the appliance using the .ova file, the appliance comes pre-configured with four network interfaces.

If you deployed a custom virtual appliance using the .iso file, make sure to configure the virtual machine as per the requirements described in [System Requirements](#). For more information on configuring networking on VMware virtual machines, see the [VMware documentation](#).

Configure OT Security ICP

Objective: Prepare the software for activation.

After you install OT Security ICP, you can configure your OT Security. Configuration involves the following steps:

1. [Set up Tenable Core](#) – Complete the initial setup for Tenable Core via CLI or the user interface.
2. [Install OT Security on Tenable Core](#) – Complete your OT Security installation on Tenable Core.
3. [Configure OT Security Settings using Setup Wizard](#) – Configure basic settings of your OT Security ICP using the Setup Wizard.

Set up Tenable Core

You can do the initial configuration of Tenable Core from both the CLI and the Tenable Core user interface.

Using the Tenable Core user interface is mandatory to finish the configuration for virtual appliance deployments.

Note: If you do not complete the setup wizard in ~30 minutes, restart the appliance.

Initial Configuration via CLI (Optional)

To configure Tenable Core using CLI:

1. Connect to the OT Security appliance using the serial console as described in [Clean Install Tenable Core + OT Security](#).
2. Log in with username `wizard` and password `admin`.



The **Network Manager** terminal interface appears.

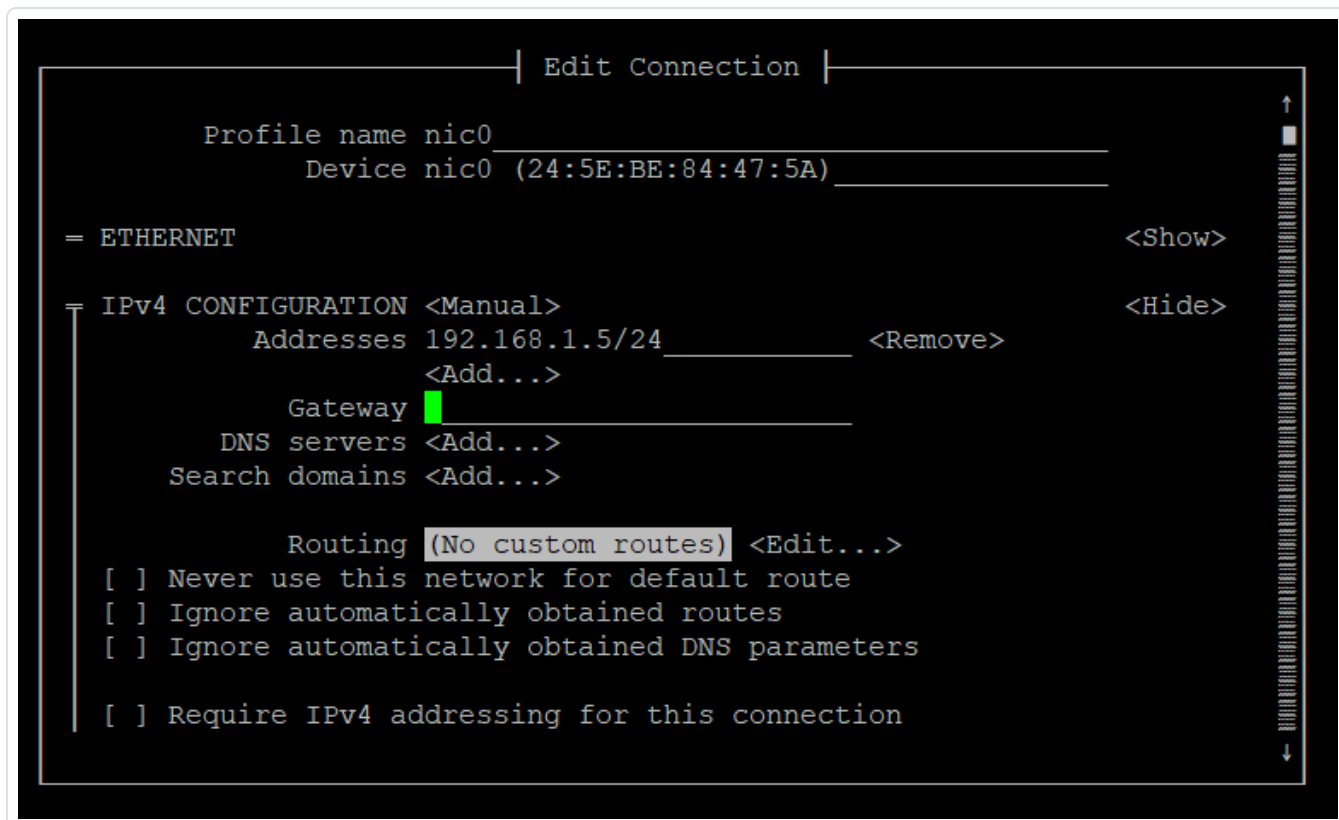
```
#####  
This system is restricted to authorized users only. Individuals attempting  
unauthorized access will be prosecuted. Continued access indicates  
your acceptance of this notice.  
#####  
tenable-bztwsz8g login: wizard  
Password:  
#####  
This system is restricted to authorized users only. Individuals attempting  
unauthorized access will be prosecuted. Continued access indicates  
your acceptance of this notice.  
#####  
Would you like to configure a static address? (y/n) 
```

3. (Optional) To configure the management IP address, type **y**.
4. Select **nic0** (or **nic2** if using the **split-port** configuration).



5. Press **Enter**.

The **Edit Connection** window appears.



6. Navigate using the arrow keys and configure your required IP address, Default-Gateway, DNS Servers, and so on. You can change this configuration later.

7. Using the down-arrow, navigate to the bottom of the screen and select **<OK>**.

The **Network Manager** window appears.

8. Select **<Quit>**.

Note: By default `nic0` is preconfigured with an IP address of `192.168.1.5/24`. You can use this IP address to finish configuring the system using the Tenable Core interface (port 8000) from any IP network reachable PC.

9. Type **y** and follow the prompts to create an administrator account. Use this account only to log in to Tenable Core (terminal console, SSH, and the Tenable Core user interface). Use separate accounts for the OT Security application.



```
#####  
# If you need to update your IP configuration, use the nmtui #  
# command to return to the configuration menu #  
#####  
  
#####  
# An administrator account needs to be created to use Tenable Core #  
#####  
Create an administrator account now? (y/n) 
```

10. After you create the account, use it to log in into the terminal via the console or using a network connection: via SSH or the Tenable Core interface (<https://<mgmt-IP>:8000>).

Initial Configuration via Tenable Core User Interface

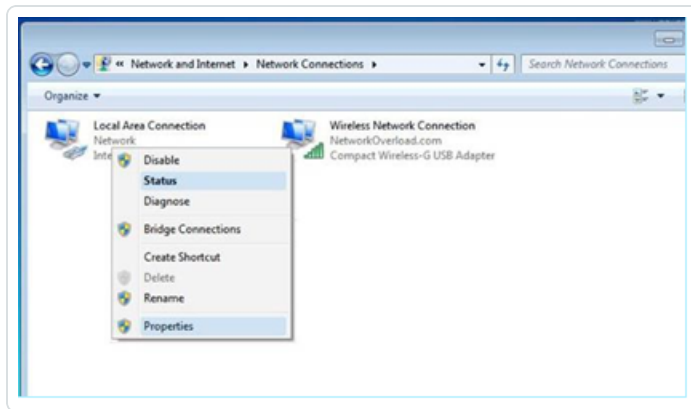
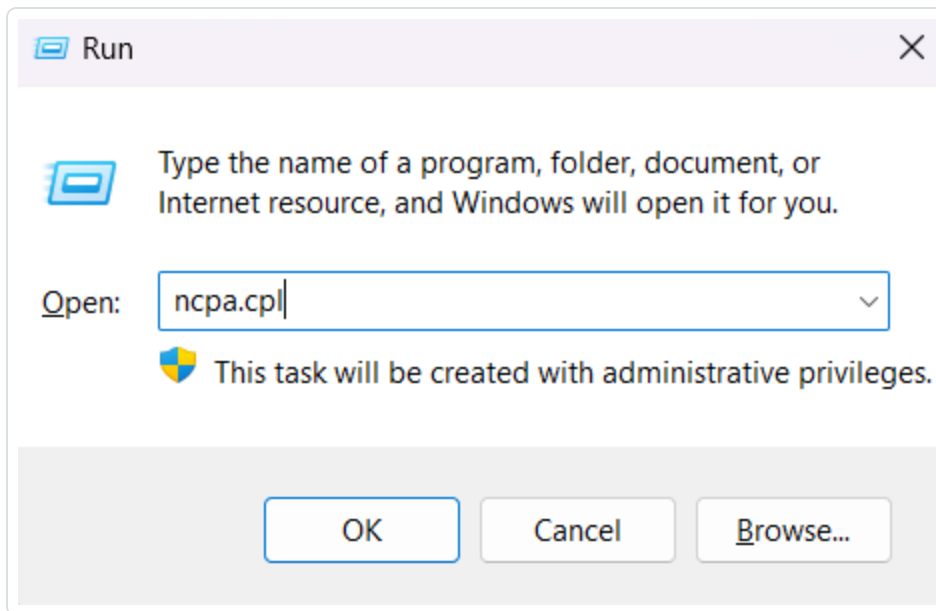
To complete the initial configuration via the Tenable Core user interface (available on <https://<mgmt-IP>:8000>) you need a working network connection to the appliance.

If you have not configured the management IP address, you can use either a directly connected PC or an appropriately configured network to reach the Tenable Core user interface on either of the following:

- **Port 1 / nic0** – default management interface, pre-configured with IP address 192.168.1.5/24
- **Port 4 / nic3** – engineering interface, pre-configured with IP address 192.168.3.3/24. If not changed later, this can be used for recovery procedures.

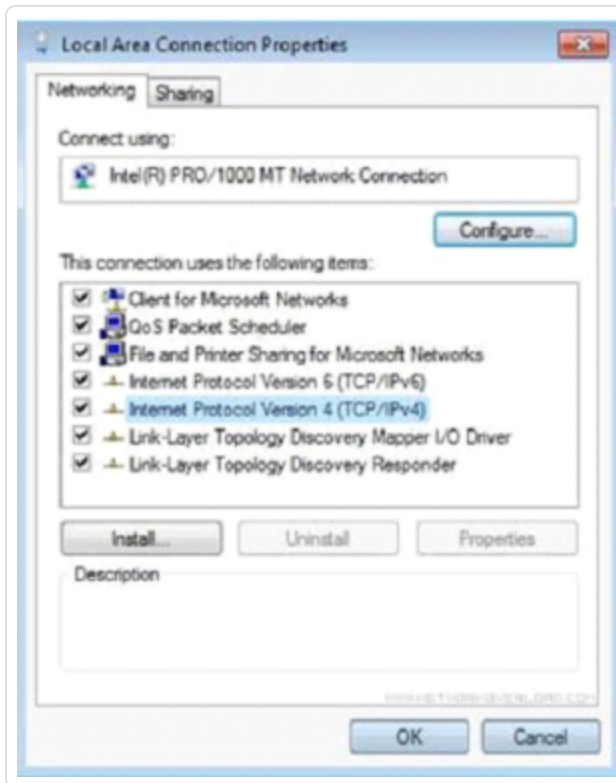
To connect to Tenable Core directly via your PC or laptop:

1. Connect an Ethernet cable between your PC and one of the pre-configured ports on the OT Security appliance.
2. On Windows, use **win+R** to open **Run** and type `ncpa.cpl` to open **Network Connections**.



3. Right-click on your network connection (named **Local Area Connection**) and select **Properties**.

The **Local Area Connection Properties** window appears.



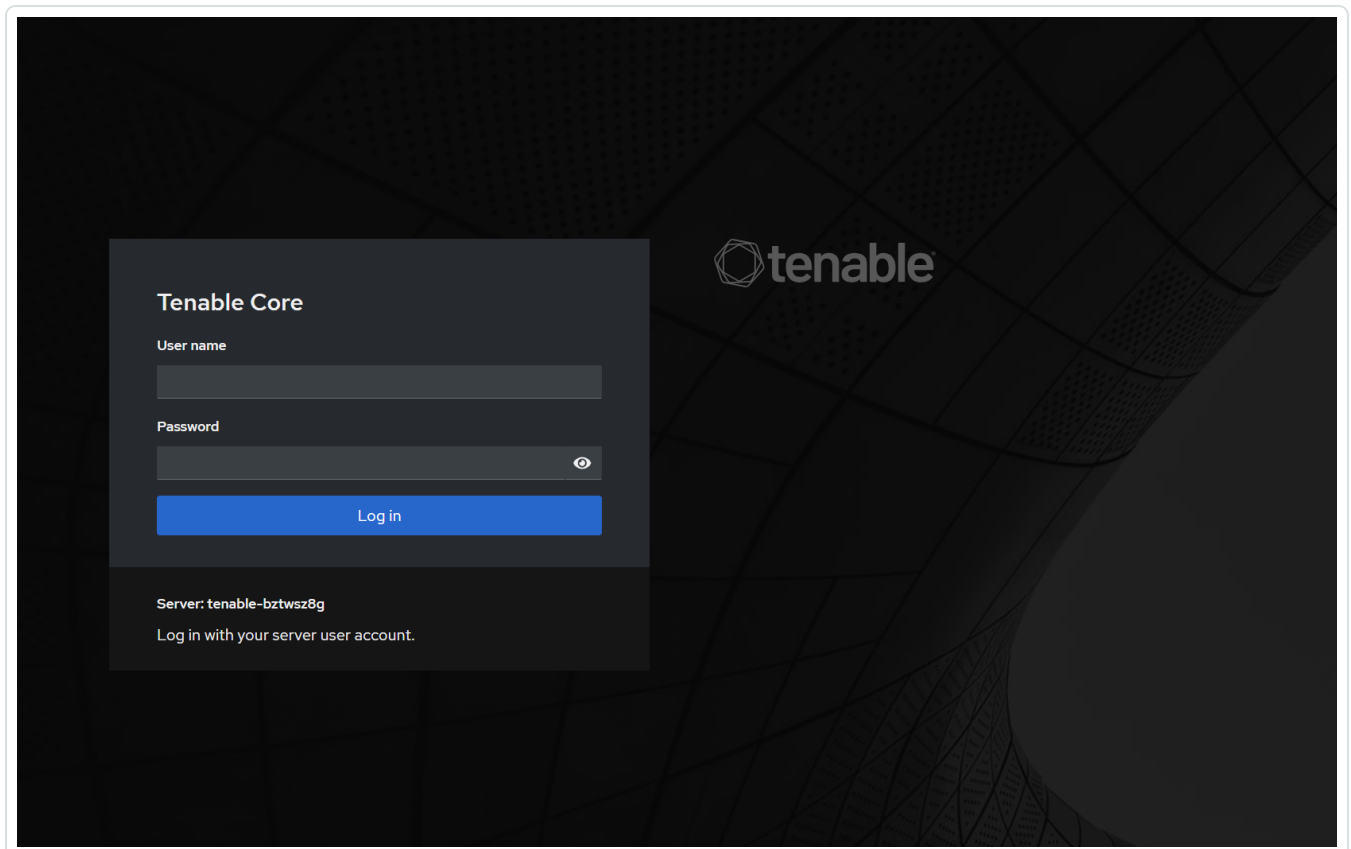
4. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

The **Internet Protocol Version 4 (TCP/IPv4) Properties** window appears.





5. Select **Use the Following IP address**.
6. In the **IP address** box, type an appropriate IP address for the interface you are connecting to. For example, 192.168.1.10 for the default address of Port 1 / nic0 or 192.168.3.10 for the default address of Port 4 / nic3.
7. In the **Subnet mask** box, type 255.255.255.0.
8. Click **OK**.
9. From your Chrome browser, navigate to `https://<mgmt-ip>:8000`.



10. If you have not yet configured the administrator user account, the system prompts you to do so now, then re-login with your newly created user. For more information, see [Create and initial Administrator Account](#).

After creating the administrator account, Tenable recommends that you configure the management IP address. If you intend to use the **split-port** configuration, make sure the interfaces can reach the appropriate networks. For more information, see [Network Considerations](#).



Note: A **split-port** configuration moves the management from port 1 (nic0) to port 3 (nic2). You might lose connectivity and may need to reconnect to Tenable Core using a new IP address, depending on your network configuration.

Note: To configure or change the management IP address, [log in back into Tenable Core](#) and enable administrative access and [edit the network configuration](#).

What to do next

[Install OT Security on Tenable Core](#)

Install OT Security on Tenable Core

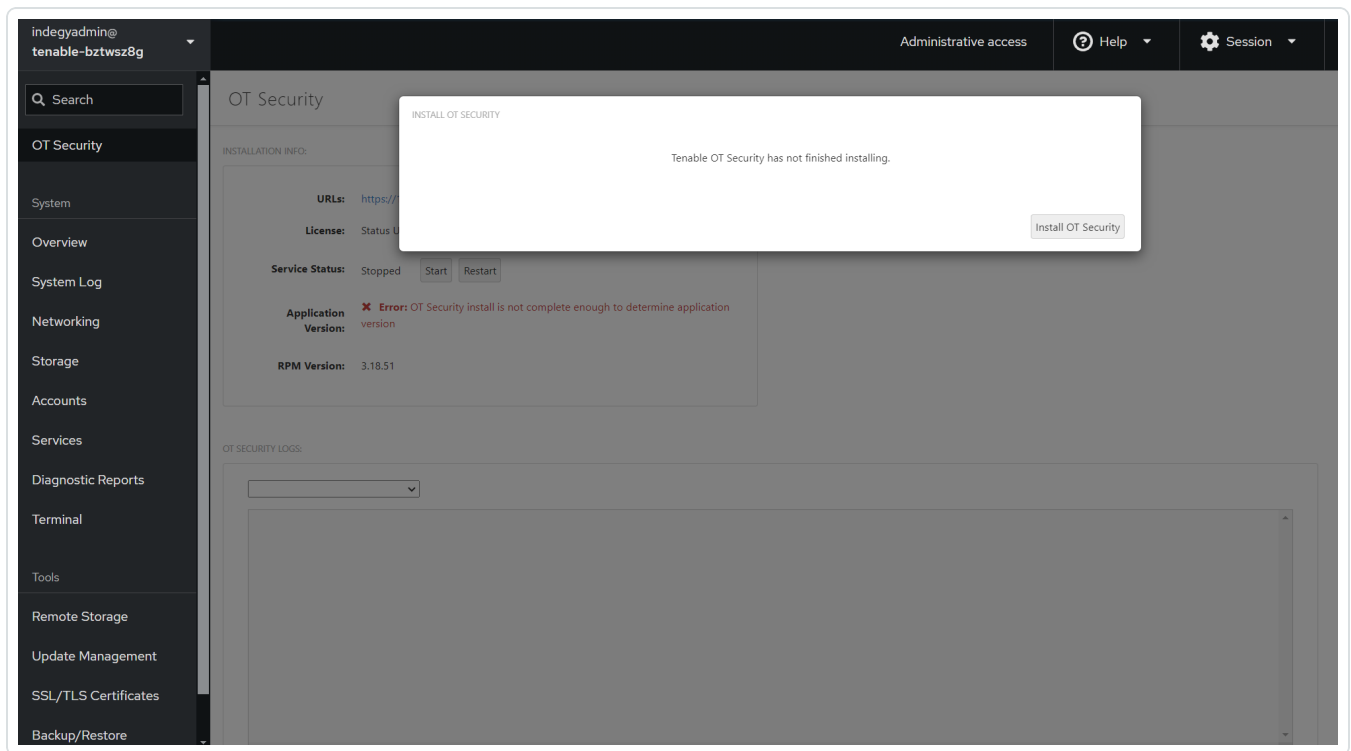
On non-Tenable-provided hardware or virtual machines, you must finish the installation of the OT Security application manually.

To install OT Security on Tenable Core:

1. To log into Tenable Core from your Chrome browser, navigate to `https://<mgmt-ip>:8000`.

Note: Make sure you have Administrative access.

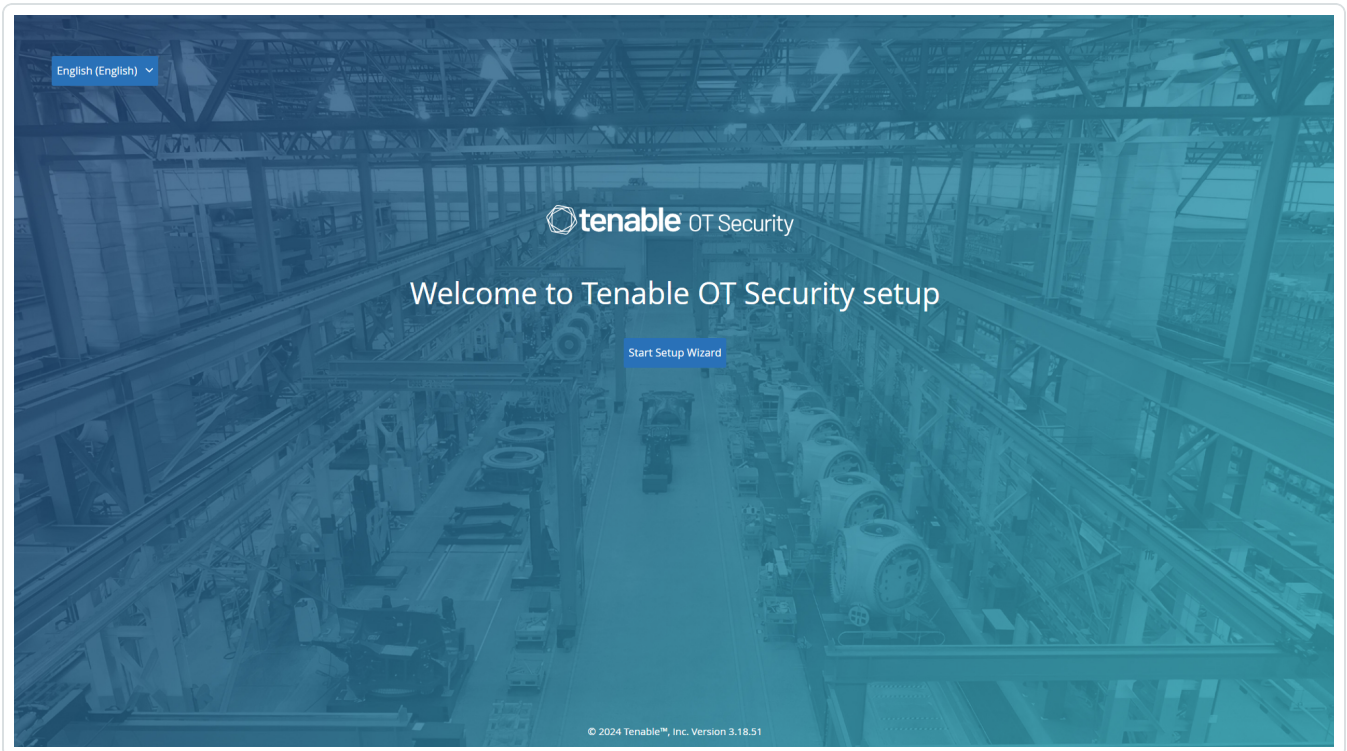
2. Navigate to OT Security.
3. At the installation prompt, click **Install Tenable OT Security**.



Note: The installation process might take some time to complete. Do not disrupt the installation process.

When the installation completes, you can log into the OT Security user interface at <https://<mgmt-ip>>.

`mgmt-ip` is your IP address that appears in the **URLs** field at the top of the Tenable Core window.



What to do next

[Configure OT Security Settings using Setup Wizard](#)

Configure OT Security Settings using Setup Wizard

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

Note: You can modify the configuration if necessary in the **Settings** screen in the Management Console (user interface).

To access the setup wizard, you must first log into the OT Security management console. For information about how to log into the management console, see [Log into the OT Security Management Console](#)

Configure the following using the setup wizard:

1. [User Info](#)
2. [Device](#)
3. [System Time](#)
4. [Connect the Separate Management Port \(Port Separation\)](#)



Note: After you complete the setup wizard, OT Security prompts you to restart the system.

Log into the OT Security Management Console

To log into the OT Security management console:

1. Do one of the following:

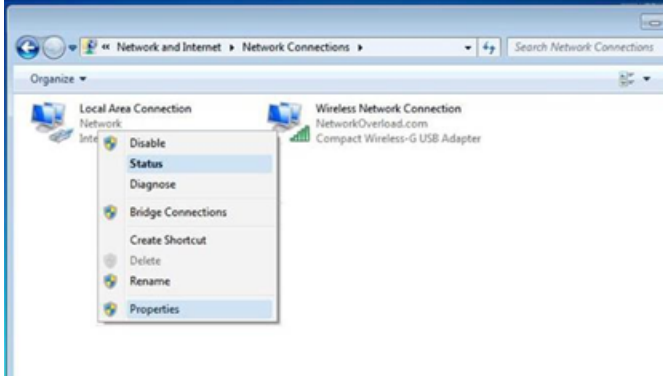
- Connect to the Management Console workstation (for example: PC, laptop, and so on) directly to Port 1 of the OT Security appliance using the Ethernet cable.
- Connect the Management Console workstation to the network switch.

Note: Ensure that the Management Console workstation is either part of the same subnet as the OT Security appliance (192.168. 1.0/24) or routable to the unit.

2. Set up a static IP to connect to the OT Security appliance as follows:

- a. Go to **Network and Internet > Network and Sharing Center > Change adapter settings**.

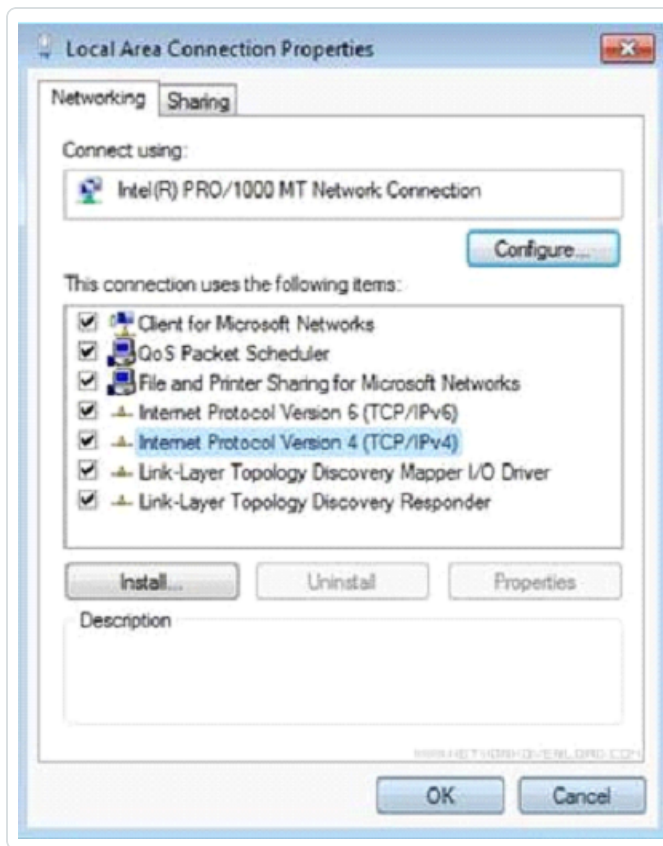
The **Network Connections** screen appears.



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

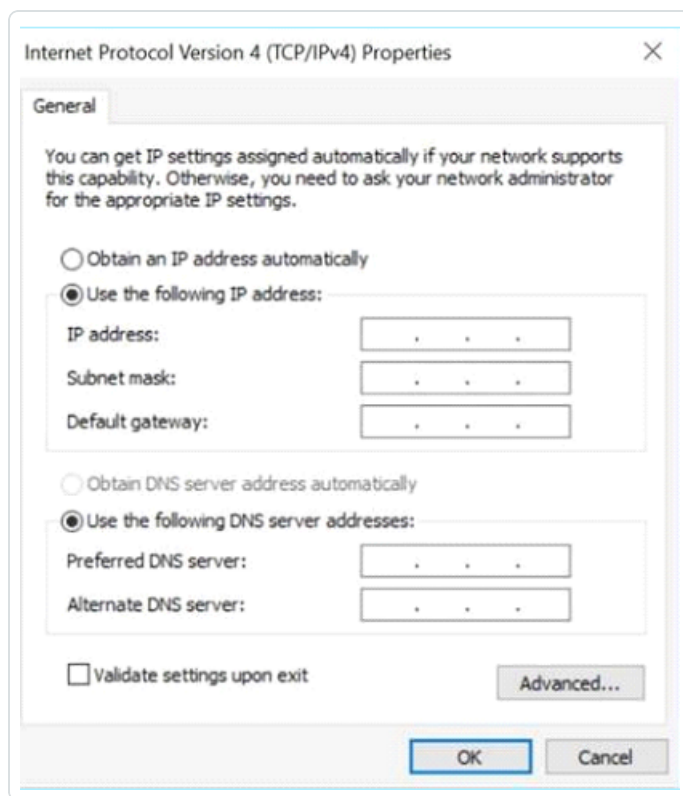
- b. Right-click on **Local Area Connections** and select **Properties**.

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 appears.



- d. Select **Use the Following IP address**.
- e. In the **IP address** box, type 192.168.1.10.
- f. In the **Subnet mask** box, type 255.255.255.0.
- g. Click **OK**.

OT Security applies the new settings.

- h. From your Chrome browser, navigate to <https://192.168.1.5>.

The **Welcome** screen of the setup wizard opens.



Note: Access to the user interface requires the latest version of Chrome.

- i. Click **Start Setup Wizard**.

The setup wizard opens with the **User Info** page.

What to do next

[User Info](#)

User Info

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

Note: You can modify the configuration if necessary in the **Settings** screen in the Management Console (user interface).

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.

Note: In the setup wizard, you can configure the credentials for an Administrator account. After you log in to the user interface, you can create additional user accounts. For more information about user accounts, see the section [Users and Roles](#).

1. In the **Username** box, type a username 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** box, re-type the username.
3. In the **Full Name** section, type your complete **First and Last Name**.

Note: This is the name that appears in the header bar and on your activity logs in the system.



4. In the **Password** box, type a password 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** box, re-type the identical password.
6. Click **Next**.

The **Device** page of the setup wizard opens.

What to do next

Configure the [Device](#).

Device

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

Note: You can modify the configuration if necessary in the **Settings** screen in the Management Console (user interface).



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

On the **Device** page, provide information about the OT Security platform:

1. In the **Device Name** box, type a unique identifier for the OT Security platform.
2. In the **Port Configuration** section, do one of the following:
 - **Port separation** – If you want to use one port for management and a separate port for Queries, select the **Separate management from active queries** checkbox. Selecting this option configures 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 want to maintain the Queries and Management in the same port, do not select the **Separate management from active queries** checkbox. In this case, you can skip step number 3 of this procedure and proceed to step 4.

3. If you select the **port separation** option:

- a. In the **Active Queries IP** box, type the IP address of the unit's Queries port.

This port connects to a regular port in the network switch, which can contact or route to the controllers. As OT Security connects to the controllers, it needs an IP address within the network subnet.

- b. In the **Active Queries Subnet Mask** box, type the subnet mask of the Queries port.

- c. In the **Active Queries Gateway** box (optional), type the IP address of the gateway in the operations network.

4. In the **Management IP** box, type an IP address (within the network subnet) to apply to the OT Security platform.

This becomes the OT Security management IP address. This IP address is also the Queries address if there is no separation between the ports.

5. In the **Management Subnet Mask** box, type the subnet mask of the network.

6. (Optional) If you want to set up a Gateway, in the **Management Gateway** box, type the Gateway IP for the network.

Note: If you do not provide the Management Gateway IP, OT Security cannot communicate with external components outside of the subnet, such as email servers, syslog servers, and so on.

7. **Initial Asset Enrichment Active Query** comprises a set of queries executed on every asset detected within the system.

This allows OT Security to classify the assets. To run these queries on each new asset that OT Security discovers, enable the **Initial Asset Enrichment Active Query** toggle.

8. Click **Next**.



The **System Time** page of the setup wizard opens.

What to do next

Configure the [System Time](#) settings.

System Time

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

Note: You can modify the configuration if necessary in the **Settings** screen in the Management Console (user interface).


System Time

The screenshot shows the 'Setup Wizard' interface. At the top, there is a progress bar with three steps: 'User info', 'Device', and 'System Time'. The 'System Time' step is currently active. Below the progress bar, there are three input fields: 'Time Zone' with the value 'Etc/UTC', 'Date' with the value '10/1/2020', and 'Time' with the value '07:10:46 AM'. At the bottom of the form, there are two buttons: 'Back' on the left and 'Complete and Restart' on the right.

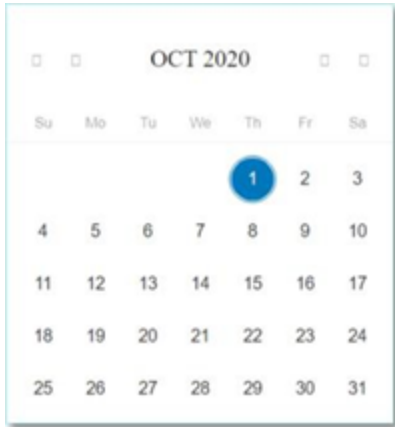
Note: Setting the correct date and time is essential for accurate recording of logs and alerts.

In the **System Time** page, the correct time and date appear automatically. If not, do the following:



1. In the **Time Zone** drop-down box, select the local time zone at the site location.
2. In the **Date** box, click the calendar icon .

A pop-up calendar appears.



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

Note: If you want to edit any of the previous pages of the setup wizard, click **Back**. After clicking **Complete** and **Restart** you cannot return to the setup wizard. However, you can change the configuration settings on the **Settings** page of the user interface.

5. To complete the setup, click **Complete and Restart**.

Once the restart completes, OT Security redirects you to the **Licensing** window.

Note: If you selected the port separation option, change your network connections as described in [Connect the Separate Management Port \(Port Separation\)](#).

What to do next

Perform the following:

- [Connect the Separate Management Port \(Port Separation\)](#)
- [OT Security License Activation](#)

Connect the Separate Management Port (Port Separation)



If you selected the **Port Separation** option (to separate Queries from the Management), you must connect Port 3 on the OT Security appliance (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.

What to do next

[OT Security License Activation](#)

OT Security License Activation

Objective: Unlock system features with license activation.

Tenable calculates licenses based on the number of unique IPs in the system. Each IP address requires a separate license. For example, Tenable bases licensing on the number of unique IPs, even if multiple devices share the same IP address, or if several devices connected to the same backplane share the same three IPs. Therefore, you need three licenses, regardless of the number of devices.

After you install the [OT Security Appliance](#), you can [activate](#) your license.

Note: To update or reinitialize your OT Security license, contact your Tenable Account Manager. Once your Tenable account manager updates your license, you can [update](#) or [reinitialize](#) your license.

For information about deploying and licensing Tenable OT Security for Tenable One, see the [Tenable One Deployment Guide](#).

Before you Begin

- [Install the OT Security Appliance](#).
- Make sure that you have the license code (20 characters letter/numbers), which you received from Tenable when you ordered your device.



- Make sure you have access to the internet. If your OT Security device is not connected to the Internet, you can register the license from any PC.
- Make sure you have access to the [Tenable Provisioning](#) portal. For access, contact your Tenable Customer Success Manager.

Activate your OT Security license

You can activate your OT Security license and facilitate the Tenable provisioning portal for creating new sites to manage your assets.

To activate your OT Security license:

1. Log in to the [Tenable Provisioning](#) portal using your community account.

The **Provisioning** page appears with the products for which you have licenses.

2. In the left pane, select **Tenable OT Security**.

The OT Security licenses appear with details such as the purchase date, expiration date, and number of licensed IPs and sites.

3. From the **Code** column, copy the 20-digit OT Security license code.

4. Generate the activation certificate in OT Security:

- a. Go to the OT Security **License Activation** page.

- b. In step 1, click **Enter new license code**.

The **Enter new license code** panel appears on the right.

- c. In the **License code** box, paste the code that you copied from the provisioning portal.

- d. Click **Verify**.

OT Security enables the **Generate activation certificate** section.

- e. Click **Generate Certificate**.

The **Generate Certificate** panel appears on the right.

- f. Click **Copy text to clipboard**, then click **Done**.



OT Security generates the certificate, which you must provide in the Tenable Provisioning Portal to add your sites.

5. In step **3 Enter activation code**, click the **Self-service** link to open the [Tenable Provisioning](#) portal.

Note: To activate your evaluation period, click the **Click here** link.

6. Navigate to the **Tenable OT Security Provisioning** page and click **+ Add Site**.


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

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

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

- c. In the **Activation Certificate** box, paste the certificate that you copied from OT Security. See [step f](#).
- d. Click **Create**.

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

- e. Click the  button, then click **Confirm**.
7. Navigate back to the OT Security instance and in the step **3 Enter activation code** section, click **Enter Activation Code**.

The **Enter Activation Code** panel appears on the right.

8. In the **Activation Code** box, paste the one-time generated code that you copied from the **Tenable OT Security Provisioning** page. See [step e](#).
9. Click **Activate**.

OT Security shows a confirmation message that the system activated successfully and the OT Security interface appears.



10. Click **Enable**.

OT Security is now enabled and ready to use.

11. Navigate back to the [Tenable Provisioning](#) portal and in the one-time generated activation code dialog box, click the **I have saved this certificate information or copied it to Tenable.ot for activation** checkbox.

12. Click **Confirm**.

The newly added site appears in the **Provisioning** page for OT Security.

Update your license

When you increase your asset limit, extend your license period, or change your license type, you can update your license.

Before you Begin

- Your Tenable Account Manager must have already updated your license information in their system before you can update the new license.
- You need access to the internet. If your OT Security device cannot reach the Internet, you can register the license from any PC.

To update your license:

1. Go to **Local Settings > System Configuration > License**.

The **License** window appears.

License	
LICENSE TYPE	Subscription
SUBSCRIPTION EXPIRES	Sep 17, 2024
LICENSED ASSETS	43/100 (43%)
LICENSE CODE	[REDACTED]
COMPUTER ID	[REDACTED]

2. From the **Actions** menu, select **Update license**.



The **Generate Certificate** and **Enter Activation Code** steps appear.

License

LICENSE TYPE	Perpetual
MAINTENANCE EXPIRES	Dec 29, 2993
LICENSED ASSETS	Unlimited
LICENSE CODE	[REDACTED]
COMPUTER ID	[REDACTED]

Follow these steps in order to update your license

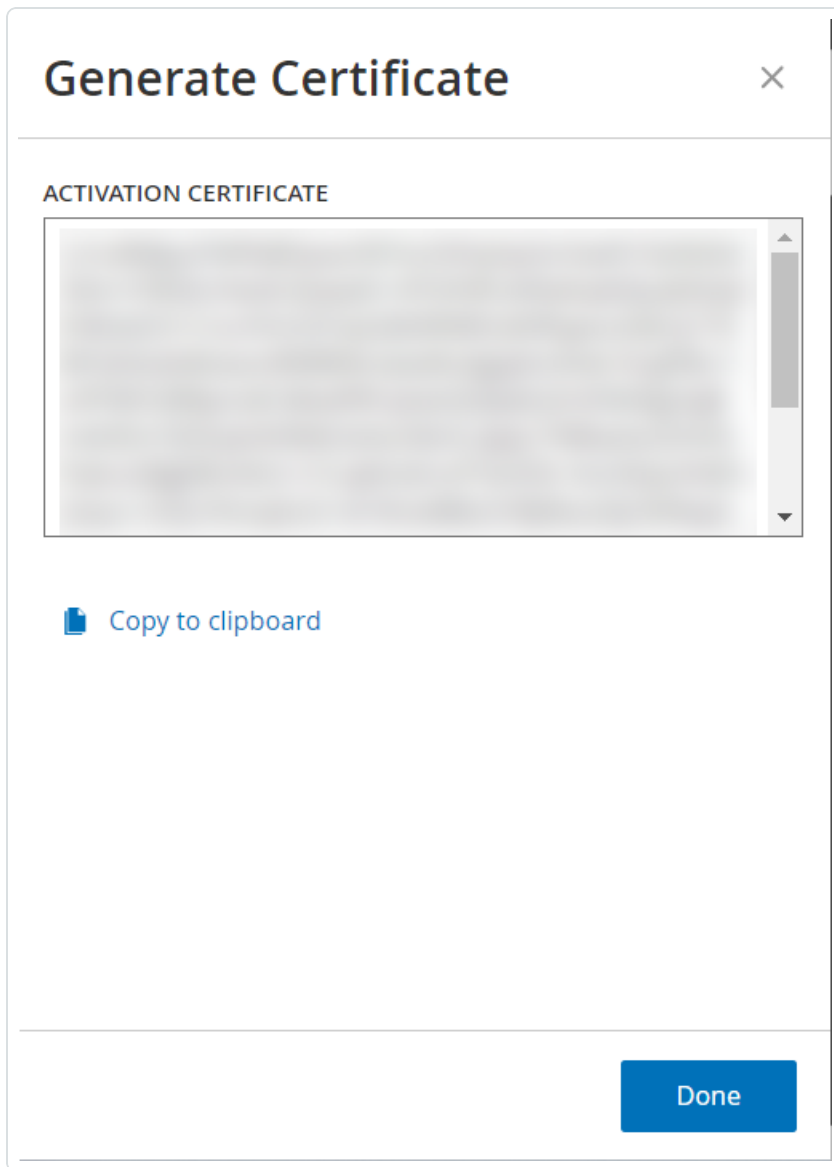
1 Certificate was generated successfully Generate certificate

2 Enter activation code, obtain an activation code from Tenable [Self-service portal](#) or from your sales rep. [Click here](#) to activate your evaluation period Enter Activation Code

Cancel


3. In the **(1) Generate activation certificate** box, click **Generate Certificate**.

The **Generate Certificate** panel appears with the **Activation Certificate**.



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

The side panel closes.

5. Edit the site details in the Tenable Provisioning portal:
 - a. In the [Tenable Provisioning](#) portal, navigate to the **Tenable OT Security Provisioning** page and in the row of the site that you want to update, click the  button.

A menu appears.

- b. Click **Edit Site**.



The edit window for the site appears.

Edit [Close]

Warning: After modifying the site size, you will need to re-enter the new activation code into your Tenable.ot instance. This will be a one-time generated code.

Label (optional) ⓘ

HQICS

IPs

1426 - +

1 4949

Activation Certificate


[Blurred Certificate Text]

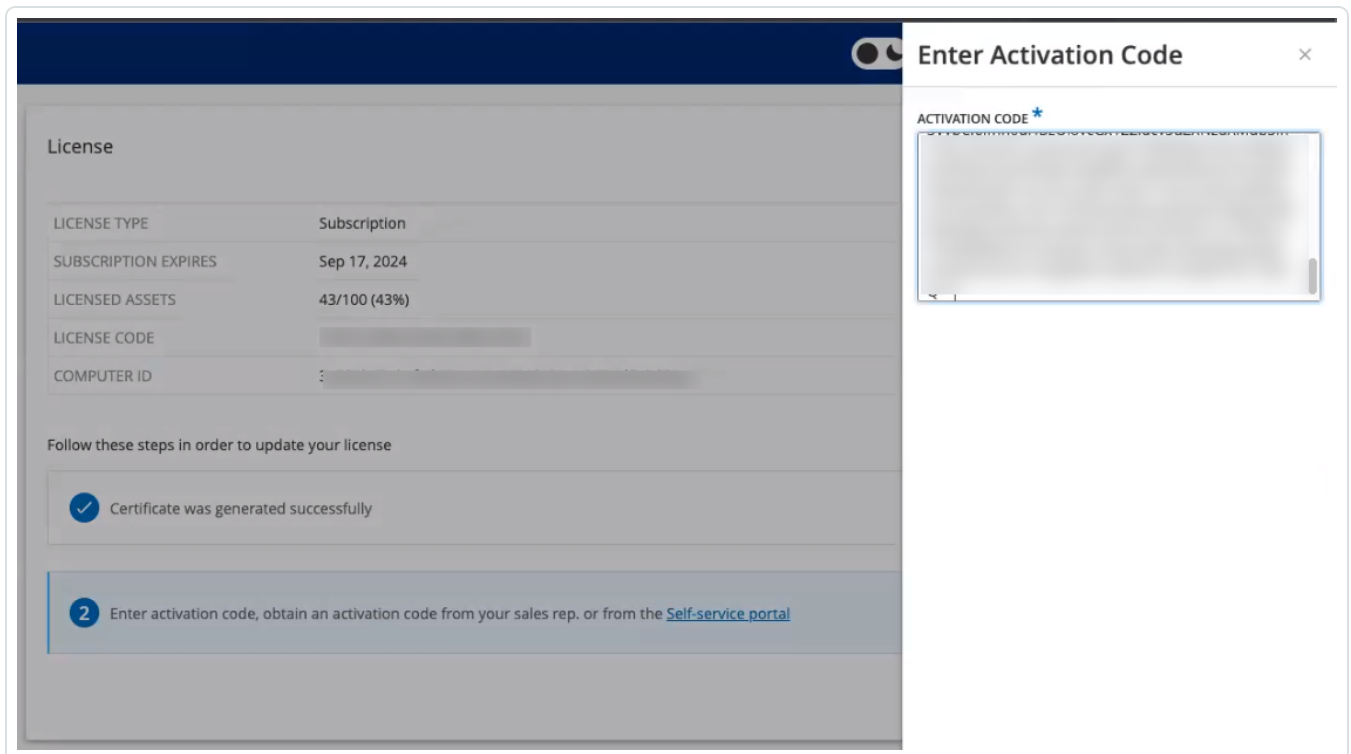
Submit **Cancel**

- c. Adjust the details as needed.
- d. In the **Activation Certificate** box, paste the certificate that you copied from the **Generate Certificate** window in OT Security.
- e. Click **Submit**.



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

- f. Click the  button, then click **Confirm**.
6. Navigate back to the OT Security instance.
7. In the **(2) Enter activation code** box, click **Enter Activation Code**.
8. In the **Activation Code** box, paste the one-time generated code that you copied from the **Tenable OT Security Provisioning** page.



9. Click **Activate**.

OT Security shows a confirmation message that the system activated successfully and the **License** page shows the updated license details.

Update your license in offline mode

1. Perform steps 1 to 4 as described in the [Update your license](#) section.
2. In the **(2) Enter activation code** box, click the Self-service portal link.



License

LICENSE TYPE	Perpetual
MAINTENANCE EXPIRES	Dec 29, 2993
LICENSED ASSETS	Unlimited
LICENSE CODE	[REDACTED]
COMPUTER ID	[REDACTED]

Follow these steps in order to update your license

Certificate was generated successfully Generate certificate

2 Enter activation code, obtain an activation code from Tenable [Self-service portal](#) or from your sales rep. [Click here](#) to activate your evaluation period **Enter Activation Code**

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

Activate Tenable OT Security Offline

1 Activation Info

Offline Activation Details

Tenable OT Security

Activation Certificate

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 Security Activation Certificate?](#)

[Tenable Security Center Offline Activation](#)

[Tenable Nessus Professional Offline Activation](#)



Note: You can 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 logged in to tenable.com, you can log in using your email address and password. Use the email account where you received your **License Code**. If you do not have the login credentials, you can either click on **Don't remember your password** (and follow the prompts) or reach out to your Tenable account manager.

3. In the **Activation Certificate** box, paste the **Activation Certificate**.
4. In the **License Code** box, type your 20-character **License Code** (which you can copy and paste from the **License** screen).
5. Click the **I have read and understand the Tenable Software License Agreement** checkbox.

The screenshot shows a web interface for generating an activation code. It features a progress indicator at the top with two steps: '1 Activation Info' and '2 Confirmation'. The 'Activation Info' section includes a text area for pasting an activation certificate, a license code input field, and a checked checkbox for the license agreement. The 'Confirmation' section provides instructions and links. A 'Generate Activation Code' button is positioned at the bottom right.

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

6. Click **Generate Activation Code**.

The **Offline Activation Code Successfully Created!** window appears.

Activate Tenable OT Security Offline



Offline Activation Code Successfully Created!

Enter this activation code in the Tenable OT Security license activation or renewal/upgrade process




7. Click the  button.

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

License

LICENSE TYPE	Perpetual
MAINTENANCE EXPIRES	Dec 29, 2993
LICENSED ASSETS	Unlimited
LICENSE CODE	[REDACTED]
COMPUTER ID	[REDACTED]

Follow these steps in order to update your license

 Certificate was generated successfully

[Generate certificate](#)

2 Enter activation code, obtain an activation code from Tenable [Self-service portal](#) or from your sales rep. [Click here](#) to activate your evaluation period

Enter Activation Code

Cancel

The **Enter Activation Code** side panel appears.



9. In the **Activation Code** box, paste your activation code and click **Activate**.

Enter Activation Code

ACTIVATION CODE *

Cancel Activate

The side panel closes, and OT Security updates the license.

Reinitialize your 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 (that is, if you receive a new license), use the following procedure.

Before you Begin

- 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 you cannot connect the OT Security device to the Internet, you can register the license from any PC.

To reinitialize your license:

1. Go to **Local Settings > System Configuration > License**.

License	
LICENSE TYPE	Subscription
SUBSCRIPTION EXPIRES	Sep 17, 2024
LICENSED ASSETS	43/100 (43%)
LICENSE CODE	[blurred]
COMPUTER ID	[blurred]

2. From the **Actions** menu, select **Reinitialize license**.

A confirmation window appears.

3. Click **Reinitialize**.

i Reinitialize License ×

Are you sure?
Once you complete the three-step process to reinitialize your license, the current license will be replaced by the new one. Until the process is completed, your current license will remain in effect.

Cancel Reinitialize

The **License** window appears with the three reinitialization steps.



License

LICENSE TYPE	Perpetual
MAINTENANCE EXPIRES	Dec 29, 2993
LICENSED ASSETS	Unlimited
LICENSE CODE	[REDACTED]
COMPUTER ID	[REDACTED]

Follow these steps in order to reinitialize your license

- 1 Enter license code
- 2 Generate activation certificate
- 3 Enter activation code, obtain an activation code from Tenable [Self-service portal](#) or from your sales rep. [Click here](#) to activate your evaluation period

4. Follow the system start-up steps for activating your license. See [Activate your License](#).

After you provide your **Activation Code**, your new license replaces your current license.

What to do next

[Enable the OT Security System](#)

Launch OT Security

Objective: Start the system and begin using it for your OT Security needs.

After you configure Tenable Core + OT Security, enable the system to start using OT Security.

1. [Enable the OT Security System](#) – Enable the OT Security system after you activate your license.



2. [Use OT Security](#) – Configure your monitored networks, port separation, users, groups, authentication servers, and so on to start using OT Security.

Enable the OT Security System

After completing the license activation, OT Security displays the **Enable** button.



Enable OT Security in order to activate the system's core functionality, such as:

- Identifying assets in the network.
- Collecting and monitoring of all network traffic.
- Logging 'Conversations' on the network.

You can view all compiled data and analysis from these functionalities in the user interface.

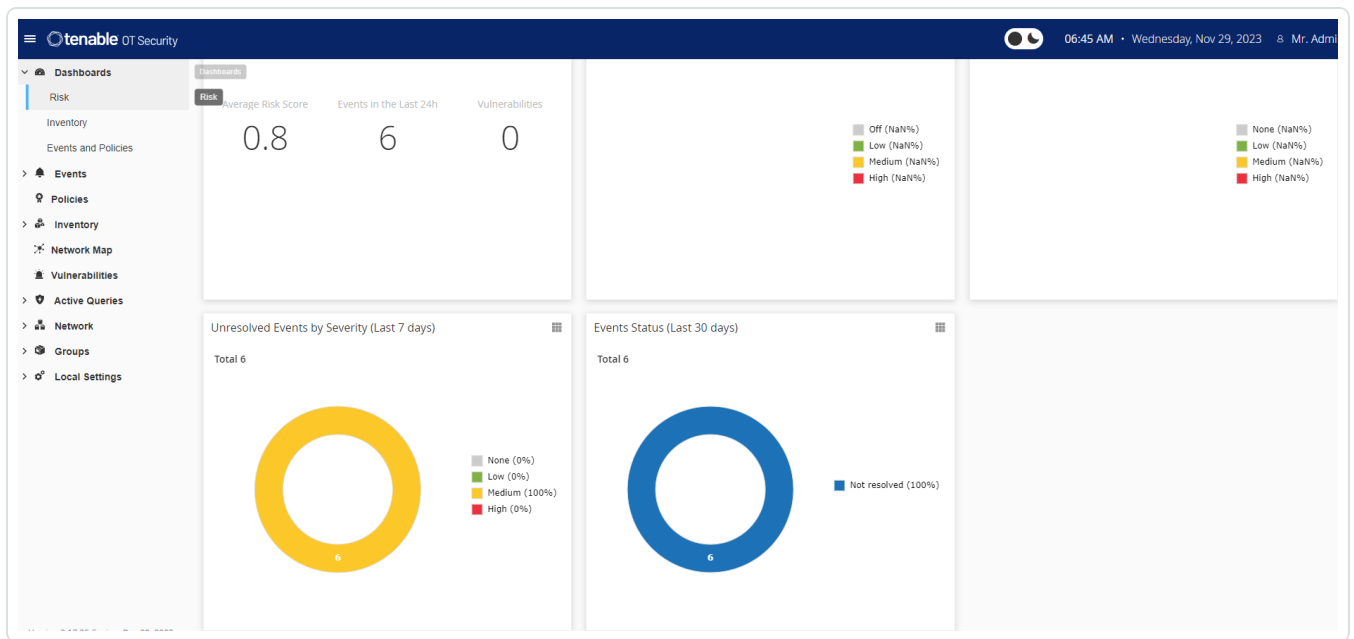
Note: These are ongoing processes that continue over time, so it may take some time for the user interface to display fully updated results.

You can configure and activate additional functions such as Active Queries on the **Local Settings** window in the Management Console (user interface). For more information, see [Active Queries](#).

To enable OT Security:

1. Click **Enable**.

OT Security enables the system and shows the **Dashboard > Risk** window.



Note: It takes a few minutes for the system to identify your assets. You may need to refresh the page to start showing the data.

Start Using OT Security

After installation, you can configure and use OT Security.

Configure Monitored Networks

Configure the network segments for OT Security to monitor and ensure to include all areas pertinent to your network. See [Monitored Networks](#).

Note: Remove unnecessary monitored networks. You can hide any assets you added from those network. For more information, see [Hide Assets](#).

Review and Configure Ports

If you have not yet done so, you can choose to [Separate the Management and Active Query Ports](#).

Configure Users, Groups, and Authentication Servers

Set your [Local Users](#) and [User Groups](#). You can configure External Authentication Servers or utilize SAML for easier SSO login.



Add Network Services

Add your DNS and NTP servers. You can also configure [Syslog](#) and [Email Servers](#) to retrieve all critical events.

Enable Active Queries

Active Queries represent one of the primary benefits of OT Security. They allow you to access your assets directly to obtain the most accurate and near real-time details and visibility. For more information, see [Active Queries](#).

Active Asset Discovery – Proactively probe and discover silent assets or those that passive monitoring traffic do not cover.

Create Nessus Scans

Configure Nessus Scans for IT devices in your OT Security network. Tenable Nessus scans are secure and only impact discovered IT assets. For more information, see [Configure Nessus Plugin Scans](#).

Set Backups

Configure periodic system backups and choose to save them locally or export to a remote storage. For more information, see [Application Data Backup and Restore](#).

Get Updates

Make sure to check feed and system updates. If your system is offline, make sure to do a manual update periodically. For more information, see [Updates](#).

Optimize

When OT Security is up and running, look at the generated events and optimize your policies according to your environment requirements.

Integrate



Integrate OT Security with other Tenable products or third-party services. For more information, [Integrations](#).



Install OT Security Sensor

Note: This section describes the procedure for configuring a sensor version 3.14 and later.

Installation of OT Security sensor involves pairing sensors with the Industrial Core Platform (ICP). To pair sensors with the OT Security ICP, use both the ICP management console and the sensor's Tenable core user interface.

You can either enable automatic approval for incoming pairing requests, or disable automatic approval and allow only manual approval for each new sensor pairing request.

Before you begin

Make sure that the following conditions are met:

- The Sensor hardware is properly installed (see [Set up the Sensor](#)).
- The Sensor is connected to your network switch (see [Connect the Sensor to the Network](#)).
- The Sensor has its own static IPv4 address (see [Access the Sensor Setup Wizard](#)).
- The Sensor is connected to the 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 the [Tenable Core + Tenable OT Security User Guide](#).
- A valid certificate in the ICP console (see [Certificate](#)).

Note: Tenable recommends a dedicated ICP user with administrator role for the process of pairing sensors, to prevent disruptions in connectivity (see [Adding Local Users](#)). You can add a new administrator user to pair multiple sensors.

Note: For information about applying offline updates to your Tenable Core machine, see [Update Tenable Core Offline](#).

Pair the Sensor

To pair a Sensor version 3.14 or later with the ICP:



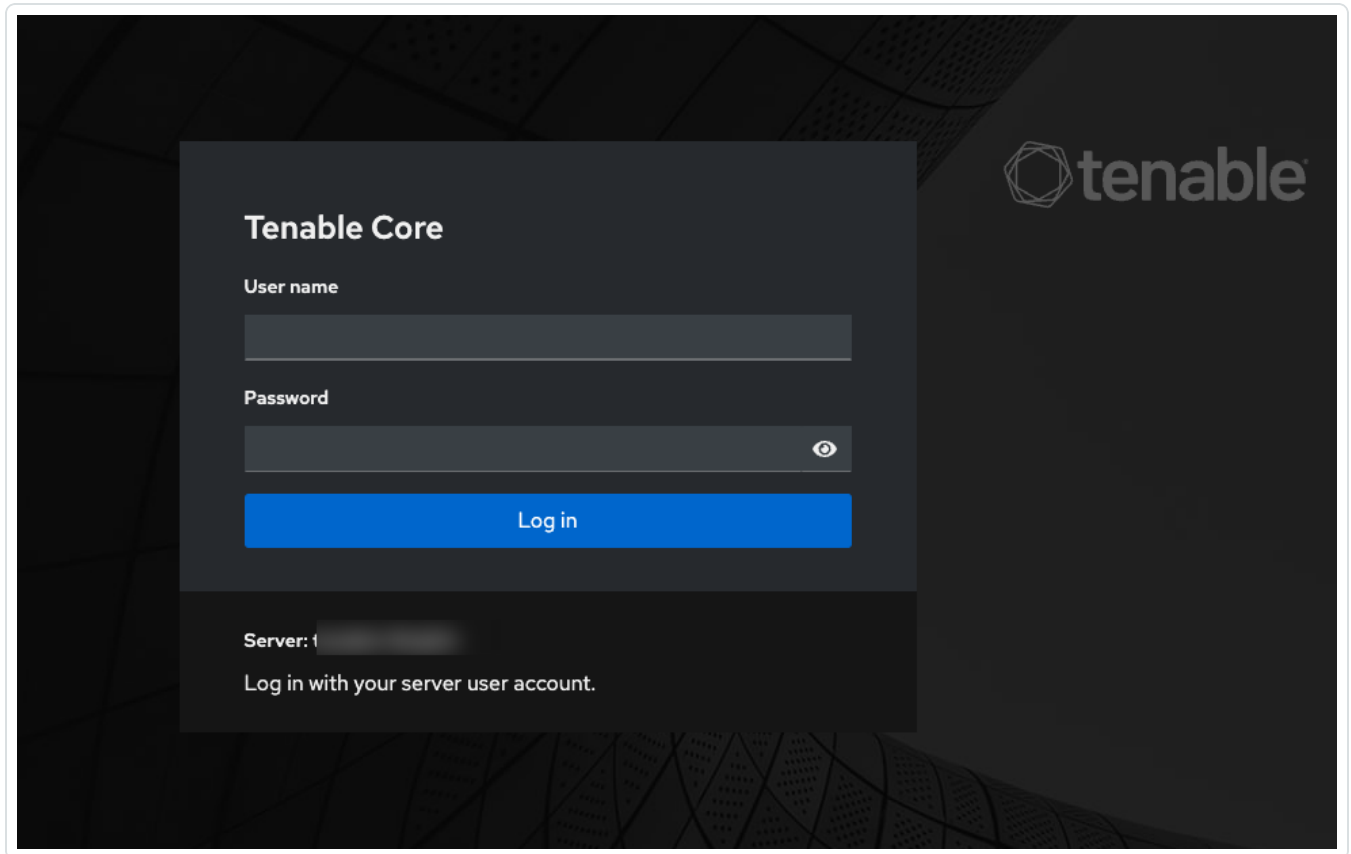
1. In the ICP Management Console (user interface), navigate to the **Local Settings > Sensors** window.



2. To enable automatic approval of Sensor Pairing, ensure that the **Auto Approve Incoming Sensor Pairing Requests** switch at the top of the page is toggled to **ON**. If not, all pairing requests require manual approval.
3. Open a new tab, leaving the ICP tab open, and type **<Sensor IP>:8000** to open the Sensor's Tenable Core user interface.

Note: You can only access the Tenable Core user interface from the latest version of Chrome.

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



Important: If you do not select the **Reuse my password for privileged tasks** upon login, you cannot restart the sensor service.

5. In the navigation menu bar, click **OT Security Sensor**.

The **OT Security Sensor Pair** window appears.



TENABLE.OT SENSOR PAIR

This Tenable.ot Sensor is not currently paired with a Tenable.ot ICP.
Enter the following information to pair it:

* ICP IP Address:

ICP User:

ICP Password:


ICP API Key:

Unauthenticated Pairing

* - Field is required to continue. Username and password OR api key is required to continue.

✘ Error: Either API Key or username and password must be provided.

Pair Sensor Close

Note: The **Tenable OT Security Sensor Pair** window only appears the first time the page loads. To open the window after this, click the  button in the **Pairing Info** section of the **Tenable Core** console.

6. In the **ICP IP Address** box, type the IPv4 address for the ICP to pair with this sensor.
7. To use unauthenticated (unencrypted) pairing, select **Unauthenticated Pairing** and skip to step 8.

Note: Sensors that use **Unauthenticated Pairing** can only passively scan their network segments and the ICP cannot manage them to send Active Queries.

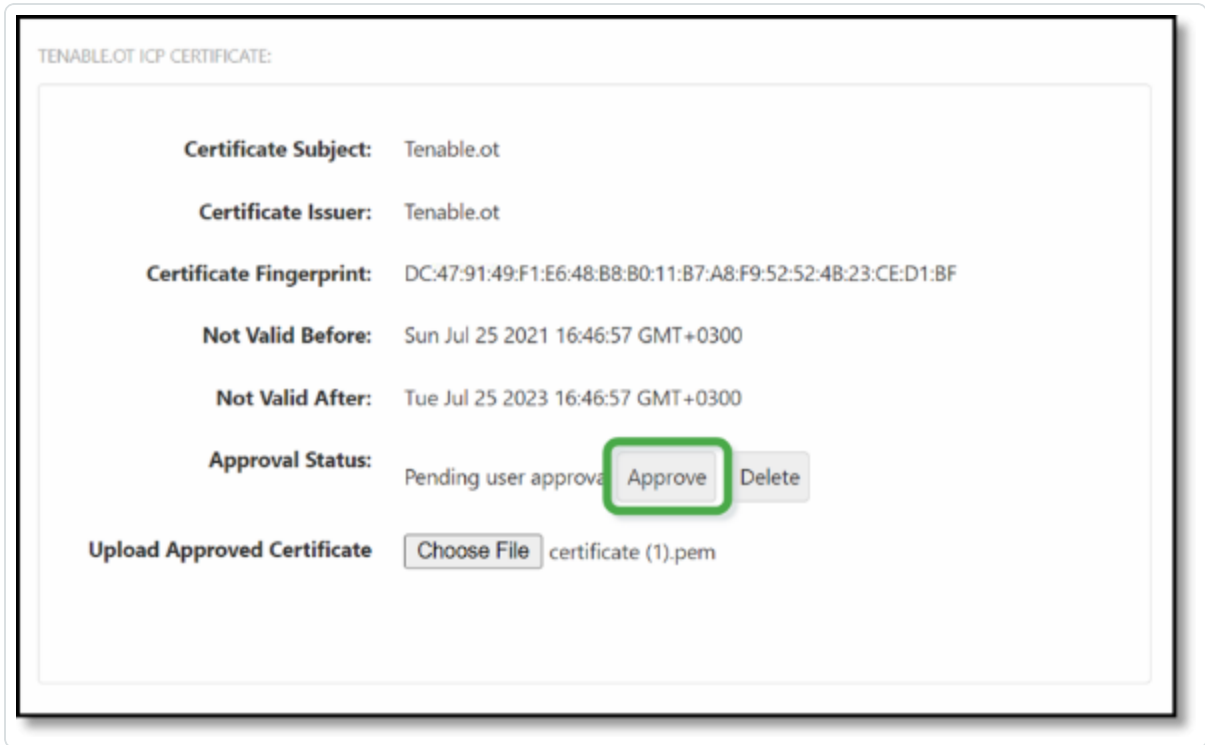
8. To authenticate the pairing, do one of the following:
 - In the **ICP User** box, type the ICP username and the ICP password in the **ICP Password** box.
 - In the **ICP API Key** box, type an API Key for the ICP.

Note: Tenable recommends that you create a dedicated ICP user for pairing sensors in order to ensure connectivity during the pairing process (see [Adding Local Users](#)).

Note: The authentication method that uses username and password offers the advantage of non-expiring credentials unlike an API Key, which eventually ages out.



9. Click **Pair Sensor**.
10. To use a certificate offered from the ICP:
 - a. In **Tenable Core**, in the **Tenable ICP Certificate** section, under **Approval Status**, wait for the certificate information to load.



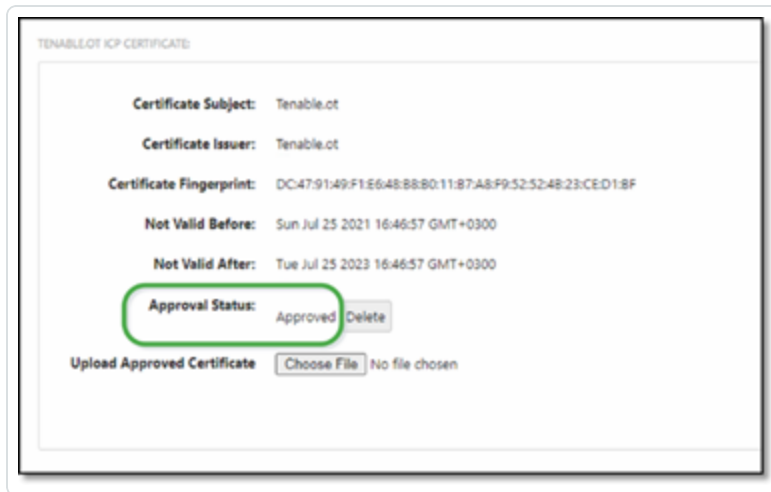
- b. Click **Approve** to approve the certificate.
- c. In the **Confirm Accept Tenable OT Security Server Certificate** window, click **Accept This Certificate**.

If you prefer to upload a certificate manually:

- a. In the **Tenable ICP** console, follow the procedure described in [Generating an HTTPS Certificate](#).
- b. In **Tenable Core**, in the **Tenable ICP Certificate** section, under **Upload Approved Certificate**, click **Choose File**.
- c. Navigate to the .pem certificate file to upload.

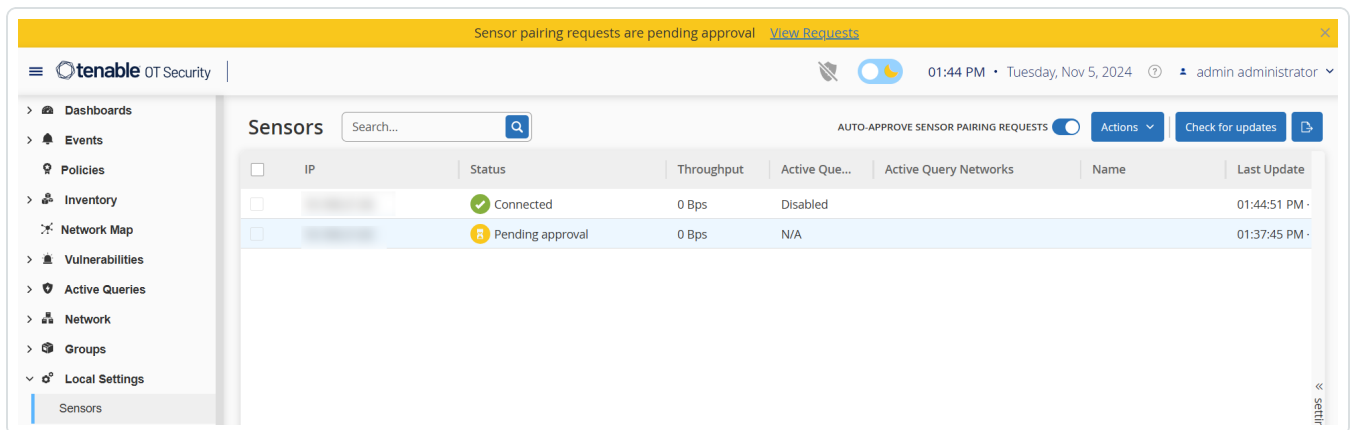


Once a valid certificate loads correctly, its **Approval Status** in the **OT Security ICP Certificate** table shows as **Approved**.

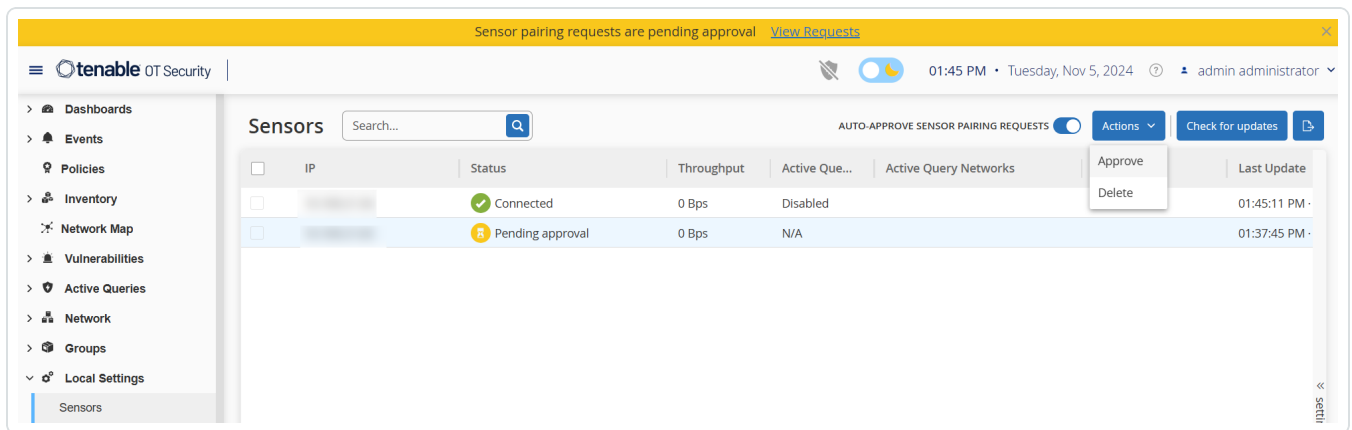


11. In the ICP user interface, navigate to **Local Settings > Sensors**.

OT Security displays the new sensor in the table, and the **Status** shows **Pending Approval**.



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



The **Status** switches to **Connected**, indicating a successful pairing. 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 paused.
- **Disconnected** – The sensor is not connected. For an authenticated sensor, this may result from an error in the pairing process. For example: tunnel error and API issue.
- **Connected (Tunnel error)** – The pairing is successful, but communication over the tunnel is inoperable. Check the connectivity of the port 28304 from the sensor to the ICP. For more information, see [Firewall Considerations](#).

Once OT Security completes the pairing for an Authenticated Sensor, you can configure Active Queries to run on that Sensor. See [Managing Active Queries](#).

Note: Once the pairing completes, Tenable recommends that you use only the ICP page to manage the Sensor, and not the Tenable Core user interface.

Set up the Sensor

There are two models of the Sensor: the Rack Mount Sensor and the Configurable Sensor, as described in [OT Security Sensor Components](#). 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).

Set up a Rack Mount Sensor



You can either mount the sensor on a standard 19-inch rack or place it 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 shown in the following image.



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 supplied rack-mount brackets to the rack frame, using the appropriate screws for rack mounting (not supplied).



Important:

- 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).

Important:

- 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).

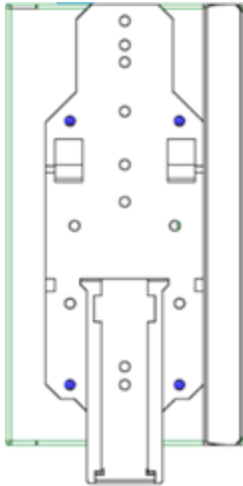
Set up a Configurable Sensor

You can either mount the Configurable Sensor on a DIN rail or on a standard 19-inch mounting rack (using the “mounting ears” adapter kit).

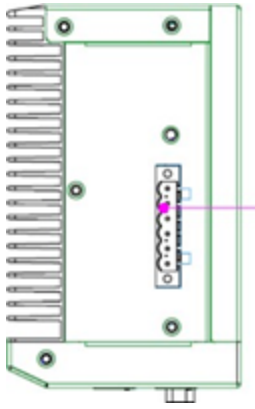
DIN Rail Mounting

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)

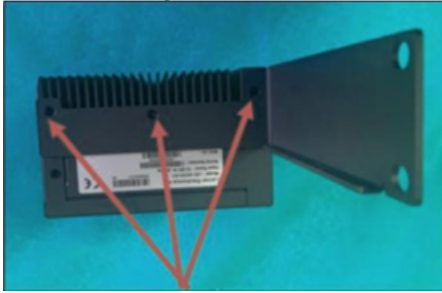
A Configurable Sensor can be attached to a mounting rack, using the “mounting ears” that are provided.

To mount the Configurable Sensor on a standard (19-inch) rack:

1. Prepare the unit for rack mounting:



- 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).

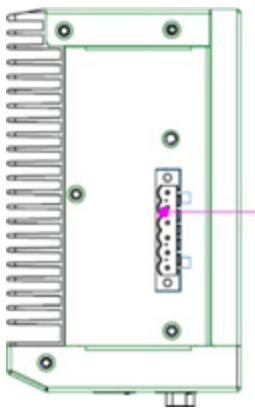


2. Insert the server unit into an available 1U slot in the rack.

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.

Connect 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, connect the unit to a mirroring port on the network switch, which is connected to the controllers/PLCs of interest.

To manage the sensor, connect the unit to a network. This 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.

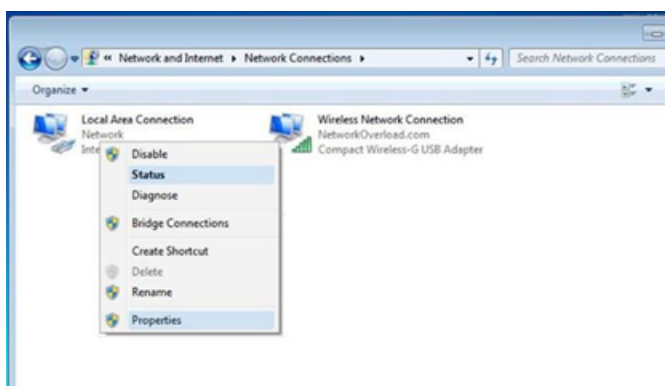
Access the Sensor Setup Wizard

To log in to the Management Console.

1. Do one of the following:
 - Connect the Management Console workstation (for example: PC, laptop, and so on.) directly to Port 1 of the OT Security Sensor using the Ethernet cable.
 - 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.

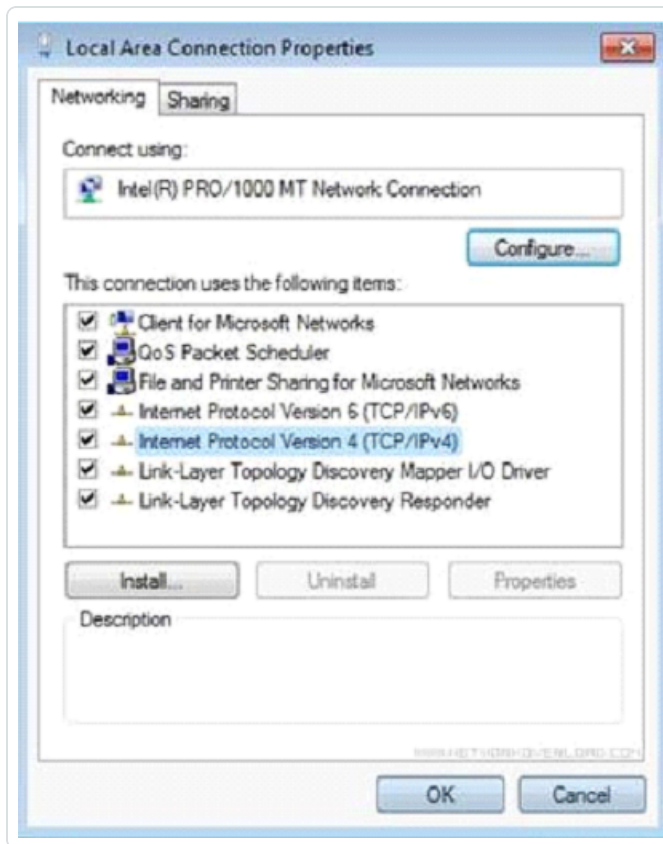
The **Network Connections** window appears.





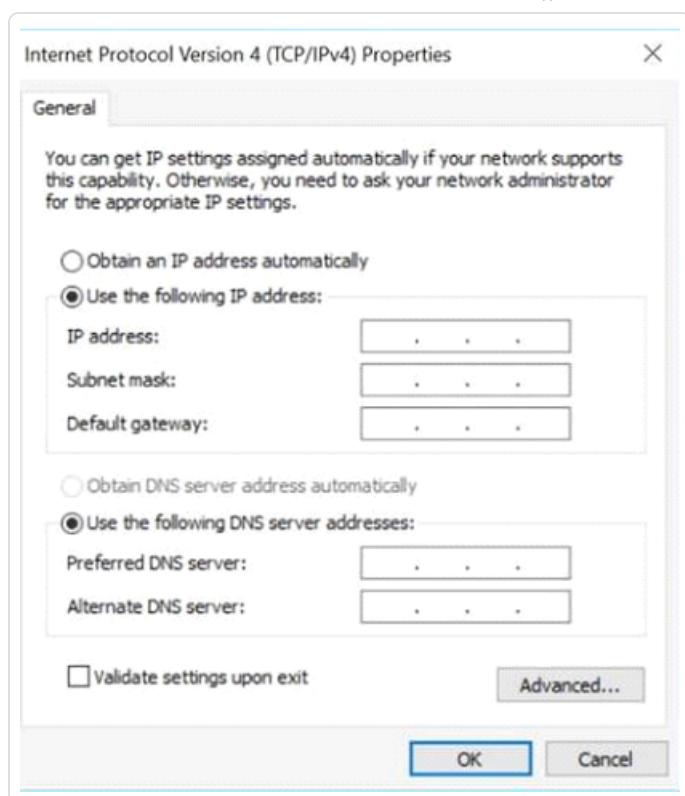
- b. Right-click **Local Area Connections** and select **Properties**.

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 appears.



- d. Select **Use the Following IP address**.
- e. In the IP address box, type **192.168.1.10**.
- f. In the **Subnet mask** box, type 255.255.255.0
- g. Click **OK**.

OT Security applies the new settings.

4. From your Chrome browser, navigate to <https://192.168.1.5:8000>.

Note: The user interface can only be accessed from a Chrome browser. Use the latest version of Chrome.

5. [Pair the sensor](#).

Restore Backup Using CLI

You can restore your OT Security using CLI or via the Tenable Core interface. For more information about restoring backup via Tenable Core user interface, see [Restore a Backup](#) in the Tenable Core + Tenable OT Security User Guide. To restore using CLI, perform the following steps.



Note: You can only restore backups taken using the Tenable Core backup utility. Older backups from OT Security before version 3.18 are not compatible. If you are trying to restore from a backup captured in an older version of OT Security, before version 3.18, contact support for the necessary instructions and commands.

Before you Begin

- Make sure you have the backup `.tar` files to restore.

Note: You can download the OT Security backup files from the **Backup/Restore** page in Tenable Core. For more information, see [Restore a Backup](#) in the Tenable Core + Tenable OT Security User Guide.

Example of an OT Security backup file: `tenable-ot-tenable-s2cc78kg-2024-03-21T135648.tar`.

To restore your OT Security backup using CLI:

1. Do one of the following to access the ICP system:
 - [Log in](#) to Tenable Core and [access](#) the terminal.
 - Log in using SSH.
2. In the terminal, run the following command:

```
sudo systemctl start tenablecore.restorelocal@$(systemd-escape /home/admin/my-tc-ot-backup.tar)
```

Where:

- `/home/admin/my-tc-ot-backup.tar` is the location of the backup files.

Note: The process takes a long time to complete since it restores the backup before the command finishes. You can view the restoration progress from **Backup/Restore > Backup/Restore Logs > Restore** logs in the Tenable Core user interface or by running the following command:

```
journalctl -xf tenablecore.restorelocal@$(systemd-escape /home/admin/my-tc-ot-backup.tar)
```

Where: `/home/admin/my-tc-ot-backup.tar` is the location of the backup files.




OT Security gets restored and you can start accessing the application. To verify that OT Security is running, use your browser to log in to the OT Security user interface via port 443 (HTTPS).

Management Console User Interface Elements

The Management Console user interface provides easy access to important data related to asset management, network activity, and security events that OT Security discovers. You can use the user interface to configure the OT Security platform functionality according to your needs.

Main User Interface Elements

The following table describes the main user interface elements.

User interfaceElement	Description
Main Navigation	Main navigation menu. Click the  icon to show/hide the main navigation menu.
Active Queries	Indicates whether Active Queries is enabled or disabled.
Dark Mode/Daylight Mode	Changes the display color scheme to Dark mode or Daylight mode.
Current Date and Time	Shows the current date and time as registered in the system.
Resource Center	OT Security resource center.
Current User Name	Shows the name of the user who is currently logged into the system. Click the down arrow for a selection menu. Menu options are About (shows software info) and Logout . After activating OT Security, you can view your Tenable customer ID in the About view. This





	customer ID is required when contacting Technical Support or Customer Success teams.
License Info	Shows the OT Security software version and the license expiration date.
Main Screen	Shows the screen that you select in the main navigation.
Export	Downloads a PDF of the dashboard.

Enable or Disable Dark Mode

You can use the **Dark Mode** color scheme on all screens by enabling the Dark Mode toggle.

To enable or disable Dark Mode:

1. Click the  (Dark Mode) toggle at the top of the window.
OT Security applies the selected setting to all screens.
2. To restore the daylight mode setting, click the  (Daylight Mode) toggle.

Check Current Software Version

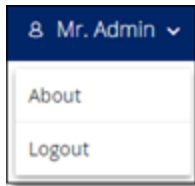
You can check the version your software using the user profile icon in the upper-right corner of the header bar.

To display the current software version:

1. In the main header bar, click the  icon in the upper-right corner to open the menu.



OT Security displays the user menu.



2. Click **About**.

OT Security displays the current software version.



Access Resource Center

The **Resource Center** displays a list of informational resources including product announcements, Tenable blog posts, and user guide documentation.

Note: Access to **Resource Center** requires internet.

To access the Resource Center:

1. In the upper-right corner, click the  button.

The **Resource Center** menu appears.

2. Click a resource link to navigate to that resource. The following resources are available:
 - Search OT Security Knowledge Base
 - New feature updates



Navigate OT Security

You can access the following main pages from the left navigation panel:

- **Dashboards** – Shows widgets containing graphs and tables that give a general view of your network’s inventory and security posture. There are separate dashboards for risk, inventory, events, and policies. See [Dashboards](#).
- **Events** – Shows all events that occurred as a result of Policy violations. A screen shows All Events with separate screens for each specific type of event. For example: Configuration Events, SCADA Events, Network Threats, or Network Events. See [Events](#).
- **Policies** – View, edit, and activate policies in the system. See [Policies](#).
- **Inventory** – Shows an inventory of all the discovered assets, allowing comprehensive asset management, status monitoring of each asset, and viewing their related events. A screen shows All Assets with separate screens for specific type of assets: Controllers and Modules, Network Assets, and IoT. See [Inventory](#).
- **Network Map** – Shows a visual representation of the network assets and their connections.
- **Vulnerabilities** – Shows a detailed list of all the threats in the network that OT Security plugins detected and provides recommended remediation steps. This section includes CVEs as well as other threats to your network assets, such as obsolete operating systems, usage of vulnerable protocols, vulnerable open ports, and so on.
- **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 [Network](#).
OT Security displays this information in three separate windows:
 - **Network Summary** – Shows an overview of network traffic.
 - **Packet Captures** – Shows full-packet captures of network traffic.
 - **Conversations** – Shows a list of all detected network conversations with details about the time of occurrence and involved assets and so on.
- **Groups** – View, create and edit groups used in policy configuration. See [Groups](#).
- **Local Settings** – View and configure the system settings. See [Local Settings](#).

Customize Tables



OT Security pages display data in a table format with a list for each item. These tables have standardized customization features, enabling you to access the relevant information.

Note: The examples given here are for the **All Events** and **All Assets** pages, but similar functionality is available for most of the pages. You can revert to the default display settings at any time by clicking **Settings > Reset table to default**.

Customize the Column Display

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

To specify which columns are displayed:

1. On the right of the table, click **Settings**.

The **Table Settings** panel appears with the **Columns** section.

The screenshot shows the Tenable OT interface. The main content area displays a table titled "All Events" with columns: S... (Status), Log ID, Time, Event Type, Severity, and Policy Name. The table contains several rows of event data. On the right side, a "Table Settings" panel is open, showing a "Columns" section with checkboxes for various columns. The "Reset table to default" button is visible at the bottom of the panel.

S...	Log ID	Time	Event Type	Severity	Policy Name	
<input type="checkbox"/>	Not resol...	1	04:22:14 PM · Oct 29, 2021	Snapshot mismat...	High	Snapshot Mismatch
<input type="checkbox"/>	Not resol...	11	01:52:27 PM · Nov 3, 2021	Change in Key Sw...	High	Change in controller key state
<input type="checkbox"/>	Not resol...	14	04:39:34 PM · Nov 3, 2021	Snapshot mismat...	High	Snapshot Mismatch
<input type="checkbox"/>	Not resol...	23	03:14:33 PM · Nov 10, 2021	Snapshot mismat...	High	Snapshot Mismatch
<input type="checkbox"/>	Not resol...	79	09:57:43 AM · Dec 30, 2021	Snapshot mismat...	High	Snapshot Mismatch
<input type="checkbox"/>	Not resol...	107	11:28:06 AM · Jan 17, 2022	Snapshot mismat...	High	Snapshot Mismatch
<input type="checkbox"/>	Not resol...	108	11:28:33 AM · Jan 17, 2022	Snapshot mismat...	High	Snapshot Mismatch
<input type="checkbox"/>	Not resol...	113	05:29:09 AM · Jan 19, 2022	Snapshot mismat...	High	Snapshot Mismatch
<input type="checkbox"/>	Not resol...	240	09:33:21 AM · Mar 7, 2022	Rockwell Code U...	Low	Rockwell Code Upload
<input type="checkbox"/>	Not resol...	241	09:33:21 AM · Mar 7, 2022	Rockwell Code U...	Low	Rockwell Code Upload
<input type="checkbox"/>	Not resol...	242	09:33:21 AM · Mar 7, 2022	Rockwell Code U...	Low	Rockwell Code Upload
<input type="checkbox"/>	Not resol...	245	09:33:35 AM · Mar 7, 2022	Rockwell Go Online	Low	Rockwell Online Session
<input type="checkbox"/>	Not resol...	246	09:33:36 AM · Mar 7, 2022	Rockwell Go Online	Low	Rockwell Online Session

2. In the **Columns** section, select the checkbox next to the columns you want to show.

3. Clear the checkbox next to the columns you want to hide.



OT Security displays only the selected columns.

4. To close the **Table Settings** window, click **x** or the **Settings** tab.

To adjust the order of display of the columns:

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

Group Lists by Categories

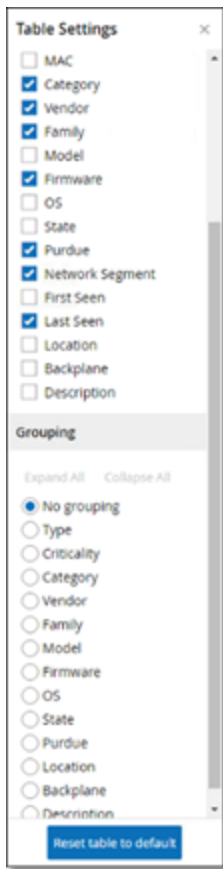
For the **Inventory** pages, you can group the lists by various parameters that are relevant to that particular screen.

To group the lists:

1. Click the **Settings** tab along the right edge of the table.

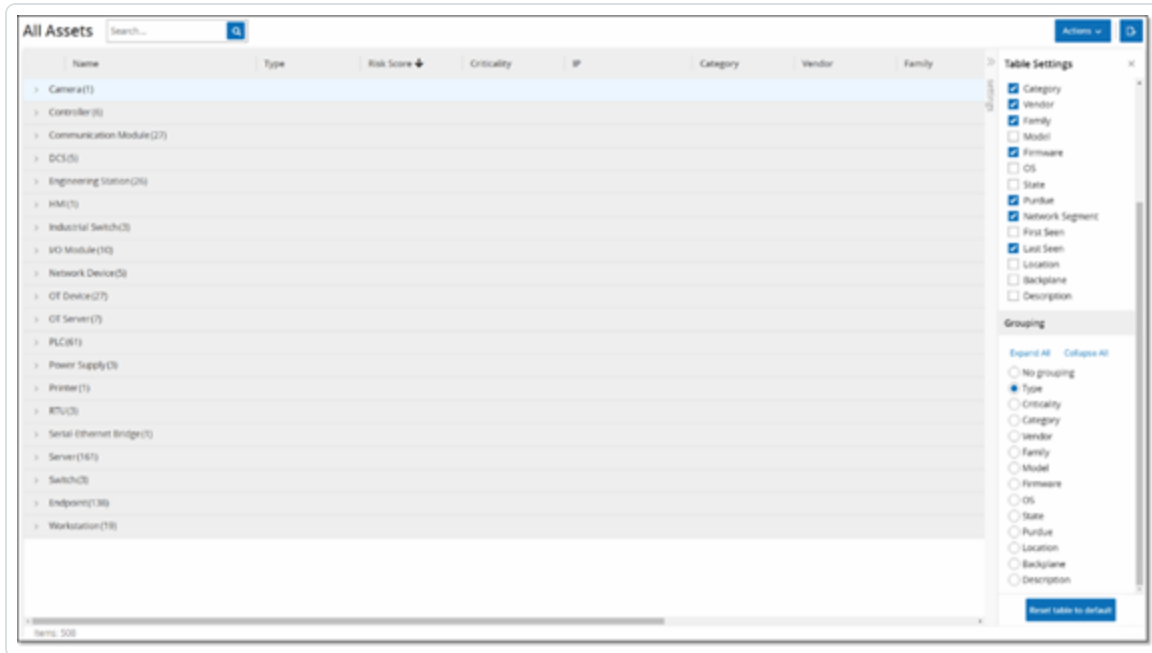
The **Table Settings** pane appears on the right with the **Columns** and **Grouping** sections.

2. Scroll down to the **Grouping** section.

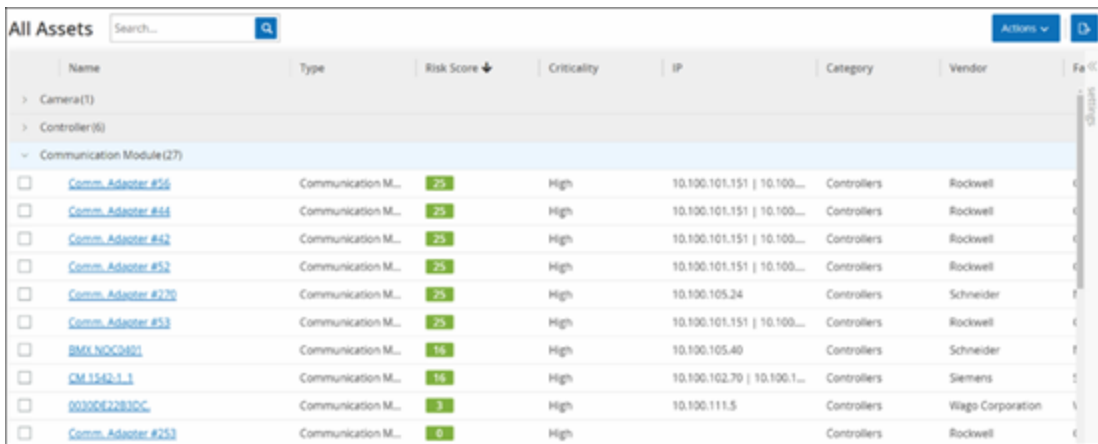




3. Select the parameter by which you want to group the lists. For example, **Type**.
OT Security displays the grouped categories.



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



Sort Columns

Note: This procedure is applicable for all versions.

To sort the lists:



1. Click a column heading to sort the assets by that parameter. For example, click the **Name** heading to display the assets in alphabetical order by Name.
2. Click the column heading a second time if you want to reverse the display order (that is, A→ Z, Z→ A).

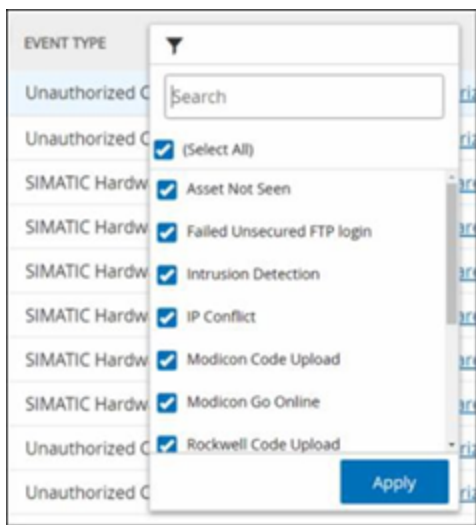
Filter Columns

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, in the **Controllers Inventory** window you can filter by **Name**, **Addresses**, **Type**, **Backplane**, **Vendor**, and so on.

To filter the lists:

1. Hover over a column heading to show the filter icon ▼.
2. Click the filter icon ▼.

A list of filter options appears. The options are specific to each parameter.



3. Select the elements you want to display and clear the checkboxes next to the elements you want to hide.

Note: You can start by clearing the **Select All** checkbox and then selecting the ones you want to show.




4. You can search the list for filters and select or clear them.
5. Click **Apply**.

OT Security filters the lists as specified.

The filter  button next to the column heading indicates that the results are filtered by that parameter.


To remove the filters:

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

Search

On each page, you can search for specific records.

To search the lists:

1. In the **Search** box, type the search text.
2. Click the  button.
3. To clear the search text, click the **x** button.

Export Data

You can export data from any of the lists shown in the OT Security UI (For example: Events, Inventory and so on.) 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 page for which you want to export data.
2. In the header bar, click **Export** .

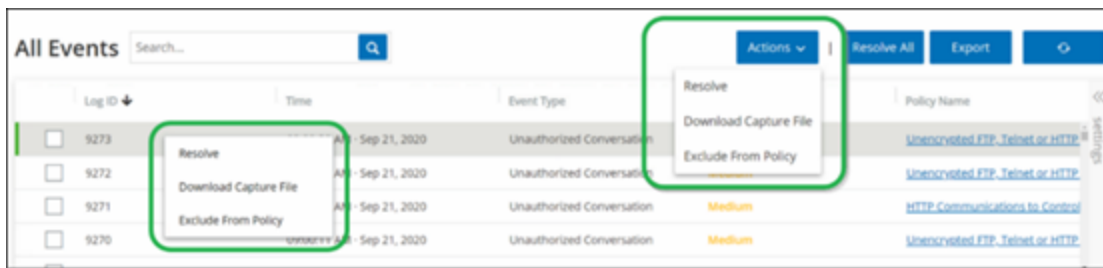
OT Security downloads a CSV format of the data.

Actions Menu

Each screen has a series of actions that you can take for the elements on the screen. For example, in the **Policies** screen, you can **View**, **Edit**, **Duplicate** or **Delete** a Policy; in the **Events** screen, you can **Resolve** or **Download Capture File** for an event and so on.

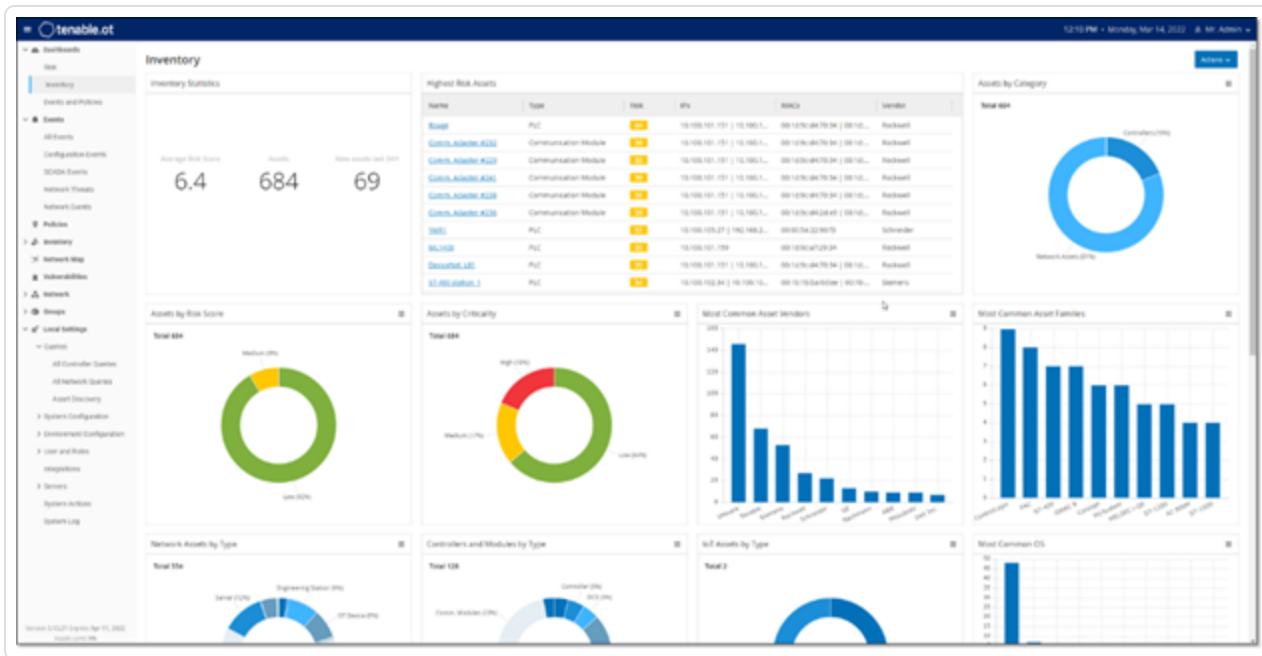
To access the **Actions** menu, do one of the following:

- Select an element, then click **Actions** in the header bar.
- Right-click the element, then select **Actions**.



Dashboards

OT Security provides three dashboards **Risk**, **Inventory**, and **Events and Policies** to give an at-a-glance view of your network's inventory and security posture.



To select a dashboard:

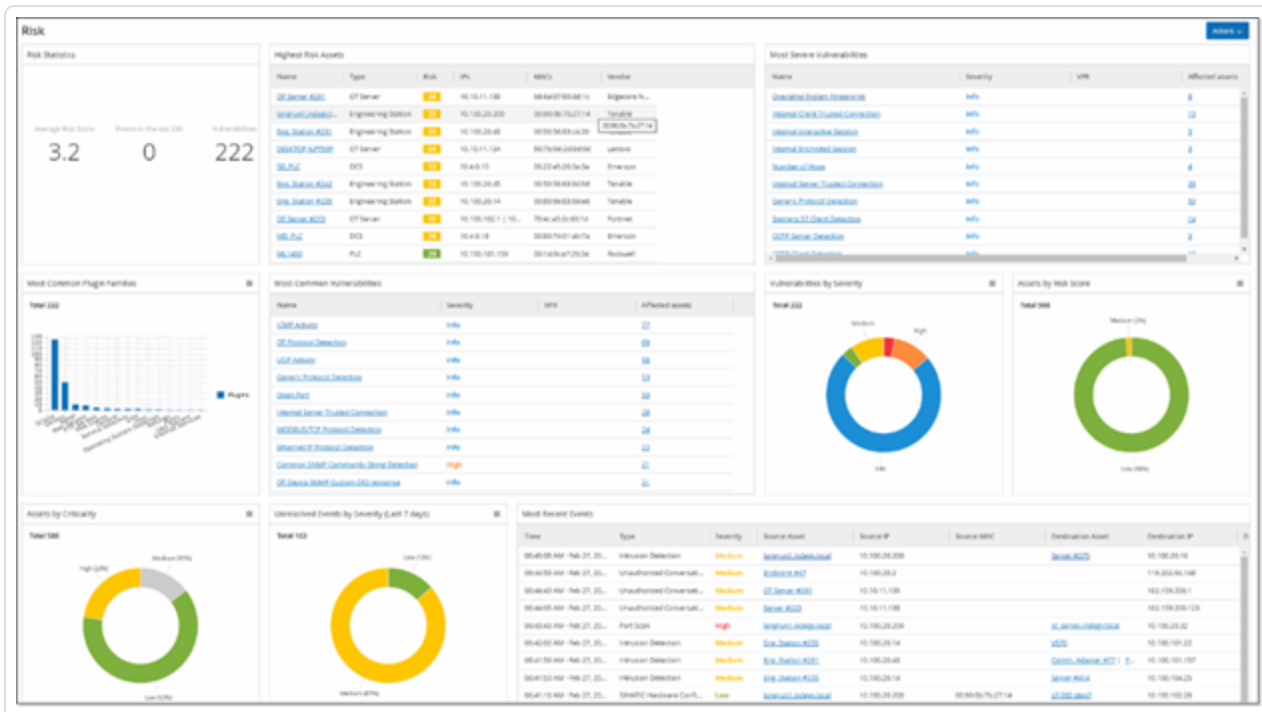
- In the main navigation menu, click **Dashboards**.

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.

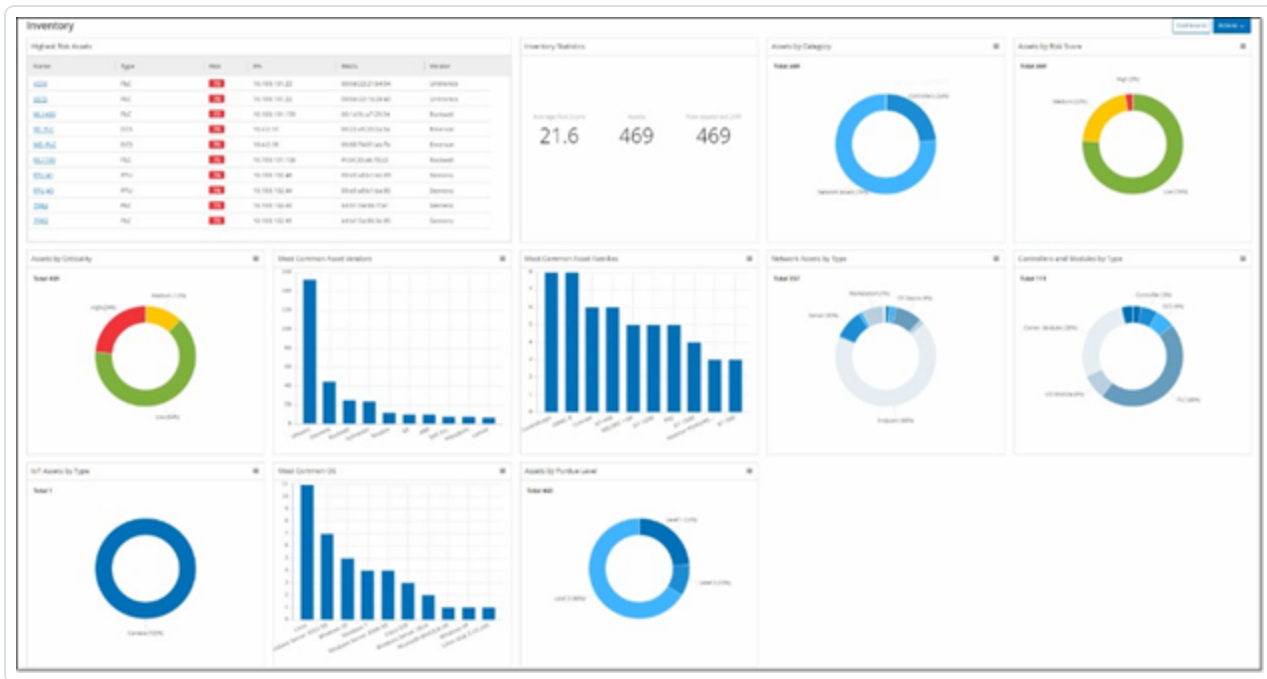


The **Risk** dashboard shows widgets such as: Risk Statistics, Assets by Risk Score, Assets by Criticality, Events by Severity, Most Common Vulnerabilities, and so on.

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

Inventory Dashboard

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

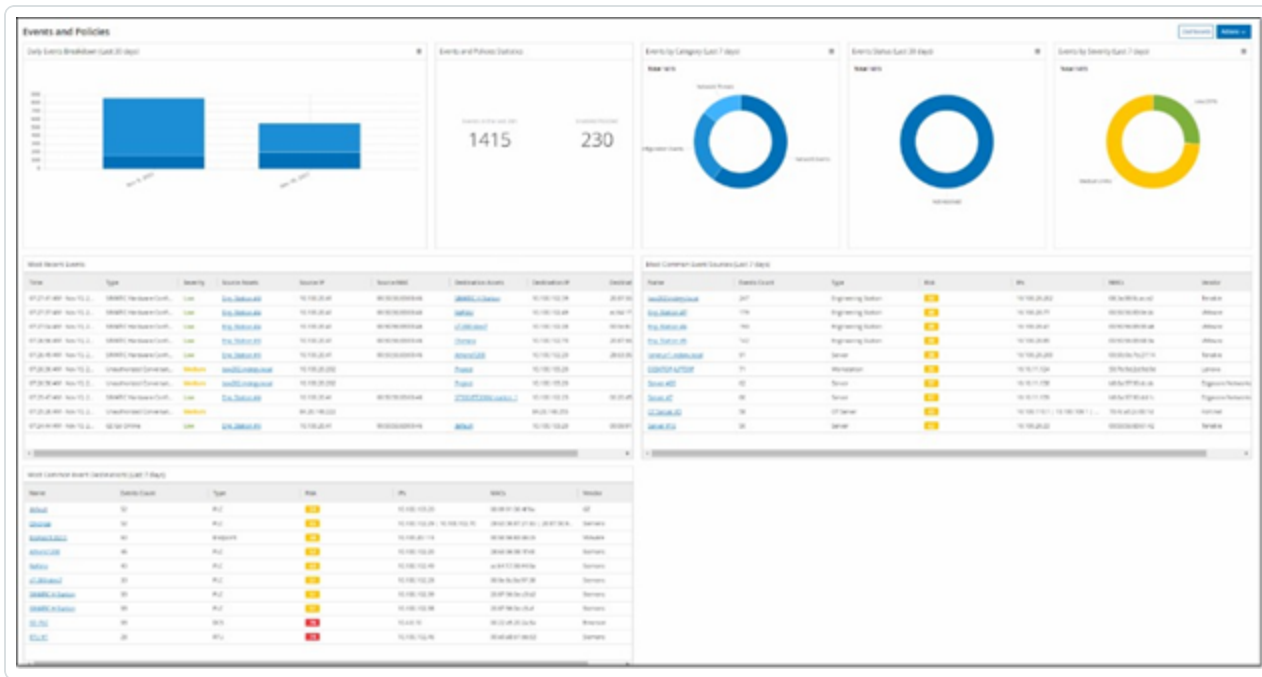


The **Inventory** dashboard shows widgets such as: Highest Risk Assets, Inventory Statistics, Assets by Risk, Controllers, and Modules by Type, Assets by Purdue Level and so on.

Clicking 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 and so on.

Clicking 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, while others allow you to toggle them between modes. Widgets with a  symbol in the upper-right corner appear in graph mode or table mode. Click the table/graph symbol to toggle between modes.

Note: You can only apply filters in table mode.

Graph mode

Graph mode shows a graphic visualization of the widget data.



You can interact with the widgets in the following ways:

- Hover over a point on the graph to display a window with data specific to that segment of the graph.



- When viewing a widget in graph mode, you can download an image of the graph by hovering

over the widget and clicking the  button.

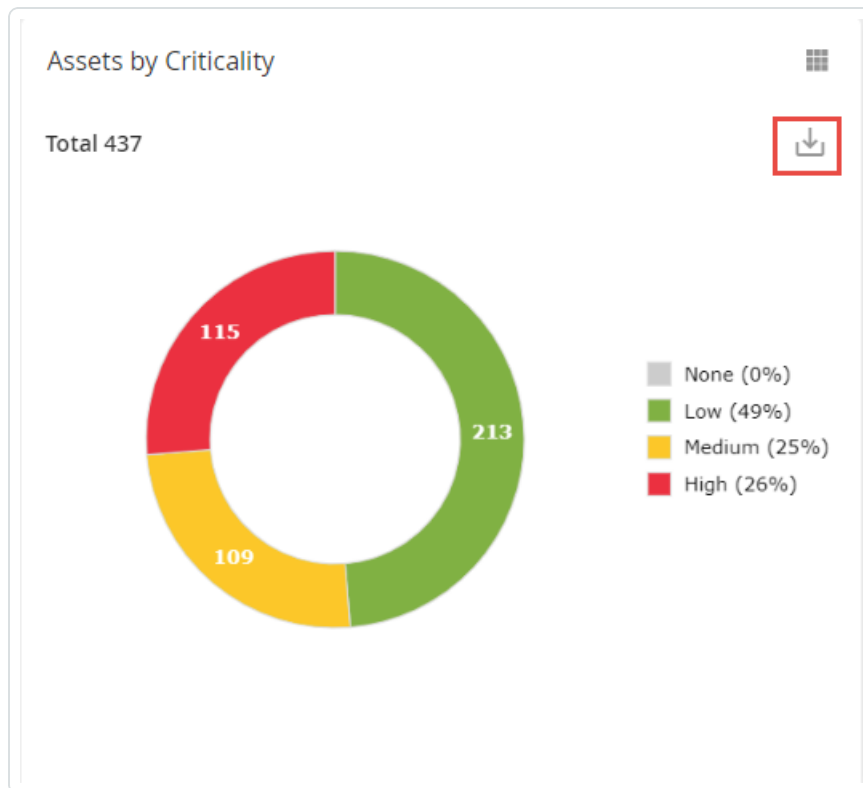
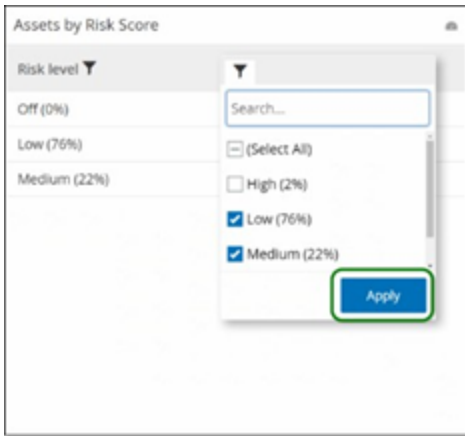


Table mode



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 that you apply in the table mode do not 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 to use as the default view.



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



OT Security updates the default dashboard and shows it the next time you access the Management Console

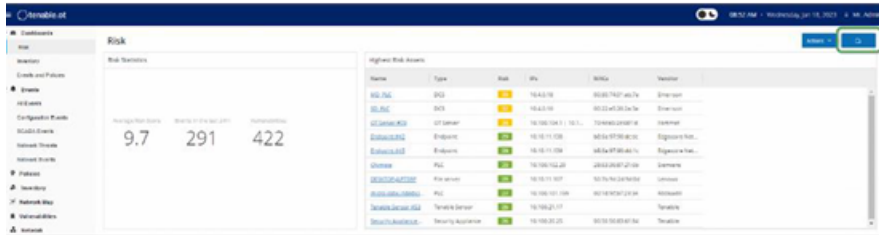
Export the Dashboard



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 upper-right corner of the Dashboard, click **Export**.



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 download completes, navigate to the downloaded file to view or share it.

Compliance Dashboard

Compliance to security frameworks such as NIS 2 Directive, ISO 27001 Controls are now mandatory for most of the critical infrastructure companies to clear audit checks.

Navigating compliance frameworks can be a complex process and require specialized knowledge. Use the **Compliance** dashboard to get a high-level understanding of all assets, vulnerabilities, and events that might affect your organization's critical business operations and also help answer these critical audit questions:

- Which security policies do you have in place to detect suspicious activity?
- How long does it take you to handle an incident?
- Are the alerts integrated with SOC/SIEM as part of your Incident Response (IR) plan?
- How many security events did you have on your critical assets in the last week or month?



The **Compliance** dashboard enables you to align key security measures with regulatory requirements, track your progress and improvements over time, and strengthen your security posture.

Using the dashboard data, you can identify areas where the organization is compliant and improve areas that impact the business from a risk perspective.

tenable OT Security | 09:31 AM • Thursday, Sep 12, 2024 • Mr. Admin

Compliance

[Security Framework Preferences](#)

General

TOTAL ASSETS IN SCOPE	724
FRAMEWORKS IN SCOPE	ISO 27001 Controls, NIS2 Directive (Article 21)

Incident Handling ⓘ

Applies to:

ISO 27001 | Controls: 5.7, 5.25, 5.28, 6.8, 8.7, 8.15, 8.16 ⓘ

NIS2 Directive (Article 21) | measures: b, f, g ⓘ

Abnormal unresolved events by asset criticality

Event Category	Asset Criticality: High	Asset Criticality: Medium	Asset Criticality: Low
Network Events	72	15	6
Network Threats	91	45	20

[Show Asset List](#)

Event Mean Time to Response (MTTR) - Last 30 Days ⓘ

Event Category	Asset Criticality: High	Asset Criticality: Medium	Asset Criticality: Low
----------------	-------------------------	---------------------------	------------------------

Version Mixed Build (Dev)
Expires Dec 29, 2993

To view the compliance dashboard:

1. In the left navigation bar, click **Dashboards > Compliance**.

The **Compliance** dashboard appears.

Note: To configure your security framework preferences, go to **Local Settings > System Configuration > Compliance**. For more information, see [Set Compliance Dashboard Preferences](#).

The dashboard includes the following widgets.

Tip: Hover over the ⓘ icon next to the widget sections for more information about the framework measures that each widget addresses.

Widget

Description



Incident Handling	<p>Provides an overview of the assets at risk by their asset criticality: High, Medium, or Low. You can use this data to respond to high-risk security incidents.</p> <p>Based on the resolution of high-critical events in the last 30 days, OT Security records the Event Mean Time to Respond (MTTR). This value helps you understand the mean time required to respond to each critical event. MTTR is a critical key performance indicator and a shorter MTTR value indicates a more efficient incident resolution process.</p> <p>Note: To view all high-risk assets with suspicious open events, click the Show Asset List link. To close the assets list, click Hide Asset List.</p>
Vulnerability Handling	<p>Provides an overview of all vulnerabilities by their severity and the affected asset types. This widget allows you to identify, assess, report, and remediate OT, network, and IoT vulnerabilities on an ongoing basis.</p> <p>Based on the vulnerabilities fixed in the last 90 days, OT Security records the Mean Time to Respond (MTTR). MTTR and Service Level Agreement (SLA) parameters help understand the mean time required to respond for each critical vulnerability and track the progress of the team in mitigating the vulnerabilities based on the defined SLAs. A shorter MTTR value indicates a more efficient incident resolution process.</p> <p>Note: To view all high-risk assets with active critical vulnerabilities, click Show Asset List. To close the assets list, click Hide Asset List.</p>
Configuration & Change Management	<p>Provides an overview of all assets with unresolved configuration events such as changes made after setting a baseline and critical controller status activities such as the stopping of the device. The data in this widget helps you detect unauthorized modifications and critical events thereby ensuring operational continuity and quick recovery during service disruptions.</p> <p>Note: To view high-risk asset with configuration change events, click the Show Asset List link. To close the assets list, click Hide Asset List.</p>



External Exposure Risk	<p>Provides an overview of external connections to Industrial Control Systems (ICS) networks. You can use the data in this widget to help identify, evaluate, and mitigate OT, network, and IoT assets from unexpected external communication. This data also ensures compliance with supply chain security where ICS equipment and machine builder vendors use hybrid models and move their portal and engineering stations to the cloud, where there is a possibility of external exposure.</p>
Insecure Cryptography	<p>Provides an overview of insecure cryptographic events, such as unsecured logins and unencrypted credentials. This data can help monitor and detect insecure cryptographic events, and in turn prevent the compromise of sensitive information and service disruption.</p> <p>Note: To view all high-risk assets with insecure authentication events, click Show Asset List. To close the assets list, click Hide Asset List.</p>
Insecure Communication Monitoring	<p>Provides an overview of high-risk assets with unsecured communication events and unauthorized access. This data can help avoid any insecure communication and suspicious unauthenticated access that may leave sensitive information or critical assets vulnerable to attackers.</p> <p>Note: To view all high-risk assets with insecure authentication events, click Show Asset List. To close the assets list, click Hide Asset List.</p>
Risk Assessment	<p>Provides an overview of assets at risk by their criticality. This data helps you assess and manage risks associated with OT, network, and IoT assets and proactively identify and mitigate potential threats.</p> <p>Note: To view all assets that are at high risk, click the Show Asset list link. To close the assets list, click Hide Asset List.</p>

Generate an Executive Report

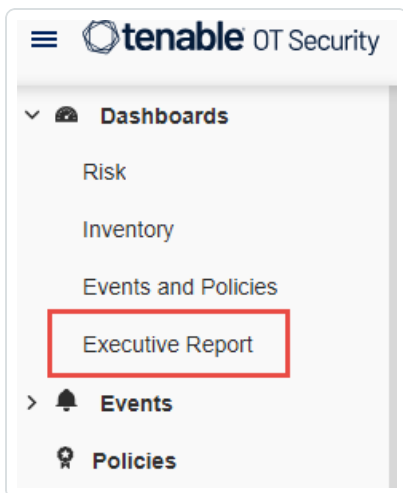


You can generate a risk assessment report for your environment based on the data from the last 30 days. OT Security uses key widgets from the **Risk**, **Inventory**, and **Events and Policies** dashboards to create a high-level graphical overview highlighting high risk assets, critical and common vulnerabilities, common plugin families, and recently discovered assets.

Use the report's charts, such as vulnerabilities by severity, assets by risk score, and assets by criticality, to identify critical assets and the most severe vulnerabilities in your environment over the last 30 days.

To generate a monthly report:

1. In the left navigation bar, go to **Dashboards > Executive Report**.



OT Security opens the report on your browser.

2. To download the report as PDF, click **Save as PDF** at the top of the page.

The **Print** dialog box appears.

3. In the **Destination** drop-down box, select **Save as PDF**.
4. Browse to the location where you want to save the report.
5. Click **Save**.

OT Security saves the report in the PDF format.

Events



Events are notifications generated in the system to call attention to potentially harmful activity in the network. Policies that you set up in the OT Security system generate events in one of the following categories: Configuration Events, SCADA Events, Network Threats, or Network Events. OT Security assigns a severity level to each policy, indicating the severity of the event.

When you activate a policy, any event in the system that fits the policy conditions triggers an event log. Multiple events with the same characteristics are clustered together into a single cluster.

Viewing Events

Status	Log ID	Time	Event Type	Severity	Policy Name	Source Asset	Source Address	Destination Asset	Destination Ad...	Protoc
<input type="checkbox"/>	Not resol...	3306460	06:49:52 AM · Aug 8, 2024	Rockwell Code U...	Low	Rockwell Code Upload	box20.5.indegy.lo...		Praetorian_Gurad	CIP (T
<input type="checkbox"/>	Not resol...	3306459	06:49:50 AM · Aug 8, 2024	Rockwell Code U...	Low	Rockwell Code Upload	box20.5.indegy.lo...		Yuval_L36	CIP (T
<input type="checkbox"/>	Not resol...	3306458	06:49:50 AM · Aug 8, 2024	Rockwell Code U...	Low	Rockwell Code Upload	box20.5.indegy.lo...		Yuval	CIP (T
<input type="checkbox"/>	Not resol...	3306457	06:49:50 AM · Aug 8, 2024	Rockwell Code U...	Low	Rockwell Code Upload	box20.5.indegy.lo...		Yuval	CIP (T
<input type="checkbox"/>	Not resol...	3306462	06:49:49 AM · Aug 8, 2024	Rockwell Code U...	Low	Rockwell Code Upload	box20.5.indegy.lo...		Yuval A10_L71 ...	CIP (T
<input type="checkbox"/>	Not resol...	3306456	06:49:48 AM · Aug 8, 2024	Modicon Code U...	Low	Modicon Code Upload	box20.5.indegy.lo...		Project	Unity
<input type="checkbox"/>	Not resol...	3306455	06:49:47 AM · Aug 8, 2024	Rockwell Code U...	Low	Rockwell Code Upload	box20.5.indegy.lo...		ML1400	PCCC
<input type="checkbox"/>	Not resol...	3306454	06:49:47 AM · Aug 8, 2024	Modicon Code U...	Low	Modicon Code Upload	box20.5.indegy.lo...		HappyNewYear	Unity
<input type="checkbox"/>	Not resol...	3306464	06:49:47 AM · Aug 8, 2024	Rockwell Code U...	Low	Rockwell Code Upload	box20.5.indegy.lo...		Yuval A10_L71 ...	CIP (T
<input type="checkbox"/>	Not resol...	3306453	06:49:46 AM · Aug 8, 2024	Rockwell Code U...	Low	Rockwell Code Upload	box20.5.indegy.lo...		ML1100	PCCC
<input type="checkbox"/>	Not resol...	3306461	06:49:45 AM · Aug 8, 2024	SIMATIC Hardwar...	Low	SIMATIC Hardware Conf...	box20.5.indegy.lo...		SIMATIC H Station	S7 (T
<input type="checkbox"/>	Not resol...	3306451	06:49:44 AM · Aug 8, 2024	Rockwell Code U...	Low	Rockwell Code Upload	box20.5.indegy.lo...		L16ER_APA	CIP (T

Items: 3306432

Event 3306460 06:49:52 AM · Aug 8, 2024 Rockwell Code Upload Low Not resolved

Details Code was uploaded from a controller to an engineering station

Code	SOURCE NAME	
Source	SOURCE IP ADDRESS	
Destination	SOURCE MAC ADDRESS	
Policy	DESTINATION NAME	
Status	DESTINATION IP ADDRESS	
	DESTINATION MAC ADDRESS	
	PROTOCOL	CIP (TCP)

Why is this important?

The system has detected an upload of the controller code that was done via the network. When not part of regular operations, a code upload can be used to gather information on the controller behavior as part of reconnaissance activity.

Suggested Mitigation

- 1) Check whether the upload was done as part of scheduled maintenance work and verify that the source of the operation is approved to perform this operation.
- 2) If this was not part of a planned operation, check the source asset of the event to determine if it has been compromised.

Version 3.19.15 (Dev)
Expires Dec 29, 2993

All events that occurred in the system appear on the **All Events** page. Specific subsets of the events appear on separate windows for each of these event categories: **Configuration Events**, **SCADA Events**, **Network Threats**, and **Network Events**.

For each of the Events pages (Configuration Events, SCADA Events, Network Threats, and Network Events), you can customize the display settings by selecting the columns to display and the position of each column. You can group the events based on Event type, Severity, Policy Name, and so on. You can also sort, filter, and search the event lists. For more information about the customization features, see [Customize Tables](#).

You can use the **Actions** button in the header bar to perform the following actions:



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

The bottom section of the page shows 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
Name	The name of the device in the network. Click the name of the asset to view the Asset Details Screen for that asset, see Inventory .
Addresses	The IP and/or MAC address of the asset. Note: An asset may have multiple IP addresses.
Type	The asset type. See Asset Types for an explanation of the various asset types.
Backplane	The backplane unit that the controller is connected to. Additional details about the backplane configuration are shown in the Asset Details screen.
Slot	For controllers that are on backplanes, shows the number of the slot to which the controller is attached.
Vendor	The asset vendor.
Family	The family name of the product as defined by the controller vendor.
Firmware	The firmware version currently installed on the controller.
Location	The location of the asset, as input by the user in the OT Security asset details. See Inventory .



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



Protocol	When relevant, this shows the protocol used for the conversation that generated this Event.
Event Category	<p>Shows the general category of the Event.</p> <div style="border: 1px solid blue; padding: 5px;"><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></div> <p>The following is a brief explanation of the Event categories (for a more detailed explanation see Policy Categories and Sub-Categories):</p> <ul style="list-style-type: none">• Configuration Events – this includes two sub-categories• Controller Validation Events – These policies detect changes that take place in the controllers in the network.• Controller Activity Events – Activity Policies relate to the Activities that occur in the network (that is, the “commands” implemented between assets in the network).• SCADA Events – policies that identify changes made to the data plane of controllers.• Network Threats Events – these Policies identify network traffic that is indicative of intrusion threats.• Network Events – Policies that relate to the assets in the network and the communication streams between assets.
Status	Shows whether or not the Event has been marked as resolved.
Resolved By	For resolved Events, shows which user marked the Event as resolved.
Resolved On	For resolved Events, shows when the Event was marked as resolved.
Comment	Shows any comments that were added when the Event was resolved.

Viewing Event Details

The bottom of the **Events** page shows additional details about the selected Event. The information is divided into tabs. Only tabs that are relevant for the selected Event are displayed. The detailed



information includes links to additional information about the relevant entities (Source Asset, Destination Asset, Policy, Group, etc.)

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

Viewing Event Clusters

To facilitate the monitoring of events, multiple events with the same characteristics are clustered together into a single cluster. The clustering is based on event type (that is 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.

The screenshot shows the 'All Events' interface. At the top, there is a search bar and buttons for 'Actions', 'Resolve All', and refresh. Below is a table of events with columns: Status, Log ID, Time, Event Type, Severity, Policy Name, Source Asset, and Source Address. The event with Log ID 62952 is selected and expanded. The expanded view shows details for an ARP Scan event, including affected assets (OT Server #5), policy, scanned addresses, and status. It also includes a 'Why is this important?' section explaining that ARP scans are used for network mapping and a 'Suggested Mitigation' section advising to check the source asset for monitoring purposes.

Status	Log ID	Time ↓	Event Type	Severity	Policy Name	Source Asset	Source Address
<input type="checkbox"/>	Not resol...	62947	07:48:59 AM · Nov 11, 2024	SIMATIC Hardwar...	Low	SIMATIC Hardware Confi...	
<input checked="" type="checkbox"/>	Not resol...	62952	07:48:59 AM · Nov 11, 2024	ARP Scan	Medium	ARP Scan Detection	
<input type="checkbox"/>	Not resol...	62944	07:48:57 AM · Nov 11, 2024	SIMATIC Hardwar...	Low	SIMATIC Hardware Confi...	
<input type="checkbox"/>	Not resol...	62949	07:48:55 AM · Nov 11, 2024	SIMATIC Hardwar...	Low	SIMATIC Hardware Confi...	
<input type="checkbox"/>	Not resol...	62943	07:48:53 AM · Nov 11, 2024	Modicon Code U...	Low	Modicon Code Upload	10.100.20.3
<input type="checkbox"/>	Not resol...	62948	07:48:52 AM · Nov 11, 2024	SIMATIC Hardwar...	Low	SIMATIC Hardware Confi...	10.100.20.3
<input type="checkbox"/>	Not resol...	62942	07:48:51 AM · Nov 11, 2024	Rockwell Code U...	Low	Rockwell Code Upload	
<input type="checkbox"/>	Not resol...	62941	07:48:37 AM · Nov 11, 2024	Rockwell Code U...	Low	Rockwell Code Upload	

Items: 63027 Selected Items: 1 Deselect all

Event 62952 07:48:59 AM · Nov 11, 2024 ARP Scan Medium Not resolved

Details
ARP scans are used to map devices in a local network

Affected Assets
SOURCE NAME [OT Server #5](#)

Policy
SOURCE MAC ADDRESS

Scanned Addresses
PROTOCOL ARP

Status

Why is this important?
ARP scans can be used for network mapping. It is important to know what assets are mapping the network and to verify that such mapping is

Suggested Mitigation
Check the source asset to determine whether it is expected to be generating ARP scans for monitoring purposes. If not, contact the source asset

Resolve Events

Once an authorized technician assesses an event and takes the necessary actions to address the problem or determines that there is no action required, then the event can be marked as **Resolved**. When one event that is part of a cluster is resolved, all events in that cluster are marked as resolved. You can select several events and mark them as **Resolved** in a batch process. You can also mark all events (or all events of a particular category) as **Resolved** simultaneously.

Resolve Individual Events

To mark specific events as resolved:

1. In the relevant **Events** page (Configuration Events, SCADA Events, Network Threats, or Network Events), select the check box next to one or more events that you want to mark as **Resolved**.



2. In the header bar, click **Actions**.

A drop-down menu appears.

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

3. Select **Resolve**.

The **Resolve Event** window appears.

The screenshot shows a dialog box titled "Resolve Events (1)". It features a "Comment" label above a large text input field. At the bottom of the dialog, there are two buttons: "Cancel" and "Resolve".

4. (Optional) In the **Comment** box, you can add a comment to describe the mitigation steps to resolve the issues.
5. Click **Resolve**.

The status of the selected event/s is marked as **Resolved**.

Resolve All Events

The **Resolve All** action applies to all events on the current page based on the filters that are currently applied to the display. For example, if the **Configuration Events** page is open, then



Resolve All resolves Configuration Events, but not SCADA Events and so on. For clustered events, all events in the cluster are marked as resolved.

To mark all events as resolved:

1. In the relevant **Events** page (Configuration Events, SCADA Events, Network Threats, or Network Events), click **Resolve All** in the header bar.

The **Resolve All Events** window appears with the number of events to be resolved.



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

3. Click **Resolve**.

OT Security displays a warning message.



4. Click **Resolve**.

OT Security marks all events in the current display as **Resolved**.

Create Policy Exclusions

If a policy generates events for specific conditions that do not pose a security threat, you can exclude those conditions from the policy (that is, 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.

You can create exclusions from the **Events** page, based on events generated by your policies. You can specify which conditions of a particular event you want to exclude from the policy.

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** page, (Configuration Events, SCADA Events, Network Threats, or Network Events), select the event for which you want to create an exclusion.
2. In the header bar, click **Actions** or right-click the event).

The **Actions** menu appears.

3. Click **Exclude from Policy**.

The **Exclude from Policy** window opens.

4. In the **Exclude Condition** section, by default all conditions are selected.

This causes events with any of the specified conditions to be excluded from the policy. You can deselect the check box next to each condition for which you want to continue generating events.

Note: For example, in the following window, to exclude the specified source and destination assets and IPs from this policy, but 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 the following table.

- (Optional) In the **Exclusion Description** box, you can add a comment about the exclusion.
- Click **Exclude**.

OT Security creates the exclusion.

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

Policy Category	Event Type	Excludable Conditions
Controller Activities	Configuration Events (Activities)	<ul style="list-style-type: none">• Source asset• Source IP• Destination asset• Destination IP
Controller	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
Network	Asset Not Seen	Source asset
	Change in USB Configuration	<ul style="list-style-type: none">• Source asset• USB Device ID
	IP Conflict	<ul style="list-style-type: none">• MAC Addresses• IP Address
	Network Baseline Deviation	<ul style="list-style-type: none">• Source asset• Source IP• Destination asset• Destination IP• Protocol
	Open Port	<ul style="list-style-type: none">• Source asset• Source IP• Port
	RDP Connection	<ul style="list-style-type: none">• Source asset• Source IP• Destination asset



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



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



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

Download 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 (for example, Wireshark, and so on). 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**, 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.



Download a PCAP File

To download a PCAP file:

1. In the **Events** page, select the check box next to the event for which you want to download the PCAP file.
2. In the header bar, click **Actions**.

The **Actions** menu appears.

3. Select **Download Capture File**.

The zipped PCAP file is downloaded to your local machine.

Create 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 is set to automatically apply to the source and destination assets involved in the OT Security Event. By default, the policy causes FortiGate to deny (that is block) traffic of the specified type. A FortiGate administrator can adjust the policy settings in the FortiGate application.

Before you 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** page (Configuration Events, SCADA Events, Network Threats, or Network Events), select the event for which you want to create a FortiGate policy.
2. In the header bar, click **Actions** or right-click the event.

A drop-down menu appears.

3. 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** drop-down box, select the required server.

The screenshot shows a dialog box titled "Create Policy on FortiGate". It has a close button (X) in the top right corner. The dialog contains three input fields: "SOURCE ADDRESS:", "DESTINATION ADDRESS:", and "FORTIGATE SERVER: *". The "FORTIGATE SERVER" field is a dropdown menu with two options: "FortiGate1" and "fortigateSTAS". At the bottom, there are two buttons: "Cancel" and "Create".

5. Click **Create**.

The policy is created in FortiGate and the panel closes. You can view the new policy in the FortiGate application. A FortiGate administrator can adjust the settings as needed.

Policies

OT Security includes policies that define specific types of events that are suspicious, unauthorized, anomalous, or otherwise noteworthy that occur in the network. When an event occurs that meets all of the Policy Definition conditions for a particular policy, the system generates an event. The system logs the event and sends notifications in accordance with the Policy Actions configured for the policy.

- **Policy-based Detection** – Triggers an event when the precise conditions of the policy, as defined by a series of event descriptors, are met.
- **Anomaly Detection** – Triggers an event when OT Security detects anomalous or suspicious activity in the network.

OT Security features a set of predefined policies (out-of-the-box). In addition, you can edit the predefined policies or define new custom policies.



Note: By default, most policies are turned on. To turn Policies on/off, see [Enable or Disable 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 triggers 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 policy parameter belongs to a group as opposed to individual entities. This 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 (for example, 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.

Policy configuration uses the following types of groups:

- **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, and so on.
- **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 having similar communication patterns.
- **Email Groups** – Group multiple email accounts that receive email notifications for specific events. For example, grouping by role, department, and so on.
- **Port Groups** – Group ports used in a similar manner. For example, ports that are open on Rockwell controllers.
- **Protocol Groups** – Group communication protocols by the type of protocol (for example, Modbus), the manufacturer (for example, Rockwell allowed protocols), and so on.



- **Schedule Groups** – Group several time ranges as a schedule group that has a certain common characteristic. For example, work hours, weekends, and so on.
- **Tag Groups** – Group tags that contain similar operational data in various controllers. For example, tags that control furnace temperature.
- **Rule Groups** – Group-related rules 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 configured in your system. The system comes with a set of predefined groups. You can edit these groups and add your own groups, see [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 that indicates the degree of risk posed by the situation that triggered the event. The following table describes the various severity levels:

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. The **Events** section shows **All Events**. The **Policy** page lists the event under the policy that triggered the event and the **Inventory** page lists the event under the affected Asset. In addition, you can configure policies to send notification of events to an external SIEM using the Syslog protocol and/or to designated email recipients.



- **Syslog Notification** – Syslog messages use the CEF protocol with both Standard Keys and Custom Keys (configured for use with OT Security). For an explanation of how to interpret Syslog notifications see the [OT Security Syslog Integration Guide](#).
- **Email Notifications** – Email messages include details about the event that generated the notification and the steps to mitigate the threat.

Policy Categories and Sub-Categories

OT Security organizes the policies by the following categories:

- **Configuration Events** – These policies relate to the activities that occur in the network. There are two sub-categories:
 - **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 (for example, firmware upgrade during a work day), and/or specific controllers.
 - **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 block lists and allowlists of assets, activities, and schedules are supported.
- **Network Events** – These policies relate to the assets in the network and the communication streams between assets. This includes assets added to or removed from the network. It also includes traffic patterns that are anomalous for the network or 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 (for example, protocols used by controllers manufactured by a specific vendor), the policy triggers an event. You can limit these policies to specific schedules and/or specific assets. Vendors organize vendor-specific protocols 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 cataloged in Suricata's Threats engine.

Policy Types

Within each category and sub-category, there are a series of different types of policies. OT Security includes the 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. For example, the “commands” implemented between assets in the network. There are many different types of Controller Activity Events. The type of controller on which the activity occurs and the specific activity defines the Controller Activity type. For example, Rockwell PLC stop, SIMATIC code download, Modicon online session, and so on.

The policy definition parameters or 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 to the controller state by adjusting the physical key position. Currently supports Rockwell controllers only.
Change in state	Affected Asset,	The controller changed from one operational state to another. For example, running, stopped, test, and so on.



	Schedule	
Change in firmware version	Affected Asset, Schedule	A change to the firmware running on the controller.
Module not seen	Affected Asset, Schedule	Detects a previously identified module that removed from a backplane.
New module discovered	Affected Asset, Schedule	Detects a new module 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
Asset not seen	Not seen for, Affected Asset, Schedule	Detects previously identified assets in the Affected Asset Group that are removed from the network for the specified duration of time during the specified time range.
Rediscovered Asset	Inactive for, Affected Assets, Schedule	Detects an asset that comes online or begins communicating again after being offline for a period of time.



Change in USB configuration	Affected Assets, Schedule	Detects when a USB device is connected to or removed from a Windows-based workstation. The policy applies to changes to an asset in the Affected Asset Group during the specified time range.
IP conflict	Schedule	Detects multiple assets in the network using the same IP Address. This may indicate a cyber-attack or it may result from poor network management. The policy applies to IP Conflicts that OT Security discovers during the specified time range.
Network Baseline Deviation	Source, Destination, Protocol, Schedule	Detects new connections between assets that did not communicate with each other during the Network Baseline sampling. This option is only available once a Network Baseline is set up in the system. To set the initial Network Baseline or to update the Network Baseline, see Setting a Network Baseline . The policy applies to communication from an asset in the Source Asset Group to an asset in the Destination Asset Group using a Protocol from the Protocol Group during the specified time range.
New asset discovered	Affected Asset, Schedule	Detects new assets of the type specified in the Source Asset Group that appears in your network during the specified time range.
Open port	Affected Asset, Port	Detects new open ports in your network. Unused open ports can pose a security risk. The policy applies to assets in the Affected Asset Group and to ports that are in the Port Group.
Spike in network traffic	Time window, Sensitivity level, Schedule	Detects anomalous spikes in the network traffic volume. The policy applies to spikes relative to the specified time window and based on the specified sensitivity level. It is also limited to the specified time range.



Spike in conversation	Time window, Sensitivity level, Schedule	Detects anomalous spikes in the number of conversations in the network. The policy applies to spikes relative to the specified time window and based on the specified sensitivity level. It is also limited to the specified time range.
RDP connection (authenticated)	Source, Destination, Schedule	An RDP (Remote Desktop Connection) was made in the network using authentication credentials. The Policy applies to asset in the Source Asset Group connecting to an asset in the Destination Asset Group during the specified time range.
RDP connection (not authenticated)	Source, Destination, Schedule	An RDP (Remote Desktop Connection) made in the network without using authentication credentials. The policy applies to asset in the Source Asset Group connecting to an asset in the Destination Asset Group during the specified time range.
Unauthorized conversation	Source, Destination, Protocol, Schedule	Detects communication sent between assets in the network. The policy applies to communication sent from an asset in the Source Asset Group to an asset in the Destination Asset Group using a Protocol from the Protocol Group during the specified time range.
Successful unsecured FTP login	Source, Destination, Schedule	OT Security considers FTP as an unsecure protocol. This policy detects successful logins using FTP.
Failed unsecured FTP login	Source, Destination, Schedule	OT Security considers FTP as an unsecure protocol. This policy detects failed login attempts using FTP.
Successful unsecured Telnet login	Source, Destination, Schedule	OT Security considers Telnet as an unsecure protocol. This policy detects successful logins using Telnet.
Failed unsecured	Source,	OT Security considers Telnet as an unsecure



Telnet login	Destination, Schedule	protocol. This policy detects failed login attempts using Telnet.
Unsecured Telnet login attempt	Source, Destination, Schedule	OT Security considers Telnet as an unsecure protocol. This policy detects login attempts using Telnet (for which the result status is 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 are cataloged in Suricata's Threats engine. The rules are grouped into categories (for example, ICS Attacks, Denial of Service, Malware, and so on.) and sub-categories (for example, ICS Attacks - Stuxnet, ICS Attacks - Black Energy, and so on). The system comes with a series of predefined groups of related rules. You can also configure your own custom groupings of various rules. Note: You cannot edit the Source and Destination asset groups for Intrusion Detection System (IDS) events.
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 in the Affected Asset Group during the specified time range.
Port scan	Source Asset,	Detects SYN scans (network reconnaissance activity) that



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



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

Enable or Disable Policies



You can enable or disable any configured policy in your system (both pre-configured and user-defined). You can turn on/off individual policies or you can select multiple policies to turn on/off in a bulk process.

Note: Most of the policies depend on queries to collect data. If some or all of the query functions are disabled, then the related policies are not effective. You can activate queries from **Active Queries**, see [Active Queries](#).

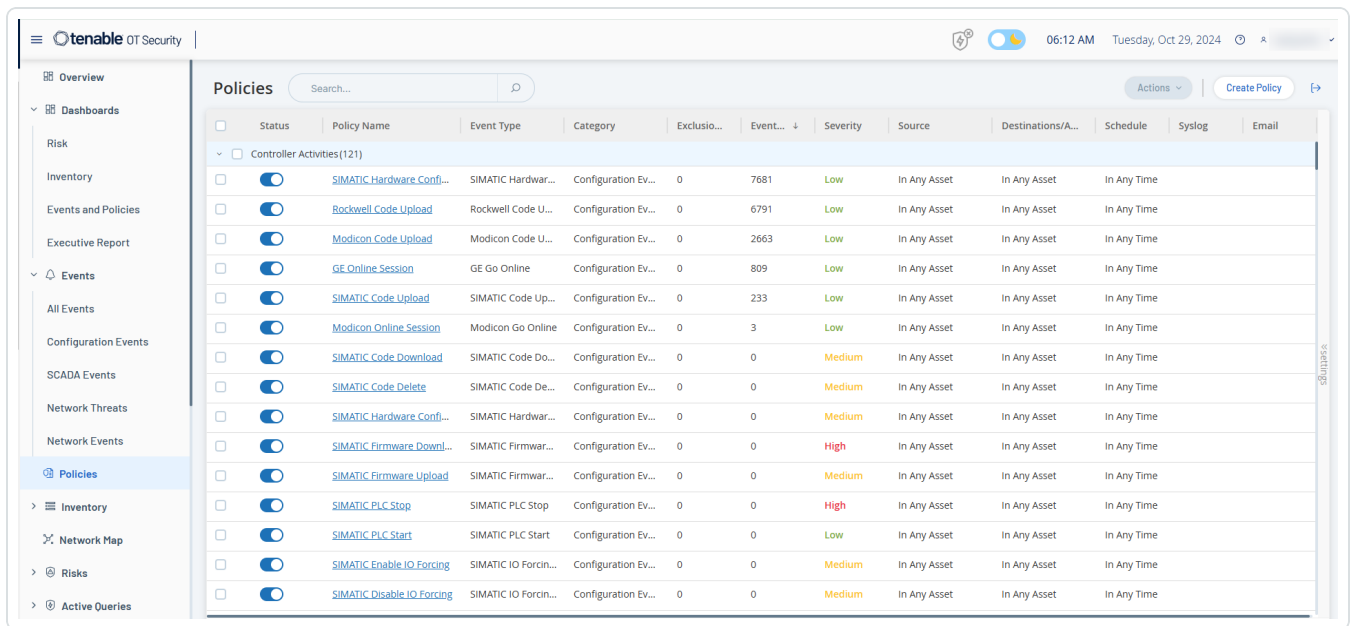
To enable or disable a policy:

1. Go to **Policies**.

The page lists all policies configured in the system, grouped by Policy Category.

The screenshot shows the 'Policies' management interface. At the top, there is a search bar and buttons for 'Actions', 'Create Policy', and 'Export'. The table below lists policies grouped into two categories: 'Controller Activities (105)' and 'Network Events (54)'. Each policy row includes a status toggle, name, severity level, event type, and category.

Status	Name	Severity	Event Type	Category
Controller Activities (105)				
Controller Validation (8)				
<input checked="" type="checkbox"/>	Snapshot Mismatch	High	Snapshot mismatch	Configuration Events
<input checked="" type="checkbox"/>	Change in controller firmware version	High	Change in Firmware Version	Configuration Events
<input checked="" type="checkbox"/>	Change in controller state	Medium	Change in State	Configuration Events
<input checked="" 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
Network Events (54)				
<input checked="" type="checkbox"/>	Asset Not Seen for 1 Hour	Low	Asset Not Seen	Network Events
<input checked="" 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

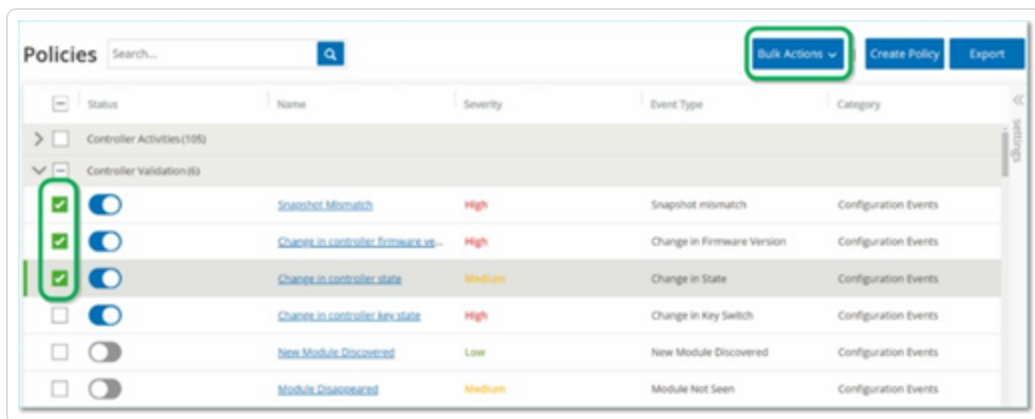


2. To enable or disable the policy, click the **Status** toggle next to the relevant policy.

To enable or disable multiple policies:

1. Go to **Policies**.

The page lists all policies configured in the system, grouped by Policy Category.



2. Select the checkbox next for each of the policies you want to enable or disable. 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. From the **Bulk Actions** drop-down box, select the desired action (**Enable** or **Disable**).

OT Security enables or disables the selected policies.

View Policies

The **Policies** screen lists all configured policies in your system. The lists are grouped for each Policy Category in separate tabs. The page lists both pre-configured policies and user-defined policies. Each policy includes a toggle that shows 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 search for keywords. For information about customizing the list, see [Management Console User Interface Elements](#).

The following table describes the policy parameters:

Parameter	Description
Status	Shows if the policy is turned on or off. If the system automatically disabled a policy because it generated too many events, then a warning icon appears next to the toggle. Toggle the status switch to turn a Policy ON/OFF.
Policy ID	A unique identifier for the policy in the system. Policy IDs are grouped by category, with a different prefix for each category. For example, P1 for Controller Activities, P2 for Network Events, and so on.
Name	The name of the policy.
Severity	The degree of severity of the event. Possible values are: None, Low, Medium, or High. See section Severity Levels for a description of the severity levels.
Event Type	The specific type of event that triggers this Event Policy.
Category	The general category of the event type that triggers this Event Policy.



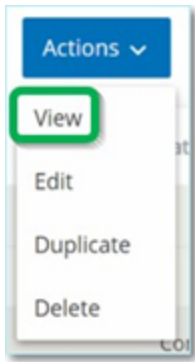
	Possible values are: Configuration, SCADA, Network Threats, or Network Event. For more information about the various categories, see Policy Categories and Sub-Categories .
Source	A policy condition. The source Asset Group/Network Segment (that is, the asset that initiated the Activity) to which the policy applies.
Destination/ Affected Asset	A policy condition. The destination Asset Group/Network Segment (that is the asset that receives the Activity) to which the policy applies. For policies that involve a single asset (no source and destination), this parameter shows the asset affected by the event.
Schedule	A policy condition. The time range for which the policy applies.
Syslog	The Syslog server (SIEM) that logs the events for this policy.
Email	The Email Group that sends the event notifications for this policy.
Sub Category	The sub-category classification of the event. The Configuration Events category comprises these sub-categories: Controller Activities and Controller Validation. For information about different sub-categories, see View Policies .
Number of Events per Policy	Lists the number of events that every policy generates. You can click the column to sort the list so that you can focus on the policies with the most violations/events.
Exclusions	Lists the number of exclusions added to each policy. For more information, see Events .

View Policy Details

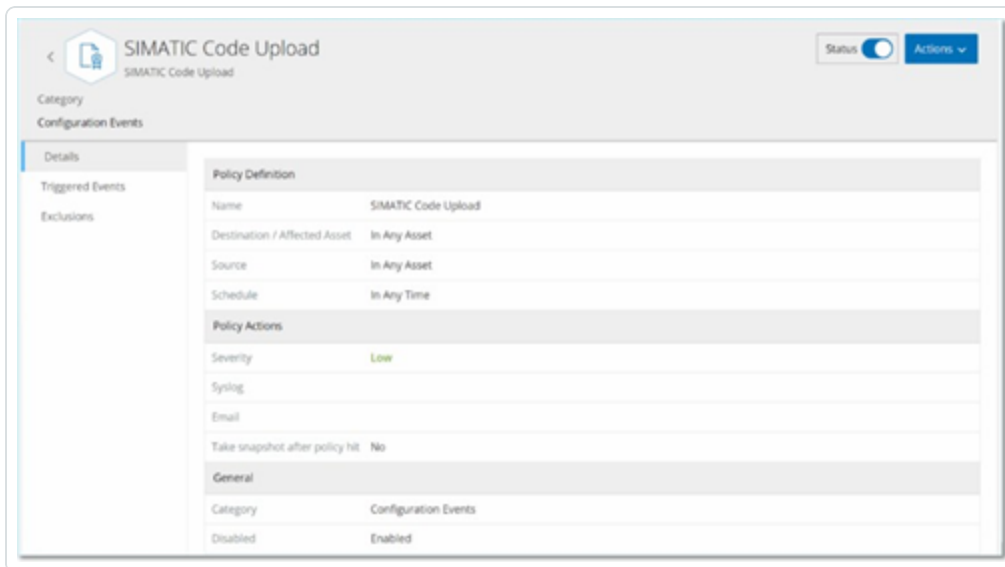
The **Policy Details** page for a policy shows additional details about the policy. This page lists all policy conditions and events that the policy triggered.

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

1. On the **Policies** page, select the desired policy.
2. From the **Actions** drop-down box, select **View**.



The Policy Details page appears for the selected policy.



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

The Policy Details page contains the following elements:

- **Header bar** – Shows the Name, Type, and Category of the policy. The page includes a toggle switch to turn the enable or disable the policy and a drop-down list of available **Actions (Edit, Duplicate, and Delete)**.
- **Details tab** – Shows details about the policy configuration in these sections:
 - **Policy Definition** – Shows all policy conditions. This includes all relevant fields according to the policy type.



- **Policy Actions** – Shows the severity level as well as destination (Syslog, Email) of Event notifications. Also, shows whether the **Take Scapshot after policy hit** feature is activated.
- **General** – Shows the category and status of the policy.
- **Triggered Events** – Shows a list of events triggered by this policy. It also shows details about the assets involved in the event and the nature of the event. The information on this tab is identical to the information on the **Events** page except that this tab shows only events for the specified policy. For an explanation of the event information, see [Viewing Events](#).

Exclusions tab – If a policy generates events for specific conditions that do not pose a security threat, you can exclude those conditions from the policy (that is, stop generating events for those particular conditions). You can add exclusions on the **Events** page, see [Events](#). The **Exclusions** tab shows all exclusions applied to this Policy and for each exclusion, it shows the specific excluded conditions. From this tab, you can also delete an exclusion thereby enabling the system to resume generating events for the specified conditions.

Create Policies

You can create custom policies based on the specific considerations of your ICS network. You can determine precisely what type of events must 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 want to give to each policy.

Note: Policies are defined by using groups configured in your system. If the drop-down list for a certain parameter doesn't show the specific grouping to which you want 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 allowlist or block list the specified Group.

- select **In** to allowlist the specified Group (that is, include it in the Policy), OR
- select **Not in** to block list the specified Group (that is, leave it out of the Policy).

For Asset Group and Network Segment parameters (that is, 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.

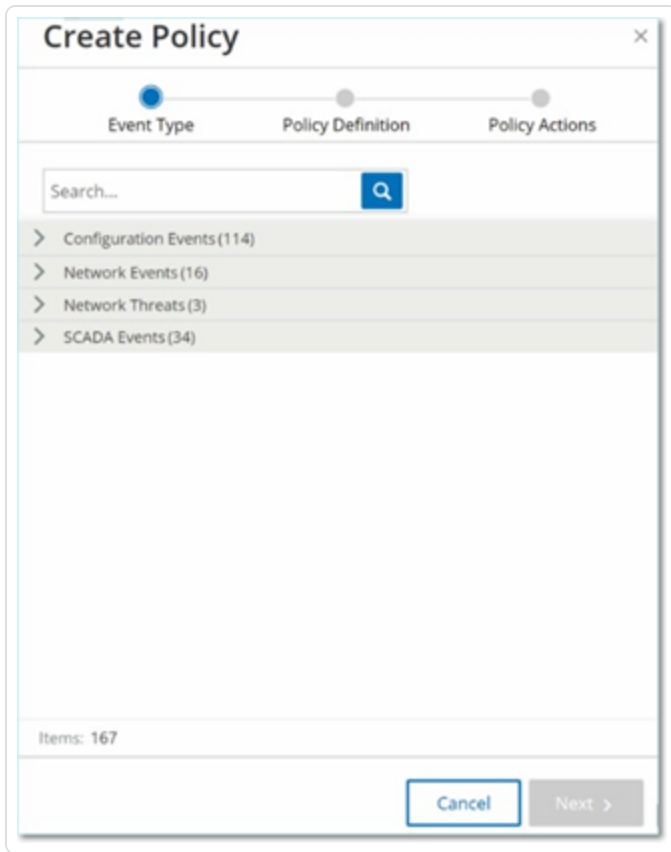
If you would like to create a new Policy with similar parameters to an existing Policy, you can Duplicate the original Policy and make the necessary changes, see section [Create Policies](#).

Note: After creating a Policy, if 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:

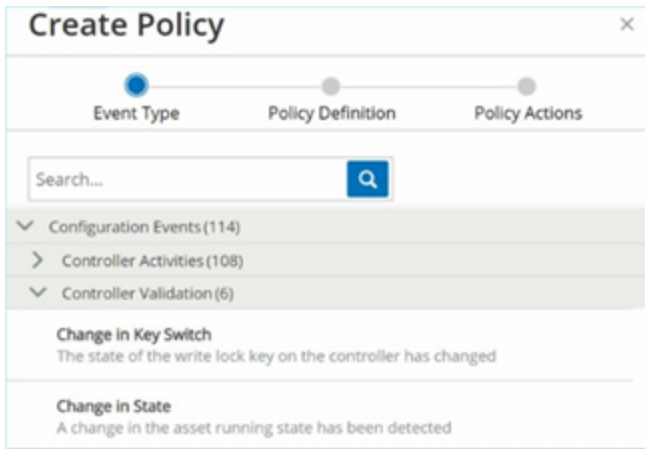
1. On the **Policies** screen, click **Create Policy**.

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.

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:

Important: You cannot edit the **Source** and **Destination** asset groups for Intrusion Detection System (IDS) events.



- a. Where relevant, select **In** (default) to allowlist the selected element or Not in to block list the selected element.
- b. Click **Select**.

A drop-down list of relevant elements (for example 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 (that is Source, Destination and Affected Assets), if you want 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 (that is Source, Destination and Affected Assets), if you want 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. Click **Next**.

A series of Policy Action parameters (that is the actions taken by the system when a Policy hit occurs) are shown.

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

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 drop-down 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. Click **Create**. The new Policy is created and automatically activated. The Policy is shown in the list on the Policies screen.

Create 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 [Create Policies](#).

The screenshot shows the 'Create Policy' dialog box with the 'Policy Definition' step selected. The event type is 'Unauthorized write'. The form includes the following fields and options:

- Policy name ***: A text input field.
- Source ***: A dropdown menu with 'In' selected, followed by a 'Select' dropdown, and a '+ Or' button.
- Tag group ***: A dropdown menu with 'Select' selected.
- Tag value ***: Three radio button options: 'Any value' (selected), 'Different from value' (with a '0' input field), and 'Out of allowed range' (with '0' and '0' input fields).
- Buttons**: '< Back', 'Cancel', and 'Next >'.



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 (for example Integer, Boolean etc.) but not for customized tags or strings.

4. Complete the Policy creation procedures as described in [Create Policies](#).

Other Actions on Policies

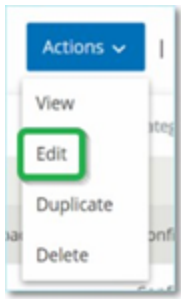
Edit Policies

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.

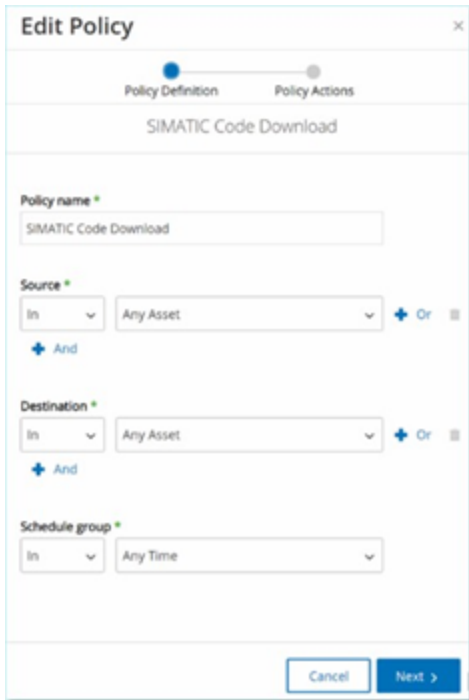
You can also edit the **Policy Action** parameters for multiple policies in a bulk action.

To edit a policy:

1. On the **Policies** window, select the checkbox next to the required policy.
2. In the **Actions** drop-down box, select **Edit**.



3. The **Edit Policy** window appears with the current configuration.



4. Adjust the **Policy Definition** parameters as needed.

Note: You cannot edit the **Source** and **Destination** asset groups for Intrusion Detection System (IDS) events.

5. Click **Next**.

6. Adjust the **Policy Actions** parameters as needed.

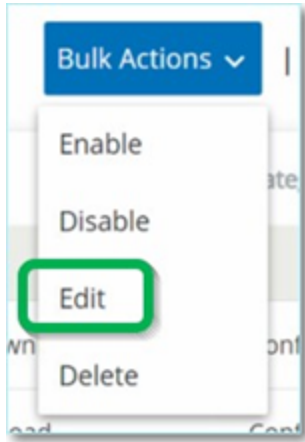
7. Click **Save**.

OT Security saves the policy with the new configuration.

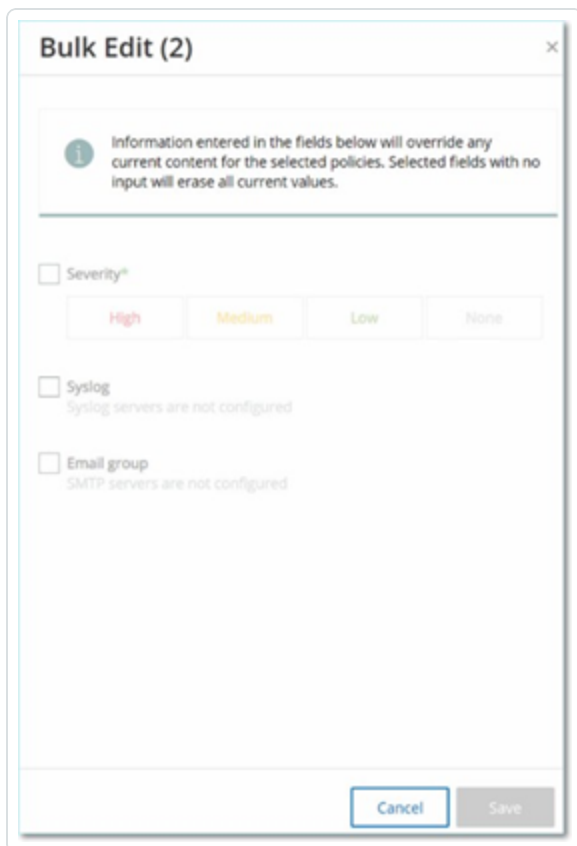
To edit multiple policies (bulk process):



1. On the **Policies** window, select the checkbox next to two or more policies.
2. In the **Bulk Actions** drop-down box, select **Edit**.



3. The **Bulk Edit** window appears with the Policy Actions available for bulk editing.





4. Select the checkbox next to each of the parameters that you want to edit: **Severity**, **Syslog**, and **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

High Medium Low None

Syslog
Syslog servers are not configured

Email group
SMTP servers are not configured

5. Set each parameter as needed.

Note: Information entered in the **Bulk Edit** window 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 are erased.

6. Click **Save**.

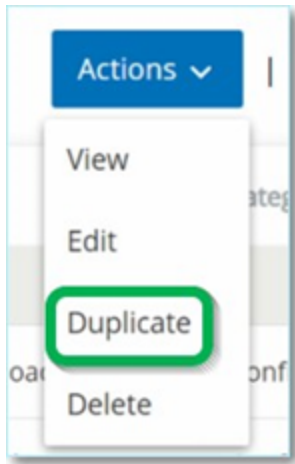
OT Security saves the policies with the new configuration.

Duplicate Policies

You can create a new policy that is similar to an existing policy by duplicating the original policy and making the required adjustments. You can duplicate both predefined and user-defined policies (except for **Intrusion Detection Policies**).

To duplicate a policy:

1. On the **Policies** window, select the checkbox next to the required policy.
2. In the **Actions** drop-down box, select **Duplicate**.



3. The **Duplicate Policy** window appears with the current configuration and the name is set to the default "Copy of <Original Policy Name>".

Duplicate Policy [X]

Policy Definition Policy Actions

SIMATIC Code Delete

Policy name *
Copy of SIMATIC Code Delete

Source *
In Any Asset + Or

+ And

Destination *
In Any Asset + Or

+ And

Schedule group *
In Any Time

Cancel Next >

4. Adjust the **Policy Definition** parameters as needed.
5. Click **Next**.
6. Adjust the **Policy Actions** parameters as needed.
7. Click **Save**.

OT Security saves the policy with the new configuration.

Delete Policies



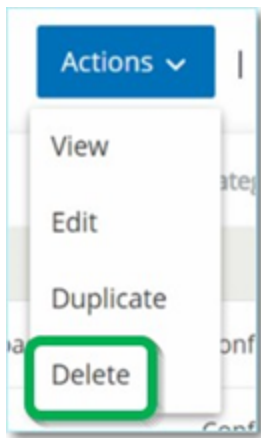
You can delete a policy from the system. You can delete both predefined and user-defined policies (except for **Intrusion Detection Policies**, which can't be deleted).

You can also delete multiple policies in a bulk action.

Note: Once you delete a policy from the system you cannot 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** window, select the checkbox next to the required policy.
2. In the **Actions** drop-down box, select **Delete**.

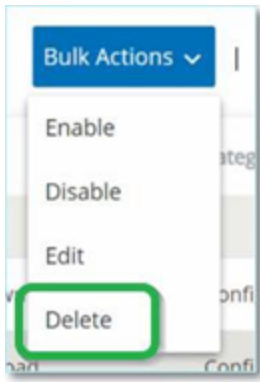


A confirmation window appears.

3. Click **Delete**.
- OT Security deletes the policy from the system.

To delete multiple policies (bulk action):

1. On the **Policies** window, select the checkbox next to each of the required policies.
2. In the **Bulk Actions** drop-down box, select **Delete**.



A confirmation window appears.

3. Click **Delete**.

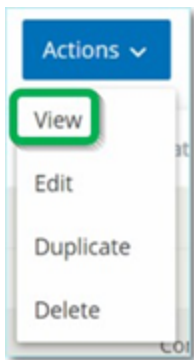
OT Security deletes the policies from the system.

Delete Policy Exclusions

If you want to delete an exclusion that has been applied to a particular policy, you can do so on the **Policies** window.

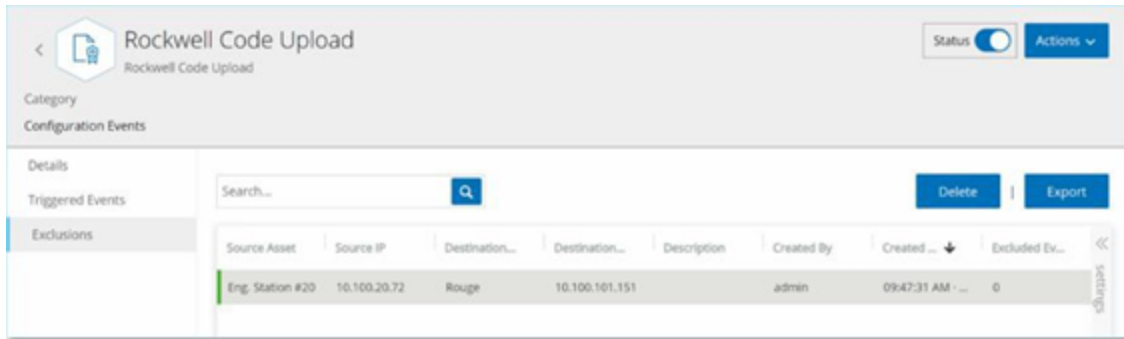
To delete a Policy Exclusion:

1. On the **Policies** window, select the required policy.
2. In the **Actions** drop-down box, select **View**.



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

3. Click the **Exclusions** tab.



A list of exclusions appears.

4. Select the policy exclusion you want to delete.
5. Click **Delete**.

A confirmation window appears.

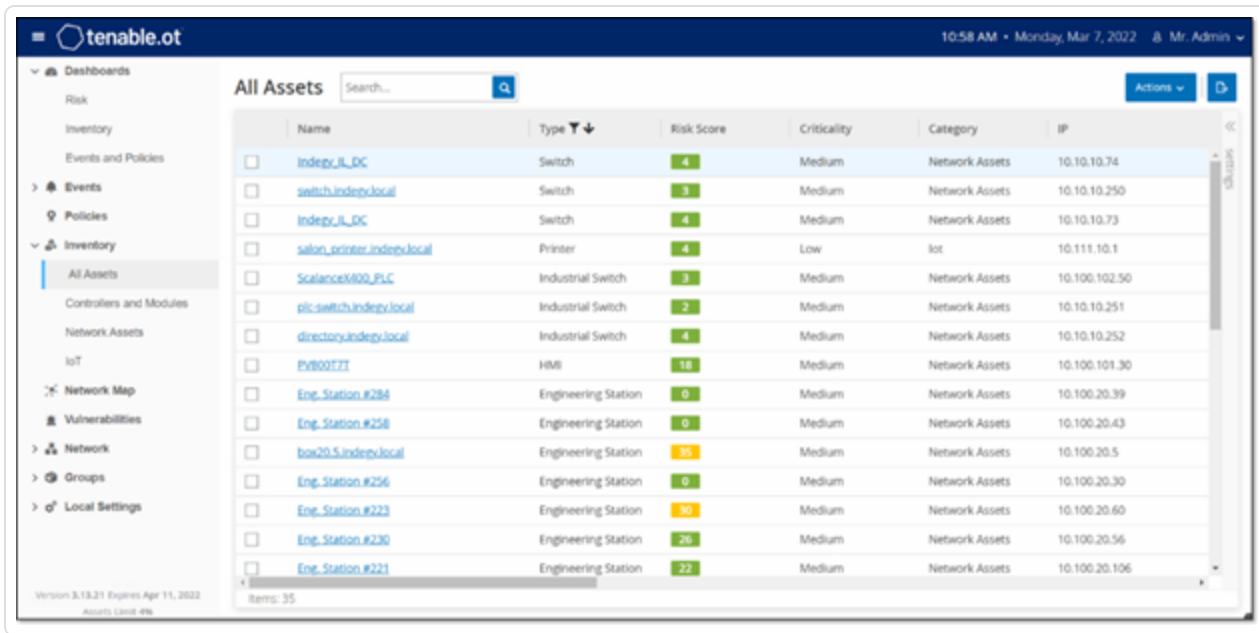
6. In the confirmation window, click **Delete**.

OT Security deletes the exclusion 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



All the assets in the network appear on the **Inventory** pages. The Inventory page includes details about the asset that enables comprehensive asset management as well as monitoring of the status of each asset and its related events. OT Security collects this data using the Network Detection and Active Query capabilities. The **All** page 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 pages (**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 assets list as well as perform a search. For information about how to customize tables, see [Management Console User Interface Elements](#).

The following table describes parameters on the **Inventory** pages.

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

Parameter	Description
Name	The name of the asset in the network. Click the name of the asset to view the Asset Details screen for that asset (See Inventory .)
IP	The IP address of the asset.



	<p>Note: An asset may have multiple IP addresses.</p> <p>Note: 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.</p> <p>Note: Assets can be filtered by IP range. For more on filtering, see Management Console User Interface Elements.</p>
MAC	The MAC address of the asset.
Network Segment	The Network Segment that the IP/s of this asset are assigned to.
Type	The type of asset, Controller, I/O, or Communication, etc. see Asset Types .
Backplane*	The backplane unit that the asset is connected to. Additional details about the backplane configuration are shown in the Asset Details screen.
Slot*	For assets that are on backplanes, shows the number of the slot to which the asset is attached.
Vendor	The asset vendor.
Family*	The family name of the product as defined by the asset vendor.
Firmware	The firmware version currently installed on the asset.
Location	The location of the asset as input by the user in the OT Security asset details. See Inventory .
Last Seen	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.
OS	The OS running on the asset.
Model Name	The model name of the asset.
State*	The device state. Possible values: <ul style="list-style-type: none">• Backup – the controller is running as a backup to a primary controller.















	<ul style="list-style-type: none">• Fault – the controller is in fault mode.• NoConfig – no configuration has been set for the controller.• Running – the controller is running.• Stopped – the controller is not running.• Unknown – the state is unknown.
Description	A brief description of the asset, as configured by the user in the OT Security asset details. See Inventory .
Risk	A measure of the degree of risk related to this asset on a scale from 0 (no risk) to 100 (extremely high risk). For an explanation of how the Risk score is calculated, see Risk Assessment .
Criticality	A measure of the importance of this asset to the proper functioning of the system. A value is assigned automatically to each asset based on the asset type. You can manually adjust the value.
Purdue Level	The Purdue level of the asset (0=Physical process, 1=Intelligent devices, 2=Control systems, 3=Manufacturing operations systems, 4=Business logistics systems).
Custom Field	You can create custom fields to tag your assets with relevant info. The custom field can be a link to an external resource.

Asset Types











The following table describes the various types of assets identified by OT Security. It also shows the icon by which each asset type is represented in the OT Security Management Console (for example 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













		industrial protocols to send information to ICS systems.		PowerMeter
				Remotel/O
				Relay
				Inverter
				IndustrialSensor
				Drive
				Actuator
OT Devices	Medium / 2	This category includes all types of OT devices.		OTDevice
				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 (for example 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
				EngineeringStation
				VirtualWorkstation
Servers	Low / 3	This category includes various types of IT servers.		Server
				FileServer
				WebServer
				VirtualServer









				SecurityAppliance
				TenableICP
				TenableEM
				TenableSensor
				Domain Controller
				IoT
IoTs	Low / 3	This category includes various type of interrelated devices.		Camera
				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

View Asset Details

The **Asset Details** page shows comprehensive details about all data that OT Security discovers for a selected asset. The details appear 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.

To access the **Asset Details** page for a specific asset:

1. Do one of the following:
 - Click the asset name on any of these pages where the asset name appears as a link: **Inventory**, **Events**, or **Network**.
 - In the **Inventory** page, click **Actions > View**.

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

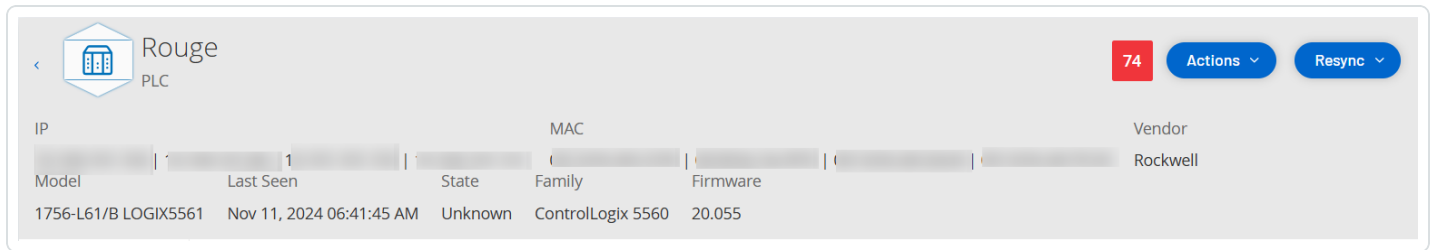


- **Header Pane** – shows an overview of essential info about the asset and its current state. It also contains an Actions menu that enables you to edit the listing for that asset.
- **Details** – shows detailed information divided into subsection with specific data that is relevant to various asset 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, that is 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, that is 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.

IP	MAC	Vendor	Model	Last Seen	State	Family	Firmware
[REDACTED]	[REDACTED]	Rockwell	1756-L61/B LOGIX5561	May 28, 2024 10:54:21 AM	Unknown	ControlLogix 5560	20.055



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 [Perform Resync](#).

Details Tab

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



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

Code Revisions

The Code Revision tab (for Controllers only) shows the various versions of the controller's code that were captured by 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.

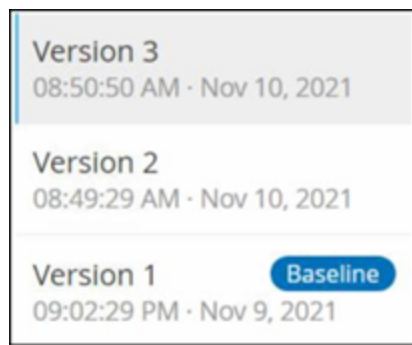
A snapshot can be triggered in the following ways:

- **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 (for example 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





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

Name	Size	Compiled on
[-] Rouge (0)		
[-] Tags (2)		
(Dir) RougeTag1	0	Nov 9, 2021 09:02:29 PM
(Bool) VAXTEK1	0	Nov 9, 2021 09:02:29 PM
[-] Tasks (2)		
[-] MainTask (2)		
[-] Programs (2)		
[-] MainProgram (2)		
[-] 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
(Dir) _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 [Compare Snapshot Versions](#).

Version History Pane

Version 1 Snapshots List	
User Initiated Snapshot	08:02:10 AM · Nov 10, 2021
Routine Snapshot	09:02:29 PM · Nov 9, 2021



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.

Compare 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 a software version control interface. At the top, there is a search bar labeled 'Version 3' and a 'Compare to' dropdown menu set to 'Previous Version'. Below this is a tree view of the file structure:

- ▼ Rouge(7)
 - ▼ Tasks(6)
 - ▼ MainTask(5)
 - ▼ Programs(4)
 - ▼ MainProgram(3)
 - ▼ Tags(2)
 - (Dint) koko (with a red square icon)
 - (Dint) koko3 (with a green plus icon)

Below the tree view is a table with the following columns: Name, Size, and Compiled on.

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.

Create a Snapshot



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

To create a snapshot of a controller:

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

The User Initiated Snapshot is created.

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

IP Trail

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

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

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

Attack Vectors

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

How do we determine the attack vector?



Once the target asset is specified, the system calculates all of the potential attack vectors that could enable access to this asset and identify the path that has the highest risk potential for compromising this asset. The calculation factors in multiple parameters and uses a risk-based approach in order to identify the most critical attack vector. The parameters 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 (for example Port closing or service removal) in order to eliminate the potential attack path.

Generate Attack Vectors

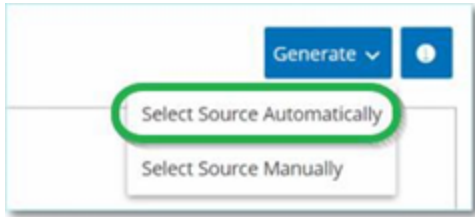
Attack Vectors need to be generated manually for each relevant target asset. This is done on the Attack Vectors tab for the desired target asset. There are two methods for generating Attack Vectors:

- **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:



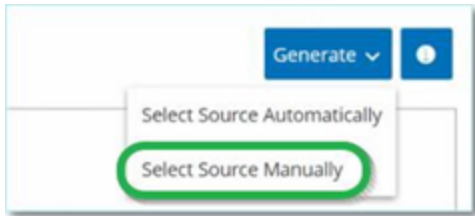
1. Navigate to the **Asset Details** page for the desired target asset and click on the **Attack Vector** tab.
2. Click **Generate** and then click **Select Source Automatically** from the drop-down list.



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 drop-down list.



The **Select Source** window appears.



Select Source



Available Assets



	Name	Risk Score ↓	Type	IP
<input type="checkbox"/>	Rouge	89	PLC	
<input type="checkbox"/>	Praetorian_Gurad	87	PLC	
<input type="checkbox"/>	Comm. Adapter #107	86	Communicati...	
<input type="checkbox"/>	Yuval	86	PLC	
<input type="checkbox"/>	Sith	84	PLC	
<input type="checkbox"/>	Yuval_L71	84	PLC	
<input type="checkbox"/>	Comm. Adapter #129	84	Communicati...	
<input type="checkbox"/>	Comm. Adapter #229	84	Communicati...	
<input type="checkbox"/>	PLC #124	83	PLC	
<input type="checkbox"/>	Yuval_L71_A4	83	PLC	
<input type="checkbox"/>	Project	81	PLC	
<input type="checkbox"/>	Comm. Adapter #63126	80	Communicati...	
<input type="checkbox"/>	olympia.cmx1542-1xb1ae58	80	Communicati...	
<input type="checkbox"/>	Modicon M340	80	PLC	
<input type="checkbox"/>	BMX NOC0401	80	Communicati...	
<input type="checkbox"/>	Comm. Adapter #60141	79	Communicati...	
<input type="checkbox"/>	Project	79	PLC	
<input type="checkbox"/>	Olympia	79	PLC	
<input type="checkbox"/>	Comm. Adapter #63820	79	Communicati...	
<input type="checkbox"/>	default	79	PLC	

settings

Items: 1243

Cancel

Generate

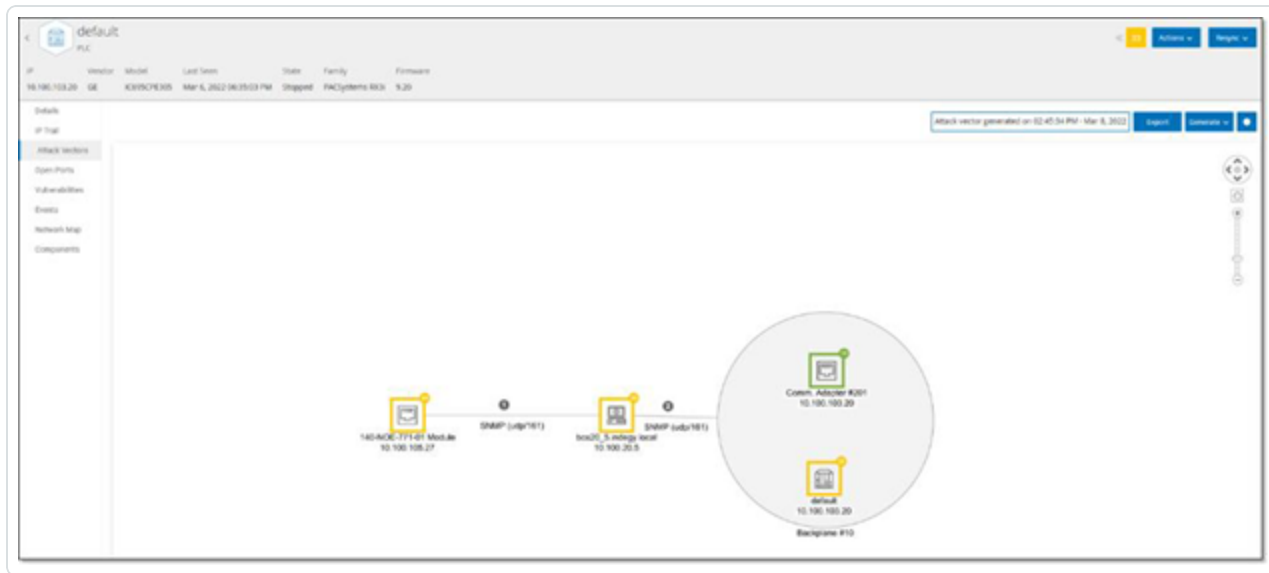


Note: By default, the source assets are sorted by Risk score. You can adjust the display settings or search for the desired asset.

3. Select the required 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.

Open Ports



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

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 [Active 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 **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 **Risks > Vulnerabilities** page , except that only vulnerabilities relevant to the specified asset are shown here. For an explanation of the vulnerabilities information, see [Vulnerabilities](#).

Events



The **Events** tab displays a detailed list of Events in the network involving the asset, as detected by 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 (for example 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 User Interface Elements](#).

Log ID	Time	Event Type	Severity	Policy Name	Source Asset	Source Address	Destination Asset	Destination Address	Protocol
1742	09:02:04 AM Mar 15, 2022	Port Scan	High	20k Scan Detected	Eng.Station#389	10.100.20.200	Eng. Station #389	10.100.20.52	Tcp
10845	08:42:18 AM Mar 15, 2022	Port Scan	High	20k Scan Detected	Eng.Station#389	10.100.20.5	Eng. Station #389	10.100.20.52	Tcp
15960	05:41:28 AM Mar 15, 2022	Port Scan	High	20k Scan Detected	Eng.Station#389	10.100.20.200	Eng. Station #389	10.100.20.52	Tcp
14775	05:05:47 AM Mar 15, 2022	Port Scan	High	20k Scan Detected	Eng.Station#389	10.100.20.5	Eng. Station #389	10.100.20.52	Tcp
12891	01:20:29 AM Mar 15, 2022	Port Scan	High	20k Scan Detected	Eng.Station#389	10.100.20.200	Eng. Station #389	10.100.20.52	Tcp
12945	01:20:14 AM Mar 15, 2022	Port Scan	High	20k Scan Detected	Eng.Station#389	10.100.20.5	Eng. Station #389	10.100.20.52	Tcp
8968	09:59:08 PM Mar 14, 2022	Port Scan	High	20k Scan Detected	Eng.Station#389	10.100.20.200	Eng. Station #389	10.100.20.52	Tcp
8663	09:48:48 PM Mar 14, 2022	Port Scan	High	20k Scan Detected	Eng.Station#389	10.100.20.5	Eng. Station #389	10.100.20.52	Tcp
8676	09:00:08 PM Mar 14, 2022	Rockwell Code Upload	Low	Rockwell Code Upload	Eng. Station #389	10.100.20.52	Destination_L81	10.100.101.152	CP (Win)
8629	09:00:04 PM Mar 14, 2022	Rockwell Code Upload	Low	Rockwell Code Upload	Eng. Station #389	10.100.20.52	Destination_L81	10.100.101.152	CP (Win)
8667	09:00:04 PM Mar 14, 2022	Rockwell Code Upload	Low	Rockwell Code Upload	Eng. Station #389	10.100.20.52	Destination_L81	10.100.101.152	CP (Win)
8665	09:00:03 PM Mar 14, 2022	Rockwell Code Upload	Low	Rockwell Code Upload	Eng. Station #389	10.100.20.52	Destination_L81	10.100.101.152	CP (Win)
8660	09:00:02 PM Mar 14, 2022	Rockwell Code Upload	Low	Rockwell Code Upload	Eng. Station #389	10.100.20.52	Destination_L81	10.100.101.152	CP (Win)
8656	09:00:00 PM Mar 14, 2022	Rockwell Code Upload	Low	Rockwell Code Upload	Eng. Station #389	10.100.20.52	Destination_L81	10.100.101.152	CP (Win)
8606	09:00:19 PM Mar 14, 2022	Rockwell Code Upload	Low	Rockwell Code Upload	Eng. Station #389	10.100.20.52	Destination_L81	10.100.101.152	CP (Win)

Event 34712 08:27:47 AM - Mar 15, 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 NAME: Eng.Station#389
SOURCE IP ADDRESS: 10.100.20.200

Destination DESTINATION NAME: Eng. Station #389
DESTINATION IP ADDRESS: 10.100.20.52

Policy PROTOCOL: Tcp

Scanned Ports

Status

Why is this important? Port scans are just 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 accurate ports for malicious communications.

Suggested Mitigation Make sure that you are familiar with the source of the port scan and that the 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 when you investigate further.

The bottom portion of the page shows detailed information about the selected Event, divided into tabs. Only tabs relevant to the Event type of the selected Event are shown. For more information about Events, see [Events](#).

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

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

Detailed information about these actions is given in the [Events](#) chapter.

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



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



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

Network Map

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



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

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

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

Device Ports

The **Device Ports** tab is available for network switches and includes details about the ports on the network switch. OT Security collects this data using SNMP queries to the switch. The details that appear for each port include the MAC address, Name, connection Status (up or down), Alias, and Description.

MAC	Name	Status	Admin Status	Alias	Description	Type	Time of Query
	P1.11	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P0.2	NotPresent	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.15	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P2.1	NotPresent	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.1	Up	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.3	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.7	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.8	Up	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P2.3	NotPresent	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P2.5	NotPresent	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P2.6	NotPresent	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.4	Up	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.6	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	vlan1	Up	Up	vlan1	Siemens, SIMATIC NE...	L3ipvlan	04:34:37 AM · May 28...
	P1.16	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.2	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...

Items: 31

Note: Activate this feature in your account for the tab to be visible. To activate this feature, contact Tenable Support.

Related Assets

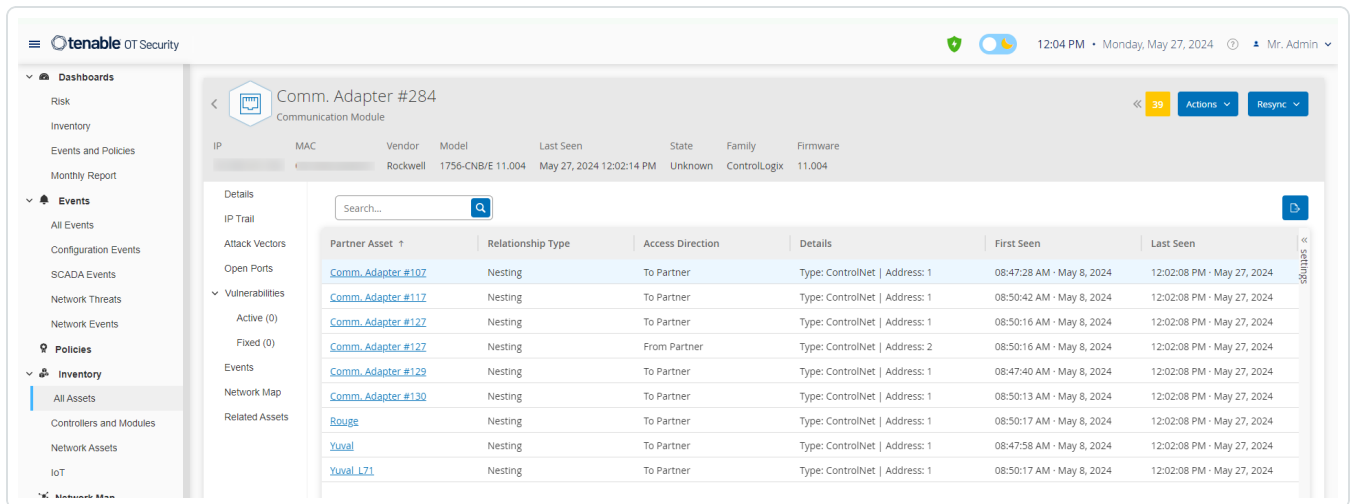


The **Related Assets** page for an asset shows the list of all its nested assets.

To access the **Related Assets** page:

1. In the **Inventory > All Assets** table, click an asset to open the asset details page.
2. In the left navigation pane, click **Related Assets**.

The **Related Assets** page appears.




The **Related Assets** page appears with the following details:

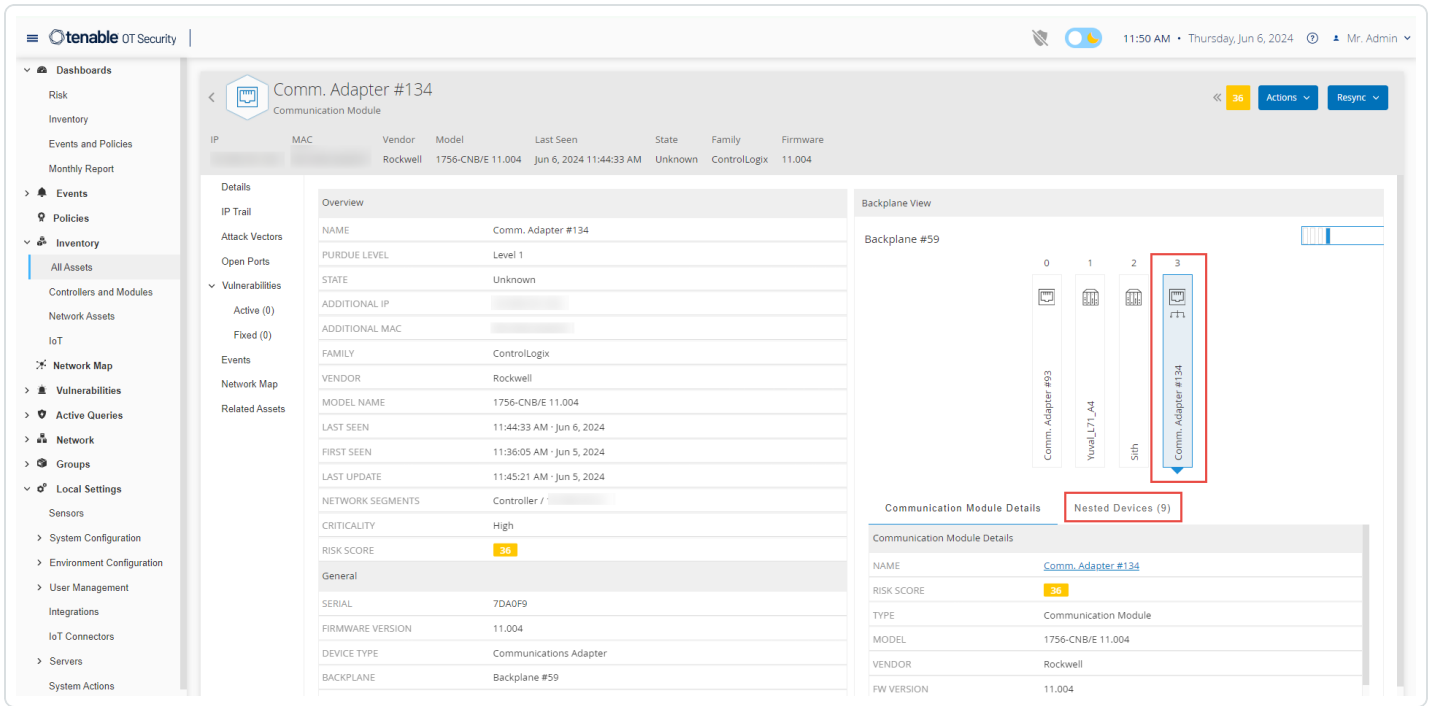
Column	Description
Partner Asset	The name of the related asset.
Relationship Type	The type of relationship with the related asset: Nesting.
Access Direction	The direction of access between the asset and its partner.
Details	The details of the asset type. For example: ControlNet or IP.
First Seen	The date when OT Security initially discovered this asset.
Last Seen	The date when OT Security last detected this asset.

Nested Asset Details

Nested devices are Programmable Logic Controller (PLC)s or other Industrial Control System (ICS) modules connected behind a PLC backplane or device. This is similar to a variable-frequency drive (VFD) connected directly to a communications adapter. To view the details of a nested asset, click



the nested asset link on the **Related Assets** page. OT Security indicates nested devices using the  icon.



The nested asset details page appears with the following details:

Section	Description
Overview	Includes details of the asset such as the name, purdue level, state, additional IP, and so on.
General	Includes details such as serial number, firmware version, device type, backplane number, and slot number.
Backplane View	Includes a graphical view of the backplane. Click the device name on the backplane view to display the Communication Module Details and the Nested Devices tabs.

Edit 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.

Edit 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 required asset.
3. In the header bar, click the **Actions** button.
4. From the drop-down list, select **Edit**.

The **Edit Asset Details** window opens.

Edit Asset Details [X]

Type *
PLC

Name
PLC #49

Criticality *
High

Purdue Level *
Level 1

Location

Description

Cancel Save

5. In the **Type** box, select the asset type from the drop-down list.
6. In the **Name** box, type a name by which the asset will be identified in the OT Security UI.
7. In the **Criticality** box, type the level of criticality of this asset to the system.
8. In the **Purdue Level** box, enter the Purdue level based on the asset type.
9. In the **Backplane** box (for Controllers), type the name of the backplane on which the asset is installed.
10. In the **Location** box, type 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** box, type a description of the asset. This is an optional field. The data is shown on the Asset Details page for this asset.
12. Click **Save**.



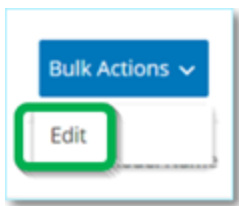
OT Security saves the edited details.

To edit multiple assets (bulk process):

1. Under **Inventory**, click **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 drop-down 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 want 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 must edit each asset manually.

5. Set each of the parameters as required.

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 is erased.

6. Click **Save**.

OT Security saves the assets with the new configuration.

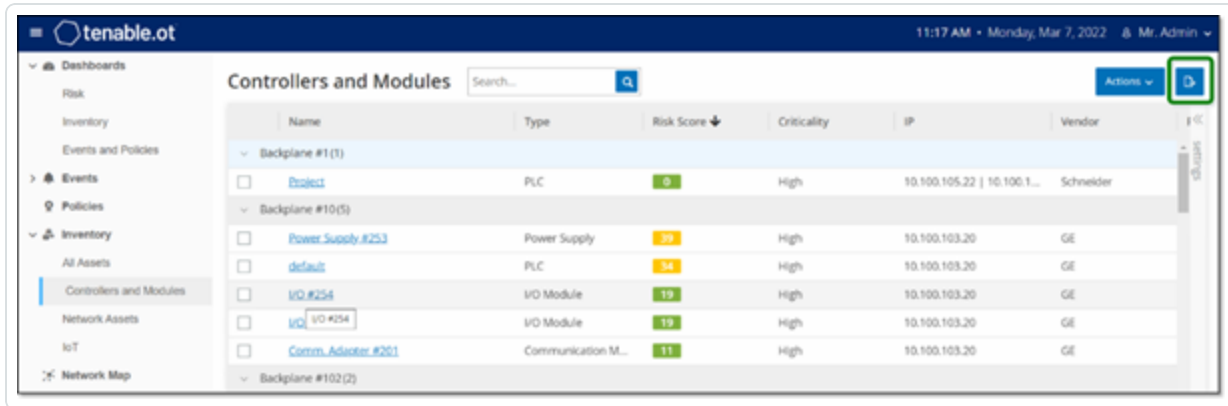
Edit Asset Details by Uploading a CSV



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 **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.

	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	Q#NaZXQIAHTA2MDE		DESKTOP-PLC	PLC	47	High-Critical	33.180.38	Beckhoff	C-Series		2.11.2305	Unknown	Level1	#####					
3	Q#NaZXQIAHTU5WAV		SIMATIC H-PLC		32	High-Critical	33.180.38	Siemens	S7-400	CPU 412-5 6.0.6	Fault	Level1	#####				Siemens, SIMATIC S7		
4	Q#NaZXQIAHJWNTN		C Yairdegy	Communik	20	High-Critical	33.180.38	Helmholtz Netlink		NETLink PI	2.7	Unknown	Level1	#####			700-884-MPI21		
5	Q#NaZXQIAHJY4@J4		aaa	Controller	20	High-Critical	33.180.38	Texas Instruments				Unknown	Level1	#####					
6	Q#NaZXQIAHJQ8M3		BMX NOCI	Communik	13	High-Critical	33.180.38	Schneider Modicon	BMX NOC		2.5	Unknown	Level1	#####	lab		Schneider Electric M		
7	Q#NaZXQIAHJFJHEK		bbab	PLC	74	High-Critical	33.180.38	Siemens	SIPROTEC	75.82		Unknown	Level1	#####					
8	Q#NaZXQIAHJFVJJK		ML1400	PLC	81	High-Critical	33.180.38	Rockwell	MicroLogix	1766-L328	2.015	Unknown	Level1	#####			Allen-Bradley 1766-L		
9	Q#NaZXQIAHJFNTIC		cccc	DCS	72	High-Critical	33.4.0.33	Emerson	S-5 Series	SD Plus	13.3	Unknown	Level1	#####	Austin, Texas		DeltaV - SD Plus Soft		
10	Q#NaZXQIAHJYDWF		S7300/ETJ	Communik	61	High-Critical	33.180.38	Siemens	S7-300	CP 343-1 L3.1.1		Unknown	Level1	#####			Siemens, SIMATIC NI		
11	Q#NaZXQIAHJEM8D		Vnd DCS #9	DCS	93	High-Critical	33.180.38	Tenable				Unknown	Level1	#####					
12	Q#NaZXQIAHJXVYV4		7UT633 V	PLC	76	High-Critical	33.180.38	Siemens	SIPROTEC	7UT63312 04.67.00		Unknown	Level1	#####			SIPROTECA 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 (for example Type, Criticality, Purdue Level). Otherwise, the corresponding asset will fail to update.

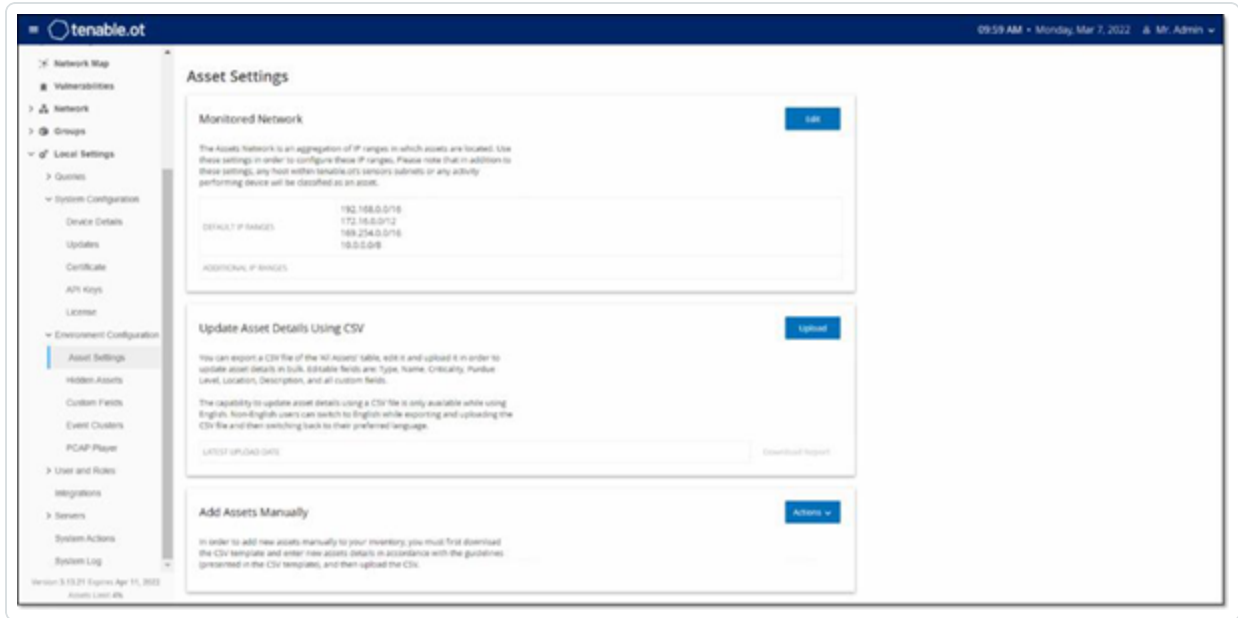
5. Save the file as a csv file type.



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.

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

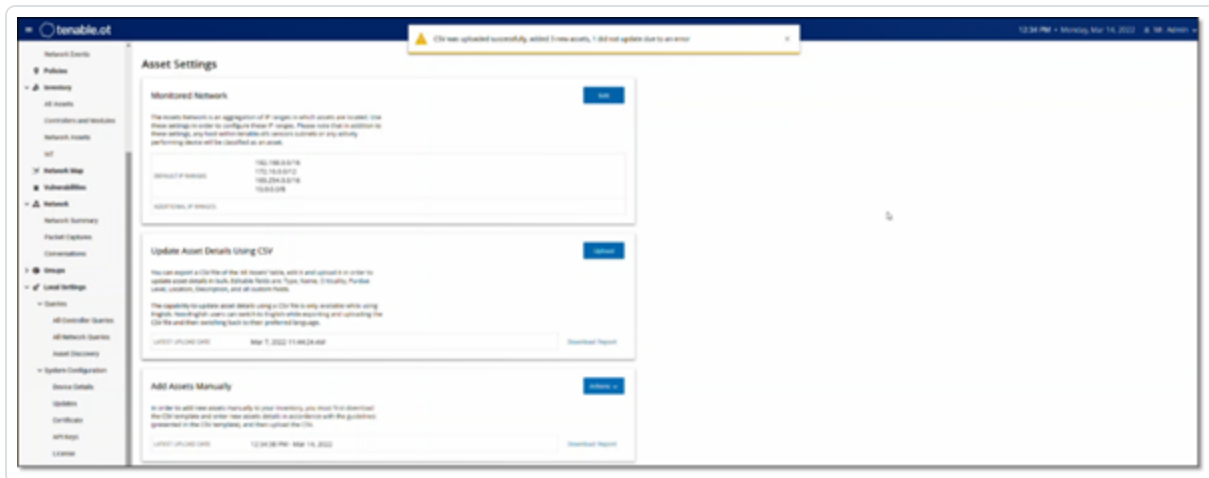
The **Asset Settings** page appears.



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

8. Follow your device's navigation prompts to upload the csv file that you just saved.

A confirmation appears indicating number of updated rows.





The **Latest Upload Date** box in the Update asset details using CSV section is updated.

9. To see more information about the results of the upload, in the **Update asset details using CSV** section, click **Download Report**.

OT Security downloads a csv file that lists the updated asset IDs and also lists the failed ones.

Hide 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.

You can restore a hidden asset from the **Local Settings > Environment Configuration > Hidden Assets** page.

To hide one or several assets:

1. Under **Inventory**, click **Controllers** or **Network Assets**.
2. Select the checkbox next to one or more assets that you want to remove.
3. In the Header bar, click **Actions**.

A menu appears.

4. Select **Hide Asset**.

The **Hidden Assets** page appears.

5. (Optional) In the **Comments** box, add text comments about the assets.

Note: The comments appear in the list of removed assets on the **Local Settings > Environment Configuration > Hidden Assets** page.

6. Click **Hide**.

OT Security hides the assets on the **Inventory** and **Groups** pages.

Export Diagnostics



You can export and download the diagnostic report of an asset or an asset group that shows false positives or has any other issue. You can share this report with the Tenable Support for a detailed analysis.

To export the diagnostics report:

1. In the left navigation bar, go to **Inventory > All Assets**.

The **All Assets** page appears.

2. In the All Assets table, select one or several assets to export in the diagnostics report.

3. Do one of the following:

- For a single asset: In the upper-right corner, click **Actions > Export Diagnostics**.
- For multiple assets: In the upper-right corner, click **Bulk Actions > Export Diagnostics**.

OT Security downloads the diagnostics report for the selected asset or assets. The diagnostics report is a tar.gz file and includes the asset details in a .json file.

The diagnostics report name includes the name of the asset, timestamp, and the OT Security version. Examples:

For a single asset: `TOTS_Rouge_3.19.15_2024-06-03T07_05_27.tar.gz`

For multiple assets: `TOTS_AssetsReport_3.19.15_2024-06-03T07_17_54.tar.gz`

4. Extract the diagnostics report and share it with Tenable Support for further analysis.

Perform 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 uses the WMI and SNMP credentials, if they are available. This action is only available for relevant PC-based machines. You can access the scan results from the Vulnerabilities page. 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. Tenable recommends that you do not use it on OT devices, as it may interfere with their normal operation.



To run a Tenable Nessus Scan on specific assets:

1. Go to **Inventory > Network Assets**.

The **Network Assets** page appears.

2. Select the checkbox next to the asset or assets you want to scan.
3. In the upper-right corner, click **Actions > Nessus Scan**.

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



4. Click **Proceed with Scan**.

OT Security runs the Nessus Scan.

Perform Resync

The Resync function initiates one or more queries to the network and the controller to capture up-to-date information for this asset. You can run all available queries or specific queries.

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 appears in the **Firmware** field in the **Assets > Controllers and Modules** page.
- **Identification query** – Uses multiple protocols to identify the asset.
- **NetBIOS query** – Sends a NetBIOS unicast packet that is used to classify and detect Windows machines in the network.



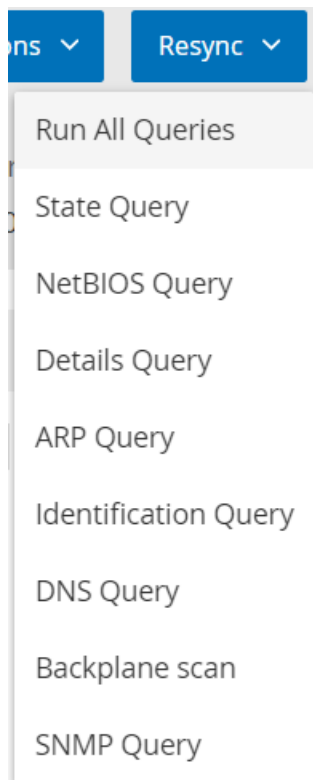
- **SNMP query (for SNMP enabled assets)** – Retrieves configuration details for SNMP-enabled assets.
- **State** – Detects the current status of the asset (**Running**, **Stopped**, **Fault**, **Unknown**, and **Test**).
- **ARP** – Retrieves the MAC address of new IPs detected in the network. The result appears in the **Details > Overview** section.

The **Resync** button may be disabled under specific conditions. Possible reasons include:

- The device is unreachable or lacks available queries.
- Permission configured on the **Active Queries** page may restrict non-administrator accounts from initiating certain queries.
- Queries are not enabled on this OT Security deployment.
- All queries in the **Active Queries > Manual** section are disabled.
- The asset lacks a known IP address for querying.

To run Resync asset data:

1. On the **Asset Details** page for the required asset, in the upper-right corner, click **Resync**.
A drop-down list of queries appears.



2. Click the query that you want to run or click on **Run All Queries** to run all available queries.

As each query runs, a notification appears with the status of the query.

The screenshot displays a log of network queries. The first entry is a successful 'Ping Query'. The second entry is a failed query with a red 'X' icon, indicating a network error. Below this is a table with columns for 'State', 'Family', and 'Firmware'. The table contains one row with the value 'Rockwell Automation 1756-L81F/B'. The following three entries are successful queries: 'SNMP Query', 'DNS Lookup', and 'State Query'. The final entry is a successful 'Details Query'.

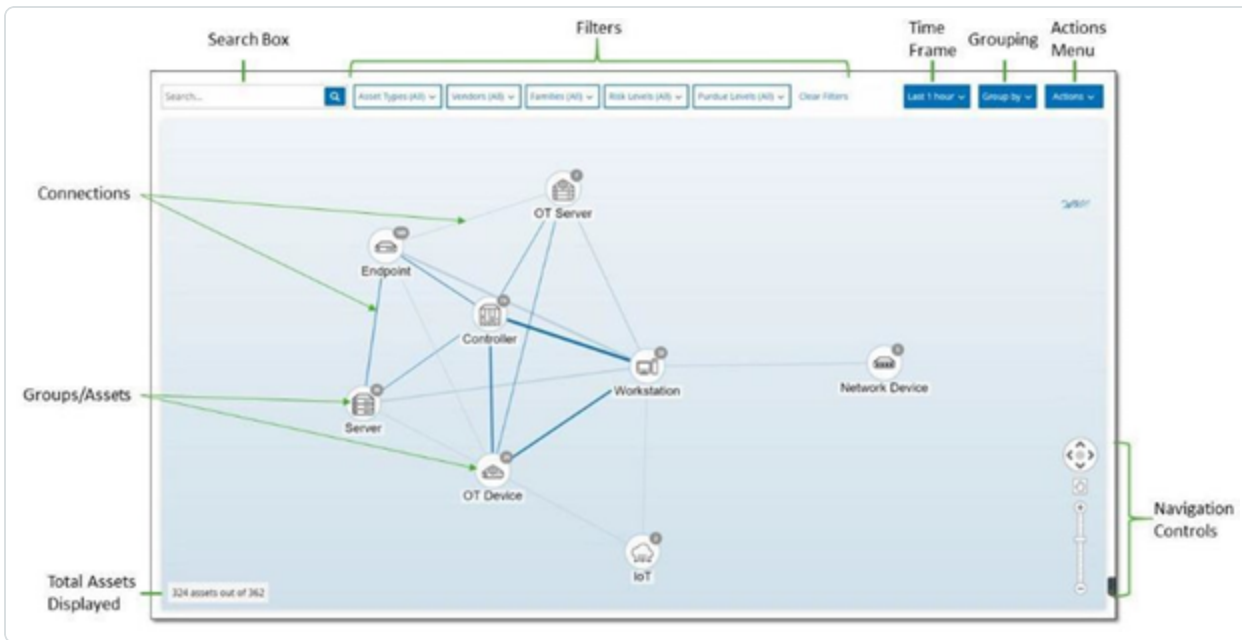
State	Family	Firmware
		Rockwell Automation 1756-L81F/B

For each completed query, OT Security updates the system data for that asset based on the new data.



Network Map

The **Network Map** screen offers a visual representation of the network assets and their connections over time, that OT Security's Network Detection capabilities discovered. Network Detection provides in-depth and real-time visibility into all activities over the operational network, focusing on control-plane engineering activities, such as firmware downloads or uploads, code updates and configuration changes, performed over proprietary, and vendor-specific protocols. Network Map shows the assets by groups of related assets or as individual assets.



The **Network Map** shows all assets and connections that Tenable discovered during the specified timeframe.

The **Network Map** page shows the following details:

- **Search Box** – Type a search text to search for assets in the display. The Network Map shows the search results by highlighting all groups that match the search text. You can drill down into each group to see the relevant assets.
- **Filters** – Filter the map display by one or several of the specified categories: **Asset Type**, **Vendors**, **Families**, **Risk Levels**, and **Purdue Levels**. For an explanation of asset types, see [Asset Types](#).



- **Time Frame** – The Network Map shows assets and network connections detected during the specified timeframe. The default timeframe is set for **Last 30 days**. In the timeframe drop-down box, select a different timeframe.
- **Grouping** – Specify the category used to group the assets in the display. The options are: **Asset type, Purdue level, Risk level, or No grouping**. The **Collapse all groups** option keeps the current grouping selection visible but collapses all other open groups.
- **Actions** – You can select the following actions from the drop-down menu:
 - **Set as baseline** – Set the baseline used for detecting anomalous network activity, see [Set a Network Baseline](#).
 - **Auto arrange** – Automatically optimize the map display for the entities currently being displayed.
- **Groups/Assets** – An icon on the map represents each group of assets, with a distinct icon depicting each asset type. as described in [Asset Types](#). For groups, the number at the top of the icon indicates the number of assets 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 timeframe and asset filters. This number is shown relative to the total number of assets detected in your network.
- **Navigation Controls** – You can adjust the display by zoom in and out and navigate to show the desired elements using either the onscreen controls or standard mouse controls.

Asset Groupings

The **Network Map** page can show assets grouped by various categories. It shows connections between groups of assets. You can click on an asset to drill-down to the elements in that group.



You can also drill-down in multiple groups simultaneously. OT Security offers multiple layers of embedded groups, so that drill-down gives you a more granular view of the included assets.

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

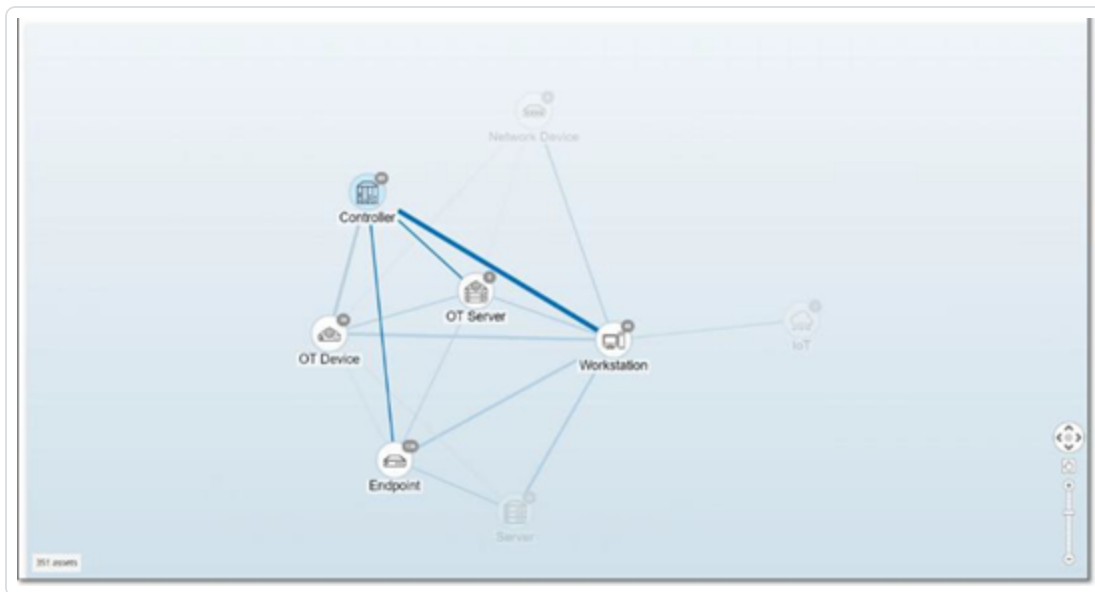
When the map displays groups by **Asset Type** (default), the drill-down hierarchy is as follows: **Asset Type > Vendor > Family > Individual Asset**.

When the Map displays groups by **Risk Level** or **Purdue Level**, it adds an additional level above the Asset Type grouping to give this hierarchy: **Purdue Level/Risk Level > Asset Type > Vendor > Family > Individual Asset**. A circle surrounds the included groups/assets, representing each level.

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

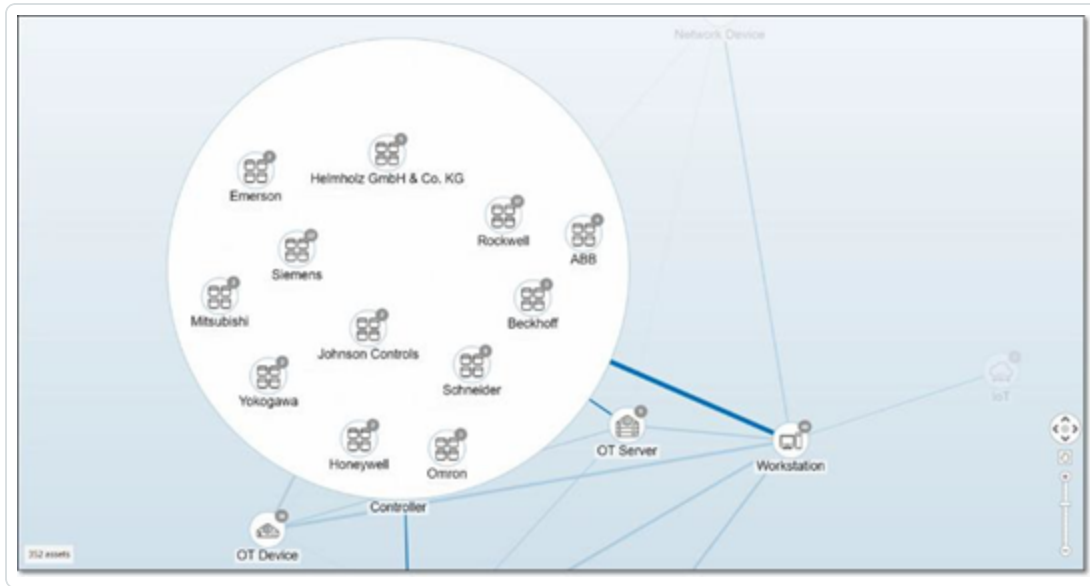
To drill down to an Asset Type Group:

1. By default, the **Network Map** screen opens with the assets grouped by Asset type.

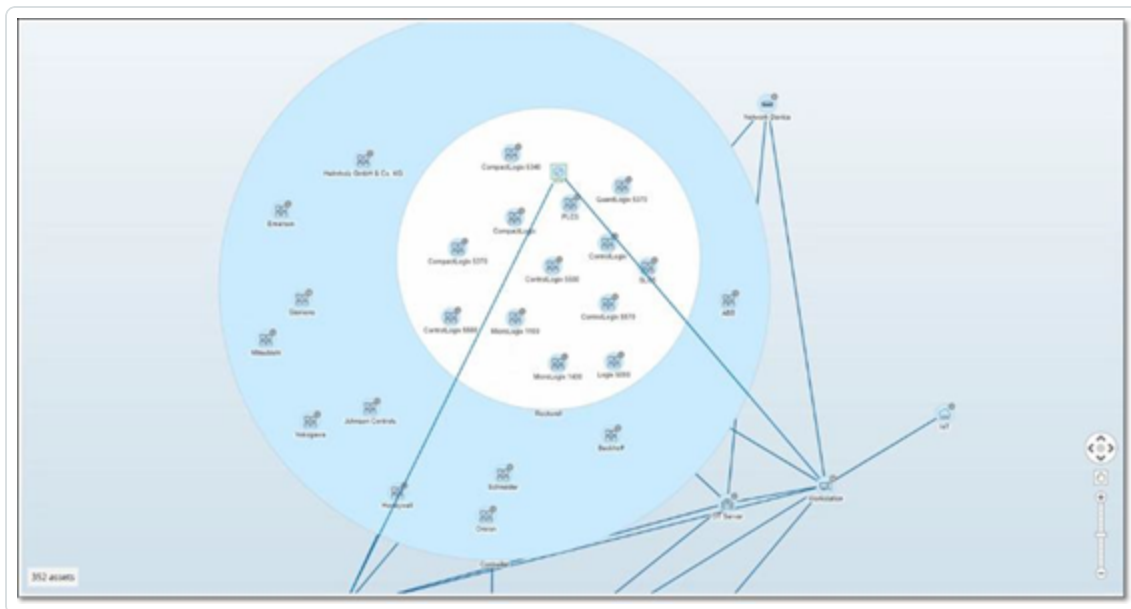


2. Double-click on the group icon that you want to drill down into (for example, Controller).

The group expands to display the Vendor groups within that group.

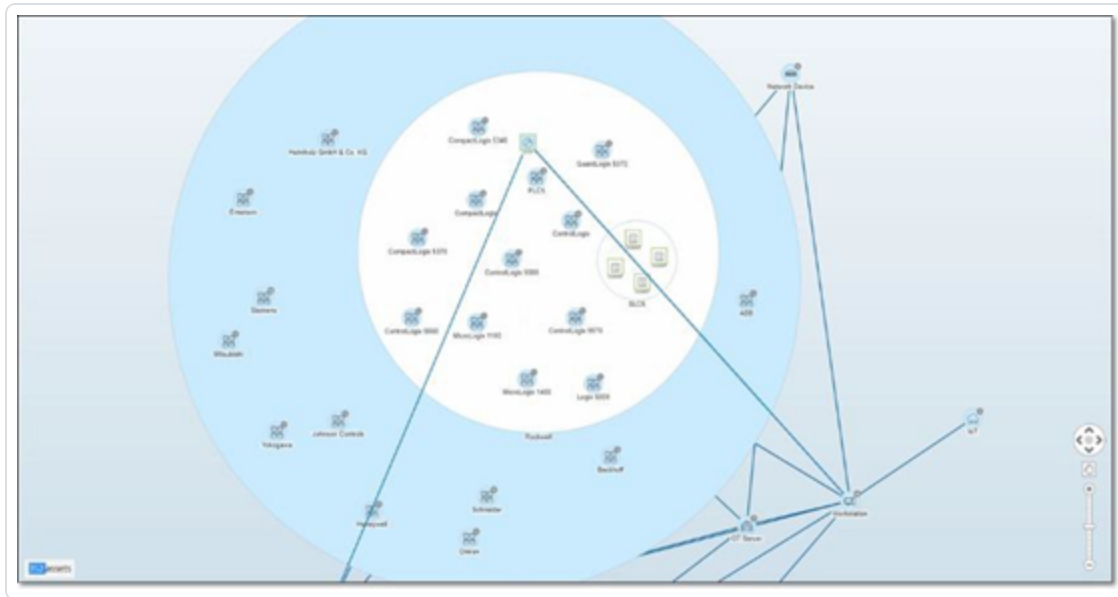


3. To drill down further, click a Vendor group (for example, Rockwell).



4. To drill down further, click a Family group (for example, SLC5).

The individual assets within that group appear.



5. You can now click 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 shows the top-level groups again.

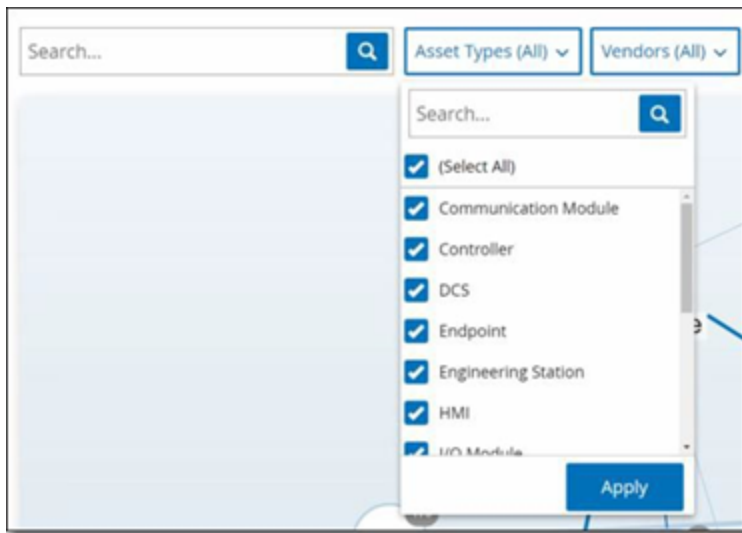
To remove all grouping:

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

The map shows all single assets without any grouping.

Applying Filters to the Map Display

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



To apply filters to the map:

1. Click the required filter category.
2. Select or clear the check boxes for each element that you want to include or exclude from the display.

Note: By default, the filter includes all elements.

3. You can click the **Select All** check box to clear all the values and 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**.

The map shows only the selected elements.

Viewing Asset Details

You can click 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 communicate with it. You can then click the asset name link to go to the **Asset Details** screen for more details about the asset.



Set 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 serves for Network Baseline Deviation Policies, which alert for anomalous conversations in the network, see [Network Event Types](#).

Assets that did not interact during the Baseline sample trigger a Policy alert for each conversation (assuming it falls within the scope of the specified Policy conditions). To enable the creation of Network Baseline Deviation policies, you must first create an initial Network Baseline on the **Network Map** screen. You can update the Network Baseline anytime by setting a new Network Baseline.

To set a Network Baseline:

1. On the **Network Map** screen, select the time range of the conversations 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 appears.

2. In the upper-right corner, select **Actions > Set as baseline**.

OT Security configures the new network baseline and applies the baseline 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 is discovered and released into the general public domain, Tenable 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 Tenable Nessus Attack Scripting Language (NASL). Plugins detect CVEs as well as other threats that can affect assets in your network (for example, obsolete operating systems, usage of vulnerable protocols, vulnerable open ports, and so on.)

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

The **Vulnerabilities** page 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 User Interface Elements](#).

(For version 3.19 only) The **Active Vulnerabilities** and **Fixed Vulnerabilities** options available on the left navigation bar allows you to view open and fixed vulnerabilities respectively.

Name	Severity	VPR	Fixed Assets	Plugin family	Plugin ID	Source	Comment	Owner
Tot(69)								
<input type="checkbox"/> Schneider Electric Modicon Missing Authentica...	Critical	6.7	1	Tenable.ot	500071	Tot		
<input type="checkbox"/> Schneider Electric Modicon Authentication Bypa...	Critical	6.7	1	Tenable.ot	500122	Tot		
<input type="checkbox"/> Schneider Electric Modicon Exposure of Resourc...	Critical	6.7	1	Tenable.ot	500125	Tot		
<input type="checkbox"/> Schneider Electric Modicon Weak Password Rec...	Critical	6.7	1	Tenable.ot	500170	Tot		
<input type="checkbox"/> Schneider Electric Modicon Weak Password Der...	Critical	6.7	1	Tenable.ot	500226	Tot		



Note: OT Security retains fixed vulnerabilities for a year before they age out.

The **Vulnerabilities** page shows the following details:

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

Plugin Details

To view the plugin details:

1. In the row of the vulnerability for which you want to view the details, click the vulnerability name.



The Vulnerability details window appears.



The Vulnerability details window shows the following details:

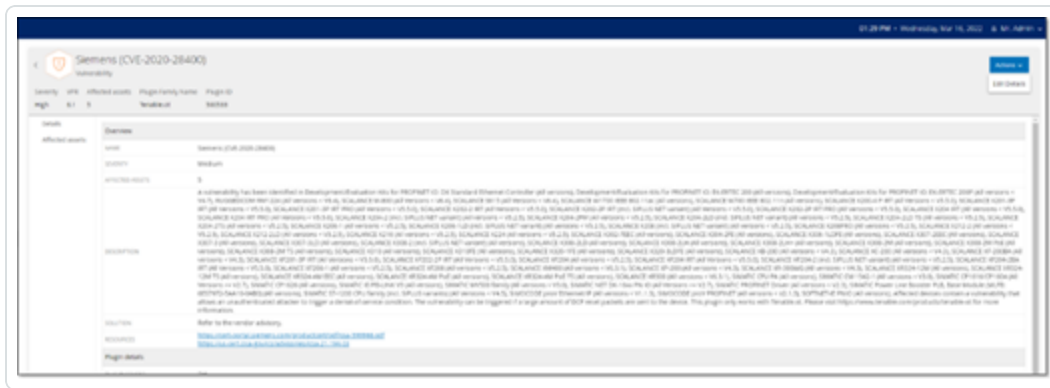
- **Header bar** – Shows basic information about the specified vulnerability. From the **Actions** menu, select **Edit Details** to edit vulnerability details. See [Edit Vulnerability Details](#).
- **Details tab** – Shows the full description of the vulnerability and gives links to relevant resources.
- **Affected Assets tab** – Shows a listing of all assets 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.

Edit Vulnerability Details

To edit vulnerability details:

1. In the relevant **Vulnerability Details** page, in the upper-right corner, click the **Actions** menu.

The **Actions** menu appears.



2. Click **Edit Details**.

The **Edit Vulnerability Details** panel appears.



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

View Plugin Output



Plugin output for an asset provides context or an explanation as to why a particular plugin is reported for an asset.

To view the plugin output details from the Vulnerabilities page:

1. Go to **Vulnerabilities**.

The **Vulnerabilities** page appears.

2. In the list of vulnerabilities, select the one for which you want to view the details and do one of the following:
 - Click the vulnerability link.
 - Right-click the vulnerability and select **View**.
 - From the **Actions** drop-down box, select **View**.

The Vulnerability Details page appears with the **Plugin Output** panel and shows the following information:

- Hit date
- Source
- Port
- Plugin output

Note: Plugin output is not available for all plugins.

To view the plugin output details from the Inventories page:

1. Go to **Inventories > All Assets**.

The **Inventories** page appears.

2. In the list of assets, select the one for which you want to view the details and do one of the following:
 - Click the asset link.
 - Right-click the asset and select **View**.



- Select the checkbox next to the asset, and then from the **Actions** drop-down box, select **View**.

The Asset Details page appears.

3. Click the **Vulnerabilities** tab.

The list of vulnerabilities appears and shows the **Plugin Output** panel with the following information:

- Hit date
- Source
- Port
- Plugin output

Note: Plugin output is not available for all plugins.

Example of a plugin output for a Tenable Nessus Plugin

MS10-031: Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution (978213)

Severity: Critical, VPR: 8.9, Affected Assets: 1, Plugin Family Name: Windows : Microsoft Bulletins, Plugin ID: 46313

Name	Last Hit Date	Type	Risk Score	Criticality	IP	MAC	Category
WIN-18OFIPB12HM	Jul 10, 2023 09:52:26 PM	Engineering S...	47	Medium	(Direct)	...	Network Assets

Items: 1

WIN-18OFIPB12HM (Direct) Engineering Station 47 Jul 18, 2023 02:50:54 PM

Plugin Output

Port: 445 / tcp / cifs Source: Nessus Hit date: 09:52:26 PM · Jul 10, 2023

```
- C:\Program Files (x86)\Common Files\Microsoft Shared\VBA\VBA6\Vbe6.dll has not been patched.  
Remote version : 6.0.87.14  
Should be : 6.5.10.53
```



Example of a plugin output for OT Security Plugin

Rockwell Automation ControlLogix Communications Modules Remote Code Execution (CVE-2023-3595)

Severity: Critical | VPR: 6.7 | Affected Assets: 3 | Plugin Family Name: Tenable.ot | Plugin ID: 501226

Name	Last Hit Date	Type	Risk Score	Criticality	IP	MAC	Category	Vendor
Comm_Adapter #50	Jul 18, 2023 07:05:36 PM	Communicati...	61	High			Controllers	Rockwell
Comm_Adapter #35	Jul 18, 2023 07:05:36 PM	Communicati...	67	High	1	...	Controllers	Rockwell
Comm_Adapter #53	Jul 18, 2023 07:05:35 PM	Communicati...	68	High		...	Controllers	Rockwell

Items: 3

Comm. Adapter #50 | 10.100.101.152 (Direct) | Communication Module | 61 | Jul 18, 2023 07:10:14 PM

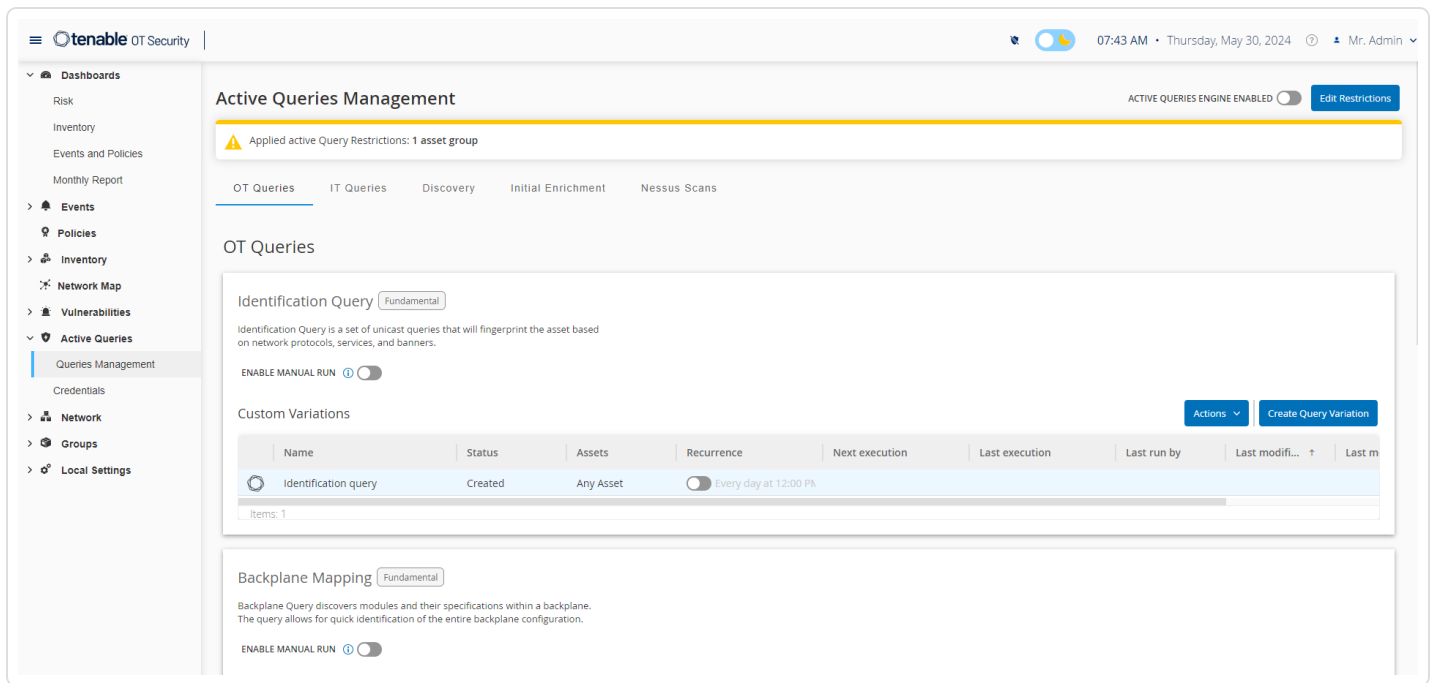
Plugin Output

```
Port: 0 / tcp | Source: Tot | Hit date: 07:05:36 PM · Jul 18, 2023
```

```
Vendor : Rockwell  
Family : ControlLogix  
Model : 1756-EN2T/D  
Version : 10.007
```

Managing Active Queries


The **Active Queries Management** page allows you to configure and enable active queries. As part of the initial setup, Tenable recommends that you activate all query capabilities. At any time, you can activate/deactivate any query functions. You can also adjust the settings for when and how to execute the queries.



In addition to the automatic queries that run periodically, you can initiate queries on demand by enabling the **Enable Manual Run** toggle in the query card. If you disable the **Enable Manual Run** option, OT Security prompts you to override it when you select [Perform Resync](#) in the **Assets Details** page (**Inventory > All Assets**).

For more information about the queries technology, see [OT Security Technologies](#).

Note: OT Security may fail to identify assets when you disable queries. OT Security tracks devices through passive monitoring as well as active querying.

Tip: To allow active queries to function, click the **Active Queries Engine Enabled** toggle. After you enable the active queries, OT Security displays a  on the header to indicate that the query engine is running. To run active queries, you must still enable each individual query separately.

The **Active Queries Management** page categorizes queries into the following types. There is a separate query tab for each query type with its list of queries.

- **OT Queries** – These are queries designed to poll controllers and embedded devices safely for more information using their proprietary protocols. OT Security performs read-only queries to gather device information, such as PLC running state and other modules connected to the



backplane. It queries devices that are listening for proprietary protocols that OT Security supports. The query types include **Identification Query**, **Backplane Mapping**, **Details Query**, **State Query**, and **Code Snapshots**.

- **IT Queries** – These queries fetch additional data points from monitored IT-type assets that OT Security observes. With the exception of NetBIOS, these IT-type queries require credentials.
 - **NetBIOS query** attempts to discover any devices listening for NetBIOS in the broadcast range of OT Security Sensor or OT Security itself. This type of query is suitable for identifying nearby Windows devices.
 - **SNMP query** uses SNMP v2 or SNMP v3 credentials to solicit network infrastructure or networked devices supporting SNMP for their identification details. OT Security queries for SNMP system description and other parameters to help add asset context and assist with fingerprinting.
 - **WMI details query** fetches a variety of important data points from Windows-based systems. This requires the system that OT Security queries to have a Windows account (local or domain) with sufficient permissions to poll the Windows Management Instrumentation (WMI) service.
 - **WMI USB State** queries determine if removable media such as USB-drives or portable hard-drives are connected to the Windows device, such as an engineering workstation or server. This query is closely related to the **Change in USB Configuration on Windows Machines** policy as it is a prerequisite for this policy to work correctly.
 - **Nessus Basic Scan** fetches system details such as IP address, FQDN, operating systems, and open ports.
 - **ARP Query** or Address Resolution Protocol query fetches the network interface hardware address or MAC address for IP connected devices in the same broadcast domain.
- **Discovery** – These queries detect live assets in the network that OT Security monitors.
 - **Asset Discovery** – Leverages Internet Control Message Protocol (ICMP) or ping to detect live and responding IP addresses.



- **Active Asset Tracking** – Regularly attempts to ping a known, monitored asset to ensure that it is still up and available.
- **Controller Discovery** – Sends a set of multicast packets to the network to provoke controllers or ICS devices to reply directly to OT Security with their information.
- **Ping Query** – Sends Internet Control Message Protocol (ICMP) pings to verify if an asset is reachable.
- **DNS Lookup** – Fetches the DNS server details.
- **Port Mapping** – Fetches details about open ports on monitored assets.
- **Initial Enrichment** – Automatic OT Security queries based on certain criteria or conditions. Asset enrichment-based queries occur whenever Tenable initially observes a device passively or actively. With Asset Enrichment, OT Security fingerprints and identifies the device as soon as it appears on the network.
- **Nessus Scans** – The Tenable Nessus plugin scan launches an advanced Nessus scan that executes a user-defined list of Plugins on the assets specified in the list of CIDRs and IP addresses. For more information, see [Create Nessus Plugin Scans](#) .

Create Custom Queries

Each type of query has a system default variation that you can run periodically or on-demand. You can also create additional variations of each query, with its own respective configuration, for different projects and functions.

For example, you can configure custom queries for the following scenarios:

- Different maintenance times for different parts of the plant.
- Different projects and criticality for different assets.
- Different queries for OT functions and IT functions.

To create a query variation:



1. Go to **Active Queries > Queries Management**.

The **Active Queries Management** page appears.

2. Click the required query type tab.

OT Security displays the query type with the list of available queries.

3. In the required query type section, click **Create Query Variation**.

The **Create Query Variation** panel appears.

4. In the **Name** box, type a name for the query.

5. In the **Assets** drop-down box, select an asset group.

Note: You can also use the **Search** box to search for a specific group.

6. To repeat the query, click the **Recurring Run** toggle.

OT Security enables the **Repeats Every** section.

7. Type a number and select **Days** or **Weeks** from the drop-down box, . For certain queries, you can also set **Minutes** and **Hours**.

If you select **Weeks**, indicate the days of the week to run the queries.

8. In the **At** box, set the time of day to run the queries (in HH:MM:SS) by clicking on the clock icon and selecting the time, or by typing the time manually.

9. (Only for Asset Discovery) In the **IP Ranges** box, type the IP addresses of assets.

10. (Only for Discovery Queries) In the **Number of Assets to poll simultaneously** drop-down box, select the number of assets (10, 20, or 30).

11. (Only for Discovery Queries) In the **Time Between Discovery Queries** drop-down box, select the time between the discovery queries (1 to 3 seconds).

12. Click **Save**.

OT Security adds the query to the **Custom Variations** table.

See [Run a Query Variation](#).

Add Restrictions



You can block queries from running on specific asset groups, such as IP ranges, OT servers, Tablets, Medical Devices, Domain Controllers, and so on. You can also apply restrictions on specific protocols (clients).

To add restrictions:

1. Go to **Active Queries > Queries Management**.

The **Active Queries Management** page appears.

2. In the upper-right corner, click **Add Restrictions**.

The **Add Restrictions** panel appears.

3. In the **Blocked Assets** drop-down box, select the required asset groups to block.

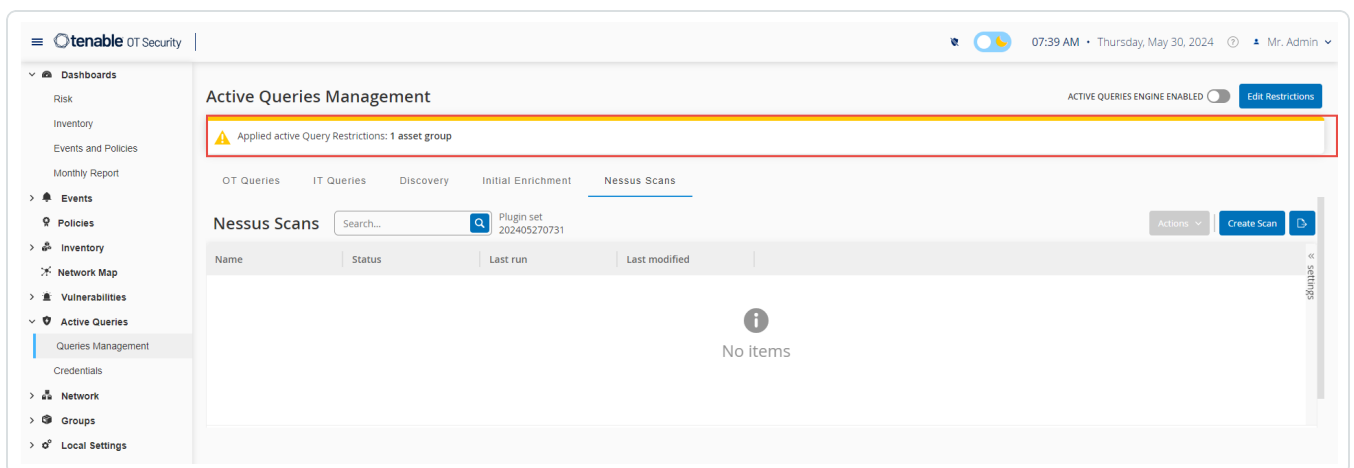
Note: You can use the search box to search for specific asset groups.

4. In the **Restricted Clients** drop-down box, select the required clients.

5. In the **Blackout Period** drop-down box, select the duration for which you want to block the active queries. Available options are based on Schedule Groups. Default options are: **None**, **Working Hours**.

6. Click **Save**.

OT Security applies the restrictions on the specific clients and asset groups. A banner appears at the top of each tab indicating that restrictions are in place.



Edit Query Variation



To edit details of a query:

1. Go to **Active Queries > Queries Management**.

The **Active Queries Management** window appears.

2. From the list of queries, select the one to edit and do one of the following:
 - Right-click the query and select **Edit**.
 - Select the query, then click **Actions > Edit**.

The **Edit Query** panel appears.

3. Modify the query as needed.
4. Click **Save**.

OT Security saves the changes to the query variation.

Duplicate a Query Variation

1. Go to **Active Queries > Queries Management**.

The **Queries Management** page appears.

2. From the list of queries, select the one to create a copy and do one of the following:
 - Right-click the query and select **Duplicate**.
 - Select the query, then click **Actions > Duplicate**.

The **Duplicate Query** panel appears with details of the query.

3. Rename the query and modify the details as needed.
4. Click **Save**.

OT Security saves the query and it appears in the Queries table.

Run a Query Variation

You can run active queries when needed.

To run a query:



1. Go to **Active Queries > Queries Management**.

The **Queries Management** page appears.

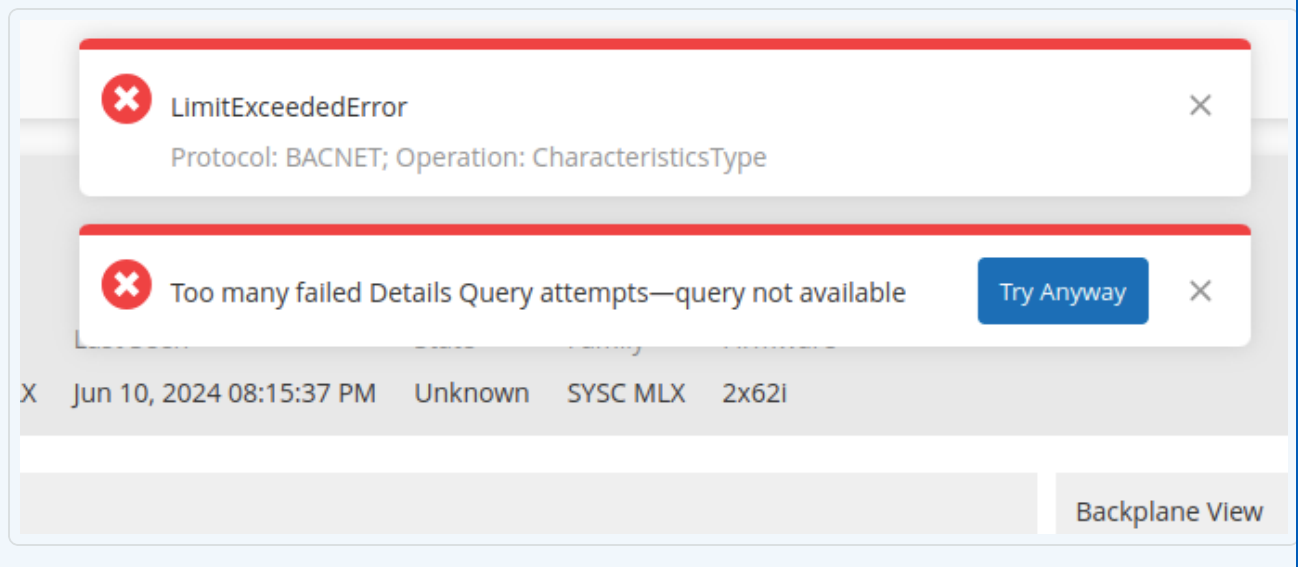
2. From the list of queries, select the one you want to run and do one of the following:
 - Right-click the query and select **Run now**.
 - From the **Actions** menu, click **Run now**.

A message asks for confirmation to run the query.

3. Click **Ok**.

OT Security runs the selected query.

Note: You can use the **Try Anyway** option to proceed with active queries on devices or network to override the limit to the number of active query attempts.



Download Query Log

You can download the log of the last run of a query variation. You can use the log to troubleshoot issues with any of the assets or protocols included in the active query.

To download the last query log:

1. Go to **Active Queries > Queries Management**.

The **Queries Management** window appears.

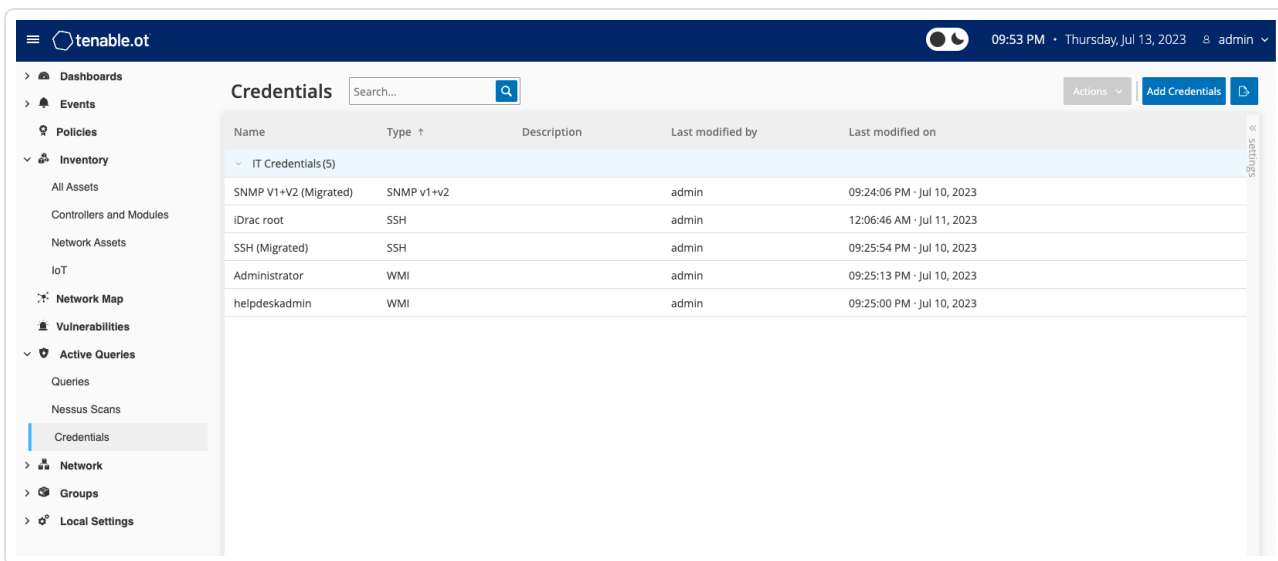


- From the list of queries, select the one for which you want to download the log and do one of the following:
 - Right-click the query and select **Download Last Run Log**.
 - From the **Actions** menu, click **Download Last Run Log**.

OT Security downloads the log of the last active query.

Credentials

Use the **Credentials** page to configure device credentials where required. When communicating in their native network protocols, or proprietary protocols, devices do not require credentials. However, certain devices that OT Security support may require credentials to perform asset discovery.



Add Credentials

To add credentials:

- Go to **Active Queries > Credentials**.

The **Credentials** page appears.

- In the upper-right corner, click **Add Credentials**.



The **Add Credentials** panel appears.

Add Credentials ×

Credentials Type Credentials Details

WMI

NAME *

DESCRIPTION

USERNAME *

PASSWORD *

TEST IP ADDRESS

[Test Credentials](#)

3. In the **Credentials Type** section, click to select the device type. Options available are:



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

4. Click **Next**.

The **Credentials Details** panel appears.

5. Provide the following details:

- **Name** – A name for the credentials.
- **Description** – A description for the credentials.
- **Username** – The username for the device.
- **Password** – The password for the device.
- **Test IP Address** – The IP address of the device.

6. Click **Test Credentials** to confirm if OT Security can reach the device using the credentials.

7. Click **Save**.

OT Security saves the credentials and they appear on the **Credentials** page.

Edit Credentials

You can edit your credential details.

To edit credentials:



1. Go to **Active Queries > Credentials**.

The **Credentials** page appears.

2. Do one of the following:

- Right-click the required credential and select **Edit**.
- Select the required credential, then from the **Actions** menu, select **Edit**.

The **Edit Credentials** panel appears.

3. Modify the details as needed.
4. Click **Save**.

Delete Credentials

You can delete the credentials that you no longer need.

To delete credentials:

1. Go to **Active Queries > Credentials**.

The **Credentials** window appears.

2. Do one of the following:

- Right-click the required credential and select **Delete**.
- Select the required credential, then from the **Actions** menu, select **Delete**.

OT Security deletes the selected credentials.

WMI Accounts

To enable OT Security to perform Windows Management Instrumentation (WMI) queries, you can set up a WMI account. OT Security relies on WMI queries to obtain more information about Windows systems.

OT Security depends on the same WMI methods as Tenable Nessus when performing WMI queries. To set up a WMI account for scanning, see the [Enable Windows Logins for Local and Remote Audits](#) section in the Tenable Nessus User Guide.

Create Nessus Plugin Scans



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

The OT Security executes the scan on responsive assets within the designated CIDRs. However, to protect your OT devices, OT Security scans only confirmed network assets in the given range (non-PLCs). OT Security excludes assets of the type **Endpoint** from the scan.

Note: Tenable Nessus is an invasive tool which works best in IT environments. Tenable does not recommend Tenable Nessus for use on OT devices, as it may interfere with their normal operation.

To run a basic Nessus scan on any one asset, see [Perform Asset-Specific Tenable Nessus Scan](#).

Note: You can run the basic scan on assets of type **Endpoint**.

Create a Nessus Plugin Scan

To create a Nessus Plugin Scan:

1. Go to **Active Queries > Queries Management**.

The **Active Queries Management** page appears.

2. Click the **Nessus Scans** tab.
3. In the upper-right corner, click **Create Scan**.

The **Create Nessus Plugin List Scan** panel appears.

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).

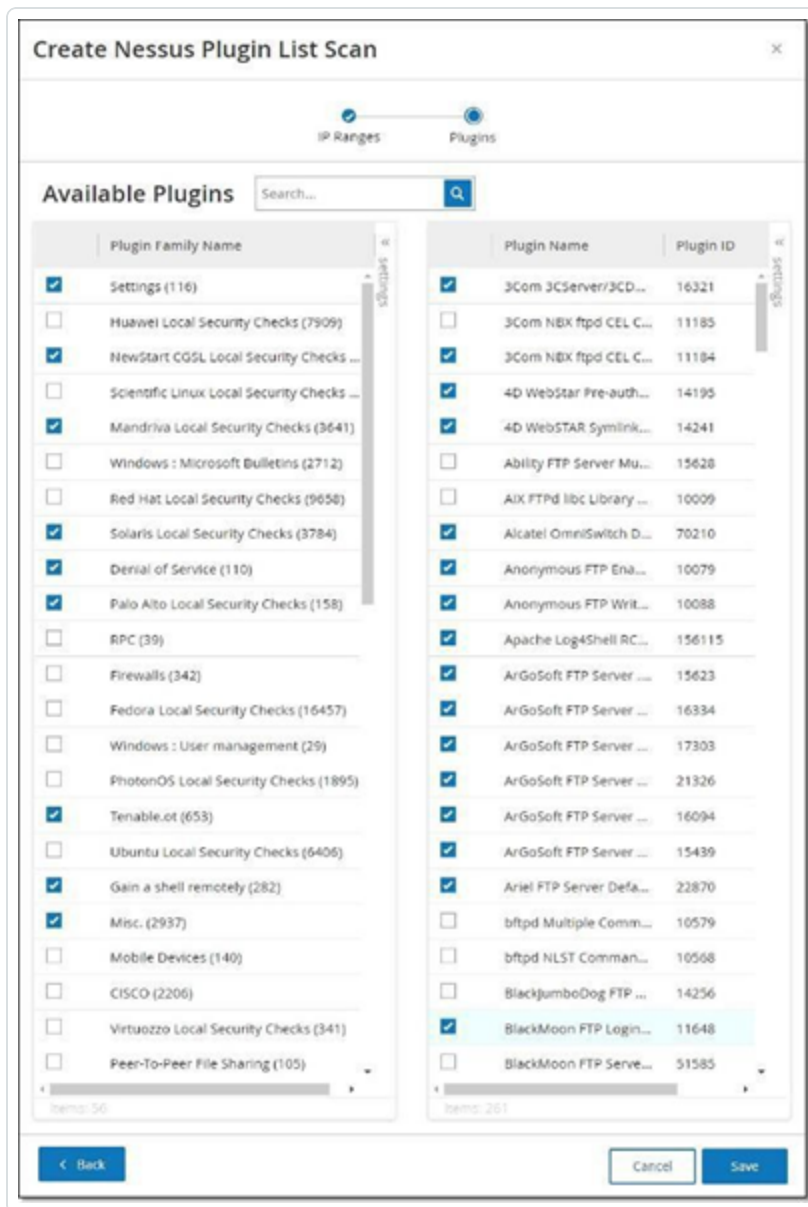
NAME *

IP RANGES *

Cancel Next >

4. In the **Name** box, type a name for the Nessus scan.
5. In the **IP Ranges** box, type a range of IPs or CIDRs.
6. Click **Next**.

The **Plugins** pane appears.



Note: OT Security lists only those plugins that are specific to the device. Your license must be up to date to receive new Plugins. To update your license, see [Update the License](#).

- In the **Plugin Family Name** column, select the required Plugin Families to include them in the scan. In the right column, clear the checkboxes for individual plugins as needed.

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

- Click **Save**.



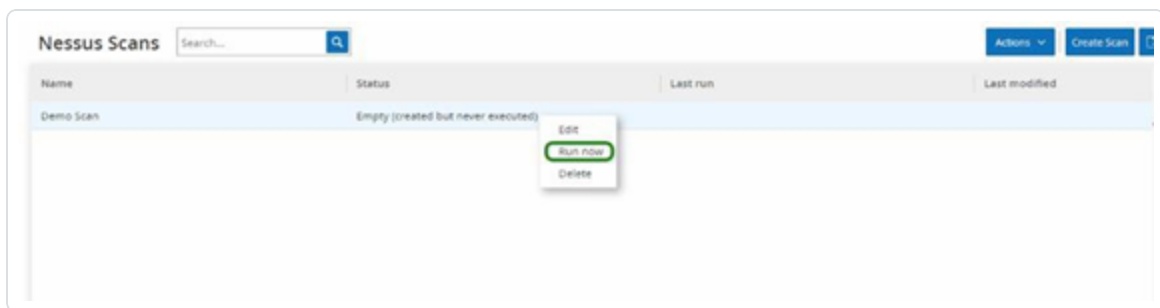
The new Nessus scan appears on the **Nessus Scans** page.

Note: To edit or delete an existing Tenable Nessus scan, right-click the scan, then select **Edit** or **Delete**.

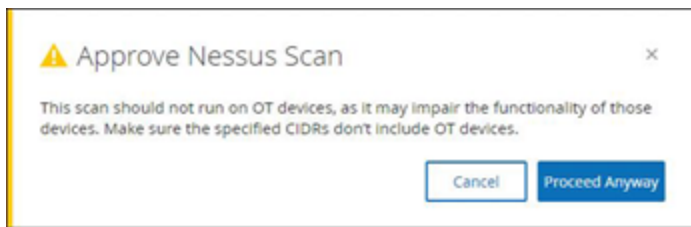
Run a Nessus Plugin Scan

To run a Nessus Plugin Scan:

1. On the **Nessus Scans** page, do one of the following:
 - Right-click the scan, then select **Run now**.
 - Select the scan you want to run, then 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 OT Security saves the scan.

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

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

4. Click **Proceed Anyway**.



OT Security now runs the scan. You can pause/resume, stop, or kill scans depending on their current status.

Network

OT Security monitors all activity in your network and shows the data on the following pages:

- **Network Summary**— Shows an overview of the network activity.
- **Packet Captures** — Shows a listing of the PCAP files captured by the system. See [Packet Captures](#).
- **Conversations** — Shows a list of all conversations detected in the network, with details about the time they occurred, involved assets, and so on. See [Conversations](#)

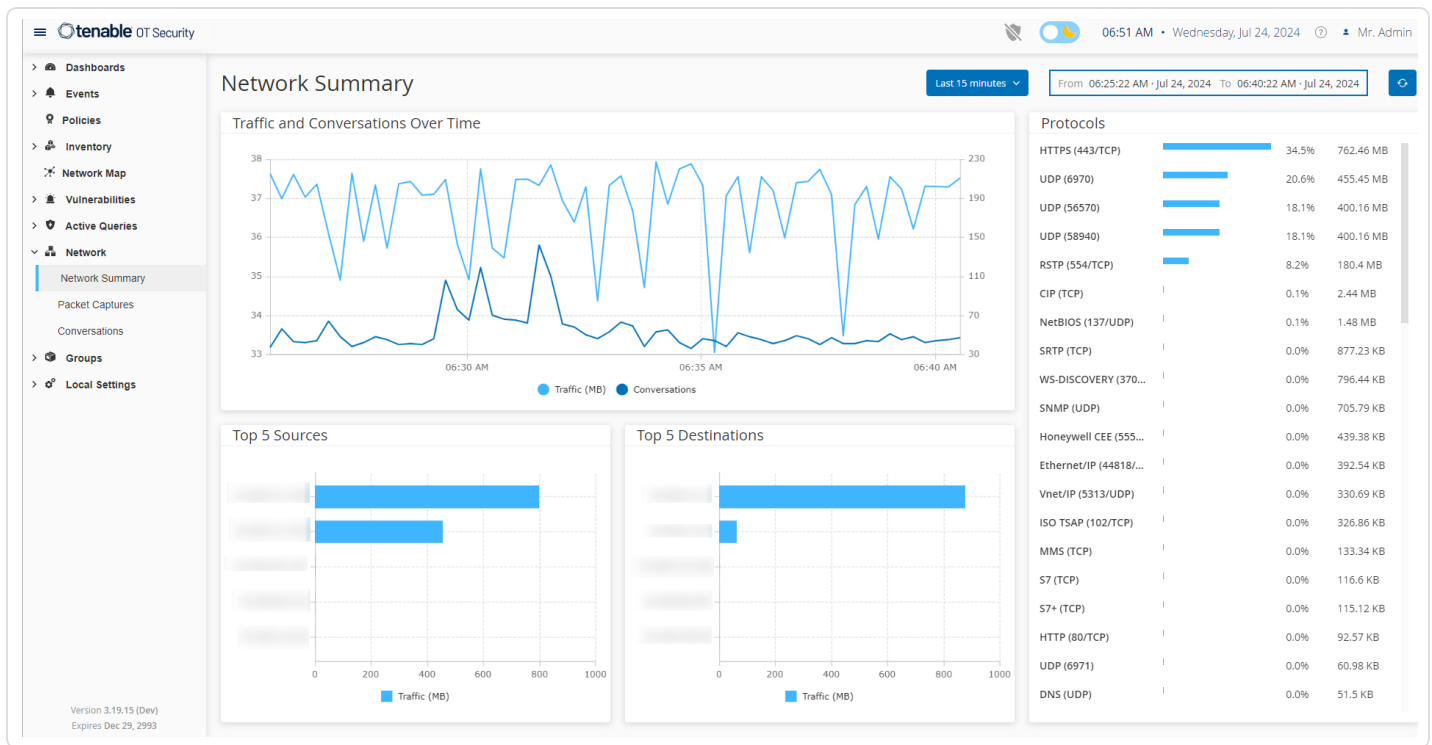
To access the **Network** page:

1. In the left navigation pane, select **Network**.

The **Network Summary** page appears.

Network Summary

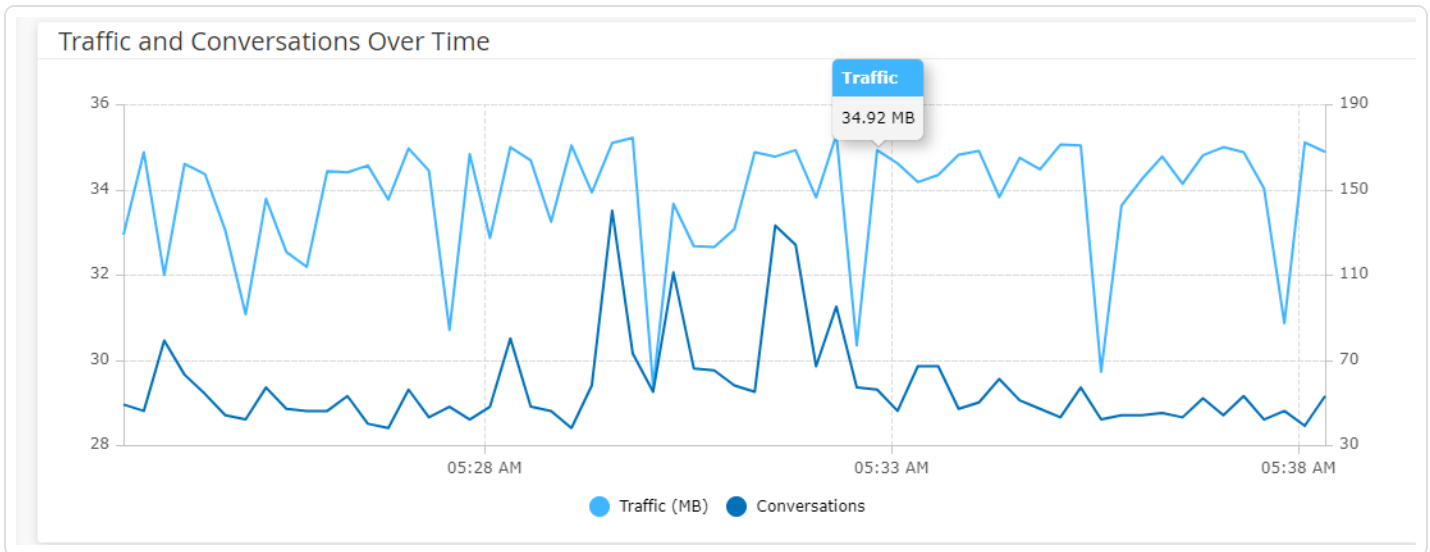
The **Network Summary** page shows visual graphs that summarize the network activity. You can view the data for a specific timeframe.



Interact with the following widgets to view additional details.

Traffic and Conversations over Time

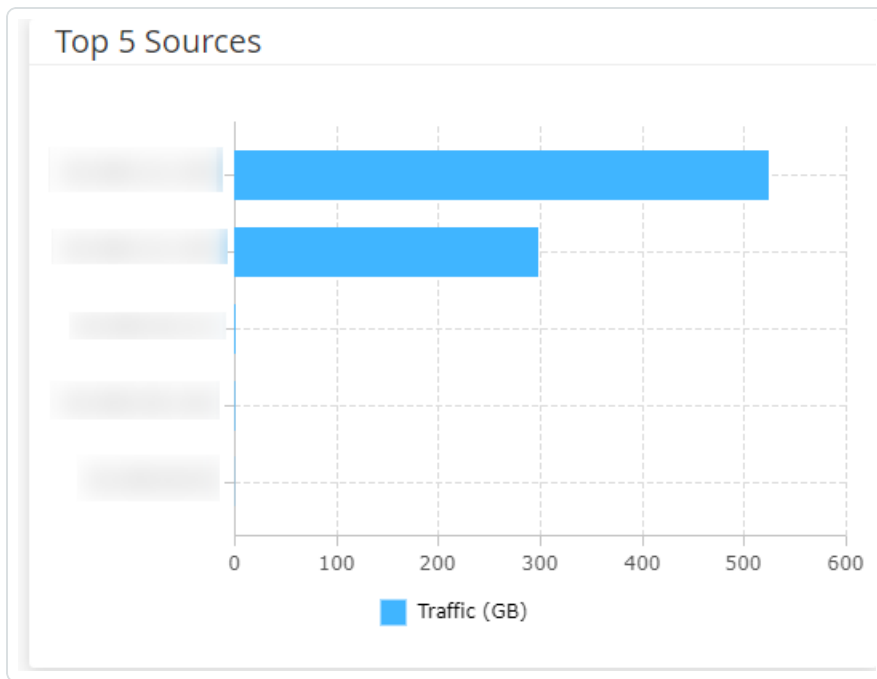
A line graph displays the volume of traffic (measured in KB/MB/GB) and the number of conversations in the network over time. The legend key appears at the top of the graph. Hover over a point on the graph to display specific data about the traffic and conversations during that time segment.



Note: The length of the time segment is adjusted according to the time scale displayed in the graph. For example, a 15-minute timeframe data shows each minute separately, while a 30-day timeframe shows the data for 6-hour segments.

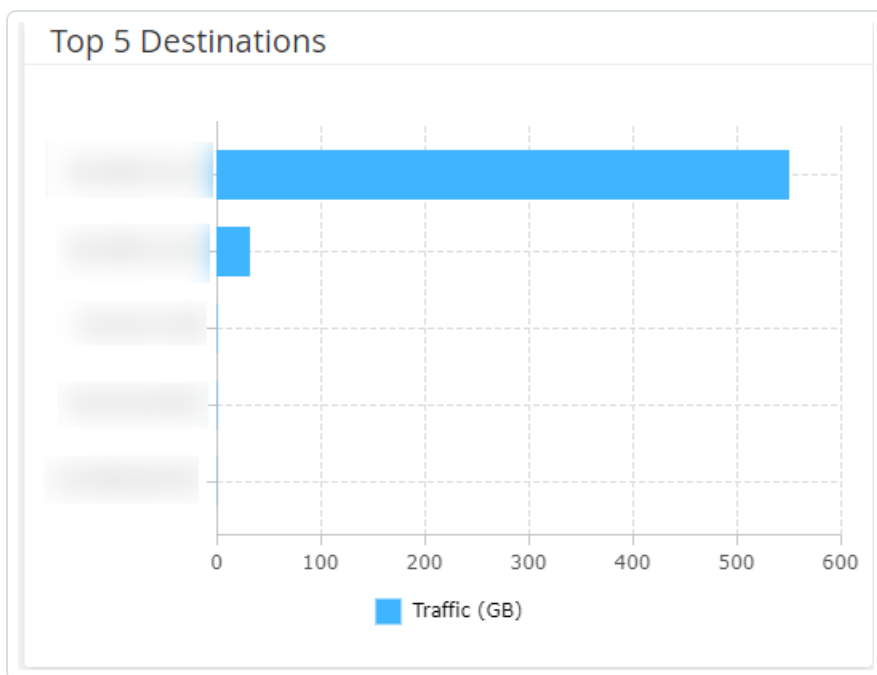
Top 5 Sources

The Top 5 Sources widget shows the number of conversations and the volume of traffic for each of the top five assets that sent communications through the network during a specific timeframe. You can identify the source assets by their IP addresses. Hover over a bar graph to see the number of conversations and volume of traffic coming from that asset.



Top 5 Destinations

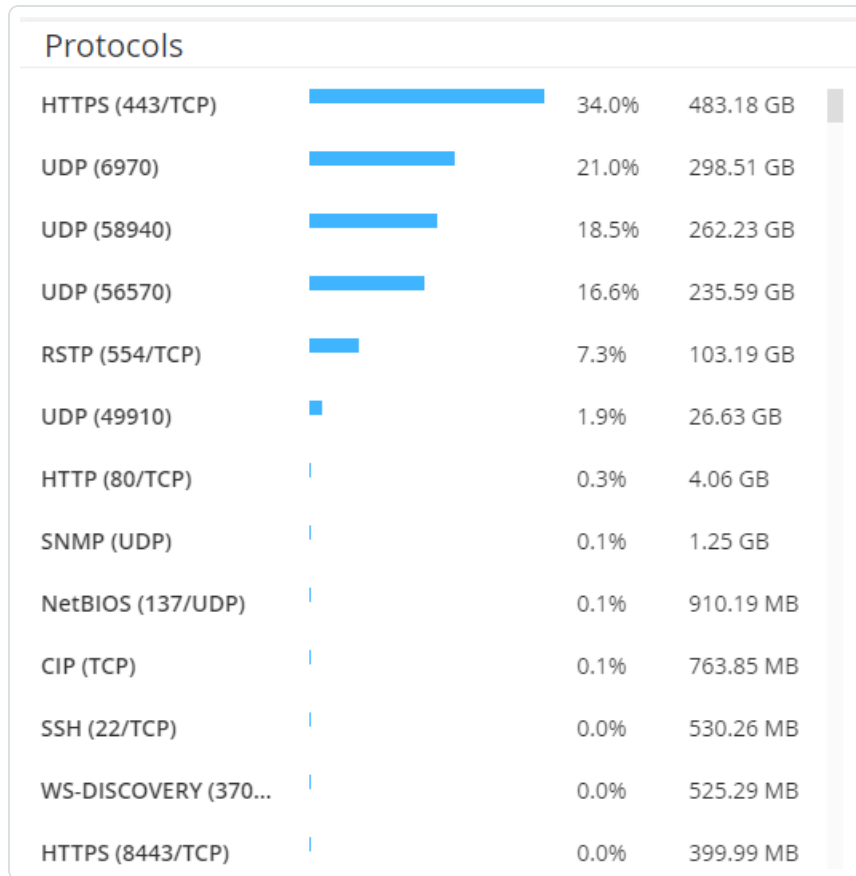
The Top 5 Destinations widget shows the number of conversations and amount of traffic for each of the top five assets that received communications through the network during the specific timeframe. You can identify the destination assets by their IP addresses. Hover over a bar graph to see the number of conversations and volume of traffic that the asset received.





Protocols

The **Protocols** widget shows data about the usage of various protocols for communication within the network during a specific timeframe.



The protocols rank from the most used (top) to least used (bottom). Each protocol shows the following information:

- A bar graph with 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.
- Percentage of usage.
- Total volume of communication.

Set the Timeframe

The **Network Summary** page displays data that represent network activity during a specific timeframe. The header bar shows the range of time for the current data display. The default

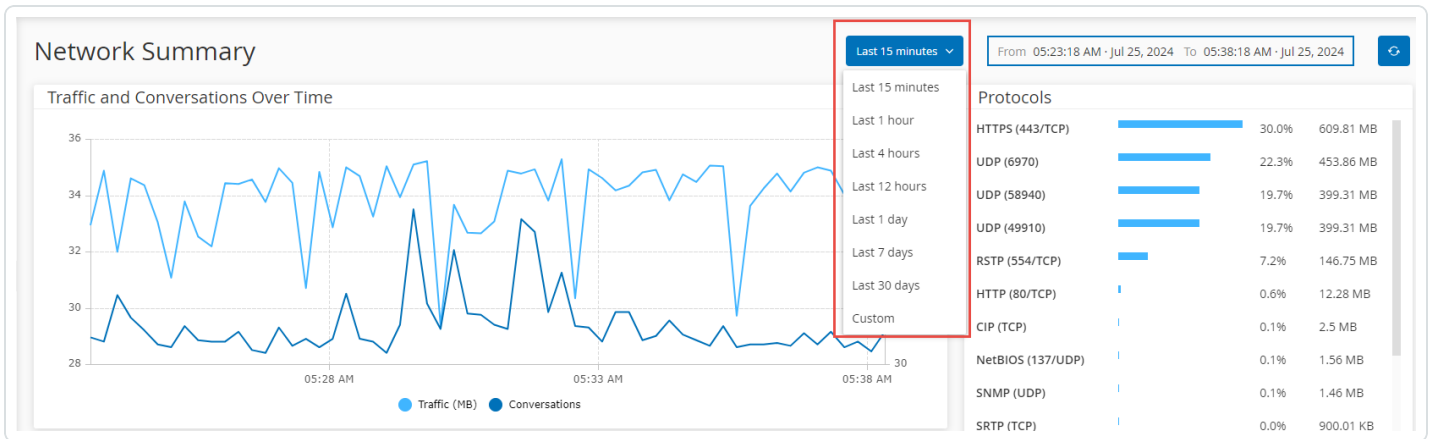


timeframe is for the **Last 15 minutes**. The header bar also shows the Start and End time of the timeframe.

To set the timeframe:

In the header bar, click the timeframe drop-down. The default is **Last 15 Minutes**.

The drop-down box lists the available options.



Select a time range using one of the following methods:

- Select a preset time range by clicking the required range. Options are: Last 15 Minutes, Last 1 Hour, Last 4 Hours, Last 12 Hours, Last Day, Last 7 Days, or Last 30 Days).
- Set a custom time range:
- Click **Custom**.

The **Custom Range** window appears.

The screenshot shows a network monitoring interface with a 'Custom Range' dialog box overlaid. The background interface includes a status bar with a shield icon, a moon icon, and the time '05:40'. Below this is a 'Custom' dropdown menu and a 'From' field showing '05:23:18 AM'. A line graph shows network activity with a peak at '05:38 AM'. A list of protocols is visible, including HTTPS (443/TCP), UDP (6970), UDP (58940), UDP (49910), RSTP (554/TCP), HTTP (80/TCP), CIP (TCP), NetBIOS (137/UDP), SNMP (UDP), SRTP (TCP), WS-DISCOVERY (370...), Honeywell CEE (555...), Ethernet/IP (44818/...), ISO TSAP (102/TCP), Vnet/IP (5313/UDP), S7+ (TCP), S7 (TCP), UDP (6971), DNS (UDP), and SNMP (161/UDP). The 'Custom Range' dialog box has the following fields:

- START DATE ***: 07/18/2024
- START TIME ***: 05:40:15 AM
- END DATE ***: 07/25/2024
- END TIME ***: 05:40:15 AM

At the bottom of the dialog box are 'Cancel' and 'Apply' buttons.

- Provide the **Start Date**, **Start Time**, **End Date**, and **End Time**.



- Click **Apply**.

After you set the timeframe, the header bar shows the start and end date/time next to the timeframe selection. OT Security refreshes the page to show data within the chosen timeframe.

Packet Captures

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

The **Packet Captures** page displays all the PCAP files in the system. The **Completed** section lists all completed files that are available for download. The **Ongoing** section shows details about the packet capture that is currently in progress.

The header bar shows the oldest captured file that is still available. It also includes an option to download files and to manually close the current Packet Capture.

Note: **Read only** and **Site Operator** roles do not have permission to stop ongoing captures or download saved packet captures.

In packet captures table, you can show or hide columns, sort, and filter the lists as well as search for keywords. For more information about customizing tables, see [Customize Tables](#).

Note: You can also download the PCAP file for an individual event from the **Events** page, see [Download Files](#).

Packet Capture Parameters

The Packet Capture list shows the following details:

Parameter	Description
Start Time	The date and time when the Packet Capture began.




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


Filter Packet Capture Display

You can filter the Packet Captures display to find a specific PCAP by providing the parameters for the start time and/or the end time.

To filter Packet Captures:

1. Go to **Network > Packet Captures**.
2. To filter by the start time, hover over **Start time** and click the  icon.

A drop-down menu appears.

1. To set the filter:
 - a. From the drop-down menu, select the required filter: **Anytime (default)**, **Started before**, or **Started after**.
 - b. If you select **Started before** or **Started after**, a window appears with the **Date** and **Time** boxes allowing you to choose the date and time.
 - c. Click **Apply**.
3. To filter by End time, hover over **End time** and click the  icon.

A drop-down menu appears.



1. To set the filter:

- a. Select required filter: **Anytime (default)**, **Ended before**, or **Ended after**.
- b. If you select **Ended before** or **Ended after**, a window appears with the **Date** and **Time** boxes allowing you to choose the date and time.
- c. Click **Apply**.

OT Security applies the filter and displays only the files generated within the specified timeframe.

Activate or Deactivate Packet Captures

You can activate or deactivate the Packet Capture feature from the **Local Settings > System Configuration > Device** .

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

The screenshot shows the 'Packet Captures' interface. At the top, there is a search bar and a status indicator 'Oldest capture file: Jul 25, 2024 06:42:16 AM'. Below this, a message box states 'Packet Capture is turned off' with a 'Turn on' button. A table below lists completed captures with columns for Start Time, End Time, Sensor, File Name, and File Size.

Start Time	End Time	Sensor	File Name	File Size
Completed (145)				
Jul 25, 2024 09:04:53 AM	Jul 25, 2024 09:05:19 AM	local_nic1	2024-07-25_09.04.53_local_nic1.pcap.gz	59.6 MB
Jul 25, 2024 09:05:19 AM	Jul 25, 2024 09:05:45 AM	local_nic1	2024-07-25_09.05.19_local_nic1.pcap.gz	120.03 MB

Important: You can activate but not deactivate the Packet Capture feature from **Network > Packet Capture**.

To activate Packet Capture:

1. Go to **Network > Packet Captures**.
2. In the **Header** bar, click **Turn on**.

OT Security starts Packet Capture.

Download Files

You can download any of the **Completed** PCAP files to your local machine. You can then analyze using Network Protocol Analysis tools such as Wireshark.



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

To download a completed file:

1. Go to **Network > Packet Captures**.
2. Select the required file from the Packet Capture lists.
3. In the **Header** bar, click **Download**.

OT Security downloads the PCAP file in a zip format to your local machine.

To manually close the current Packet Capture:

1. Go to **Network > Packet Captures**.
2. In the **Header** bar, click **Close ongoing captures**.


OT Security stops the current capture and the file becomes available for download.

OT Security automatically starts a new Packet Capture.

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** page shows a list of the current and past conversations, including detailed information about the conversations.

You can do the following actions from the **Conversations** page:

- **Search** – Use the **Search** box to search for specific conversations by providing identifying information.
- **Export** – Use the  Export button to export all data from the **Conversations** tab onto your local machine as a .csv file.

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

To access the **Conversations** page:



1. Go to **Network > Conversations**.

The **Conversations** page appears.

Start Time ↓	End Time	Duration	Bytes	Packets	Source Address	Destination Address	Protocol
Completed (10000)							
Jul 25, 2024 09:54:38 AM	Jul 25, 2024 09:54:38 AM	1 second	1042	6	10.100.16.144		HTTP (80/TCP)
Jul 25, 2024 09:54:38 AM	Jul 25, 2024 09:54:38 AM	1 second	200	3	10.100.16.144		HTTP (80/TCP)
Jul 25, 2024 09:54:37 AM	Jul 25, 2024 09:54:37 AM	1 second	54	1	10.100.111.28		CINEGRFX-LM (1743/UDP)
Jul 25, 2024 09:54:37 AM	Jul 25, 2024 09:54:37 AM	1 second	54	1	10.100.111.28		ENCORE (1740/UDP)
Jul 25, 2024 09:54:37 AM	Jul 25, 2024 09:54:37 AM	1 second	54	1	10.100.111.28		3COM-NSD (1742/UDP)
Jul 25, 2024 09:54:37 AM	Jul 25, 2024 09:54:37 AM	1 second	54	1	10.100.111.28		CISCO-NET-MGMT (1741/...

The Conversations page includes the following details:

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

Groups

Groups are the fundamental building blocks to construct Policies. When you configure a Policy, you set each policy condition using Groups instead of individual entities. OT Security comes with some predefined Groups. You can also create your own user-defined Groups. To streamline the process of editing and creating Policies, Tenable recommends that you configure the Groups you need in advance.



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

View Groups

To view groups:

1. In the left navigation bar, click **Groups**.

The **Groups** section expands to display the group types.

Name	Type	Members	Used in Policies	Used in Zones	Used in Queries
Predefined asset groups (121)					
3D Printers	Function Group				
ABB 800X Controllers	Function Group		Use of Unauthorized Protocols in ABB 800X Controllers Use of ...		
ABB Masterbus300 Controllers	Function Group				
ABB RTUS00 RTUs	Function Group				
ABB TotalFlow Controllers	Function Group				
Access Control Systems	Function Group				
Actuators	Function Group				
Any Asset	Function Group		SIMATIC Code Download SIMATIC Code Upload SIMATIC Code Delet...		Port Mapping - Continuous Port Mapping - Update Open Ports Butt...
Apogee Controllers	Function Group		Use of Unauthorized Protocols in Apogee Controllers Use of ...		
Bachmann M1 Controllers	Function Group		Use of Unauthorized Protocols in Bachmann M1 Controllers Use of ...		
Barcode Scanners	Function Group				
Beckhoff Controllers	Function Group				
Bosch PSI Controllers	Function Group		Use of Unauthorized Protocols in Bosch PSI Controllers Use of ...		
Cameras	Function Group				
CNCs	Function Group				
Cognex Cameras	Function Group				
Cognex DataMan Cameras	Function Group				

Under **Groups** you can view all Groups configured in your system. Groups are divided into two categories:

- **Predefined Groups** – These are pre-configured and you cannot edit these groups.
- **User-Defined Groups** – You can create and edit these groups.

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 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 comprises a group of related rules, 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 can use an Asset Group Controller 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.

View Asset Groups



The screenshot shows the 'Asset Groups' interface. At the top, there is a search bar and buttons for 'Actions', 'Create Asset Group', and 'Export'. Below is a table with columns: Name, Type, Members, and Used in Policies. The table is filtered to show 'Predefined asset groups (92)'. The visible rows are:

Name	Type	Members	Used in Policies
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 asset groups** tab includes groups that are built into the system, which you cannot edit, duplicate, or delete. The **User-defined asset groups** tab includes custom groups created by the user. You can edit, duplicate, or delete these groups.

The Asset Groups table shows the following information:

Parameter	Description
Status	Shows if the policy is turned on or off. If the system automatically disables the policy because it was generating too many events, then the system displays a warning icon. Toggle the status switch to turn a Policy ON/OFF.
Name	The name of the Policy.
Severity	The severity of the event. Possible values are: None, Low, Medium, or High. See section Severity Levels for more information.
Event Type	The event type that triggers this Event Policy.
Category	The category of the event that triggers this Event Policy. Possible values are: Configuration, SCADA, Network Threats, or Network Event. For an explanation of the various categories see Policy Categories and Sub-Categories .
Source	A Policy condition. The source Asset Group to which the Policy applies. An Asset group is the asset that initiated the Activity.
Name	The name to identify the Group.
Type	The Group type. Options are:



	<ul style="list-style-type: none">• Function – A predefined Asset Group created to serve a particular function.• Asset List –Specified assets are included in the Group.• IP List – Assets with the specified IP address.• IP Range – Assets within the specified range of IP addresses.
Members	<p>Shows the list of assets included in this Group. No value is shown for Function Groups.</p> <div style="border: 1px solid #0070C0; padding: 5px;"><p>Note: If there is no room to display all assets in this row then click Table Actions > View > Members tab.</p></div>
Used in Policies	<p>Shows the name of each policy that uses this Asset Group in its configuration.</p> <div style="border: 1px solid #0070C0; padding: 5px;"><p>Note: To view more details about the policies in which the Group is used, click Table Actions > View > Used in Policies tab.</p></div>
Used in Queries	<p>Shows the name of the query that uses this Asset Group.</p>

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](#).

Create Asset Groups

You can create custom Asset Groups to use when configuring 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 included in the Group.
- **IP List** – Specify the IP addresses of the Assets included in the Group.
- **IP Range** – Specify the range of IP addresses of the Assets that are included in the Group.

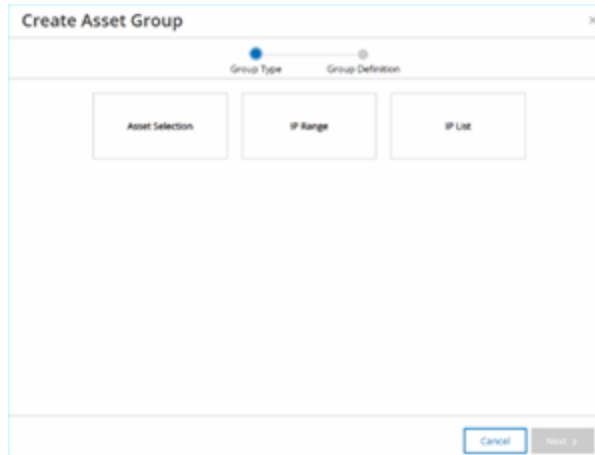
There are different procedures for creating each type of Asset Group.



To create an asset selection type asset group:

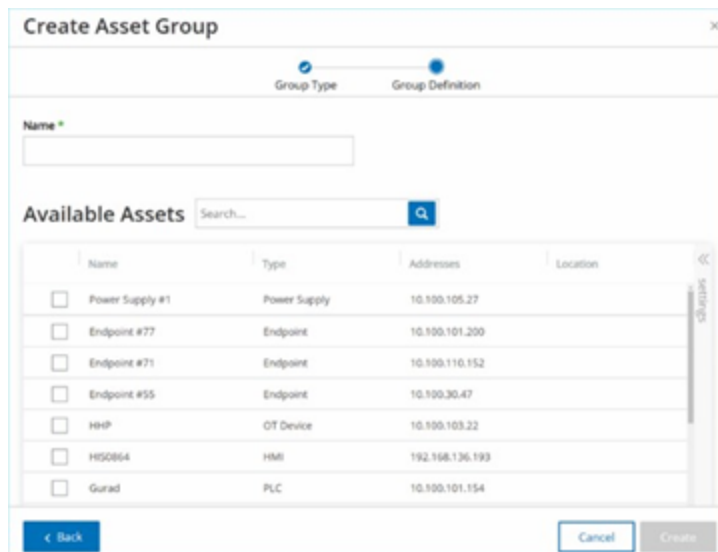
1. Go to **Groups > Asset Groups**.
2. Click **Create Asset Group**.

The **Create Asset Group** panel appears.



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

The list of **Available Assets** appears.



5. In the **Name** box, type a name for the group.



Choose a name that describes a common element that categorizes the assets included in the group.

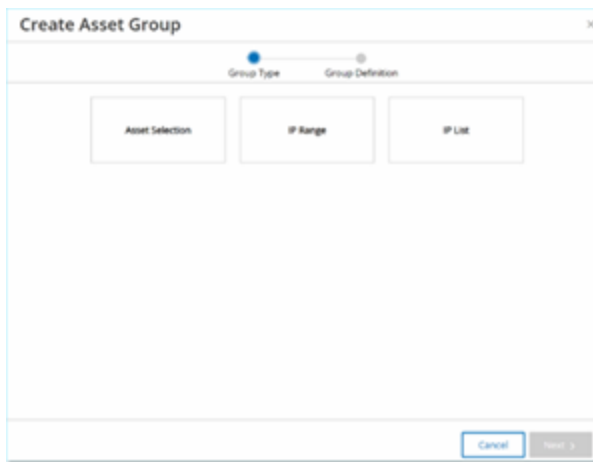
6. Select the check box next to each asset you want to include in the group.
7. Click **Create**.

OT Security creates the new asset group and displays it on the **Asset Groups** screen. You can now use this group when configuring policies.

To create an IP range type asset group:

1. Go to **Groups > Asset Groups**.
2. Click **Create Asset Group**.

The **Create Asset Group** panel appears.



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

The IP Range selection panel appears.

The screenshot shows a 'Create Asset Group' dialog box. At the top, there are two progress indicators: 'Group Type' (completed) and 'Group Definition' (current step). Below this, there are three input fields: 'Name *', 'Start IP *', and 'End IP *'. At the bottom, there are three buttons: '< Back', 'Cancel', and 'Create'.

5. In the **Name** box, type a name for the group.

Choose a name that describes a common element that categorizes the assets included in the group.

6. In the **Start IP** box, type the IP address at the beginning of the range you want to include.
7. In the **End IP** box, type the IP address at the end of the range you want to include.
8. Click **Create**.

OT Security creates the new Asset Group displays it on the **Asset Groups** screen. You can now use this group when configuring policies.

To create an IP list type Asset Group:

1. Go to **Groups > Asset Groups**.
2. Click **Create Asset Group**.

The **Create Asset Group** panel appears.

The screenshot shows a 'Create Asset Group' window. At the top, there's a progress bar with two steps: 'Group Type' and 'Group Definition'. The 'Group Definition' step is active. Below the progress bar, there's a 'Name' field with an asterisk and an empty text box. Underneath that is the 'IP List' section, which has a sub-header 'One IP or Subnet (CIDR) per line' and a large empty text area. At the bottom of the window, there are three buttons: 'Back', 'Cancel', and 'Create'.

3. Click **IP List**.

4. Click **Next**.

The **IP List** panel appears.

5. In the **Name** box, type 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, type an IP Address or a Subnet to be included in the group.

7. To add more assets to the Group, type each additional IP address or Subnet on a separate line.

8. Click **Create**.

OT Security creates the new Asset Group and displays it on the **Asset Groups** screen. You can now use this group when configuring policies.

Network Segments

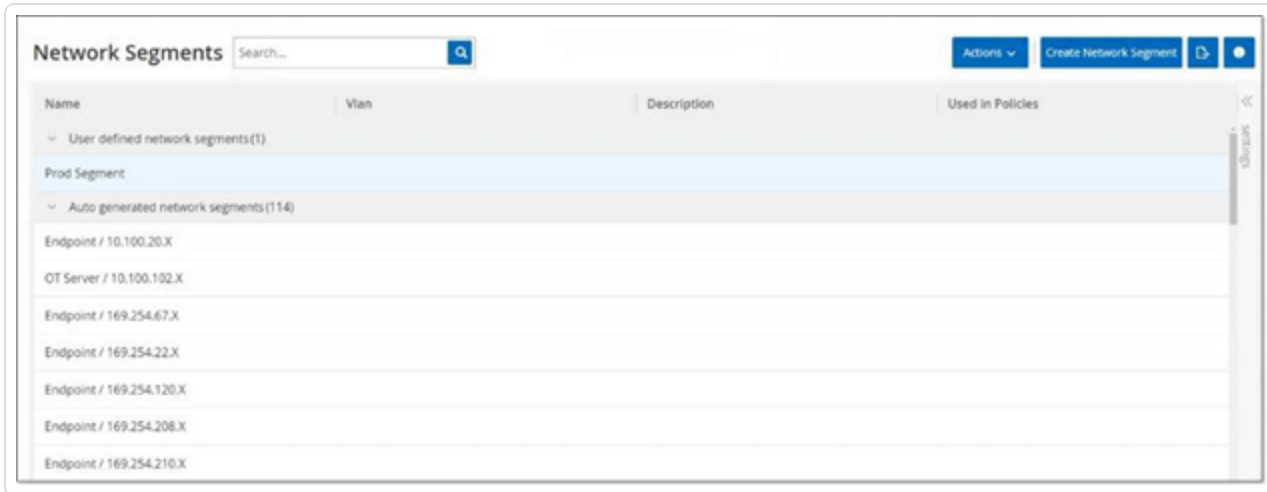
With Network Segmentation, you can create groups of related network assets, enabling you to logically isolate asset groups from one-another. OT Security automatically assigns each IP address that is associated with an asset in your network to a Network Segment. For assets with more than one IP address, each IP is associated with a Network Segment. Each auto-generated segment



includes all Assets of a specific Category (Controller, OT Servers, Network Devices, and so on) that have IPs with the same class C network address (that is, the IPs have the same first 24 bits).

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

View 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 the system automatically generates. The **User-defined** tab includes custom Network Segments created by the user.

The Network Segments table shows the following details:

Parameter	Description
Name	The name used to identify the Network Segment.
VLAN	The VLAN number of the Network Segment. (Optional)
Description	A description of the Network Segment. (Optional)
Used in Policies	Shows the names of the Policies that apply to this Network Segment. <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;">Note: To view more details about the Policies in which the Network Segment is used, click Actions > View > Used in Policies tab.</div>



You can View, Edit, Duplicate, or Delete an existing Network Segment. For more information, see [Actions on Groups](#).

Create 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. Go to **Groups > Network Segments**.
2. Click **Create Network Segment**.

The **Create Network Segment** panel appears.

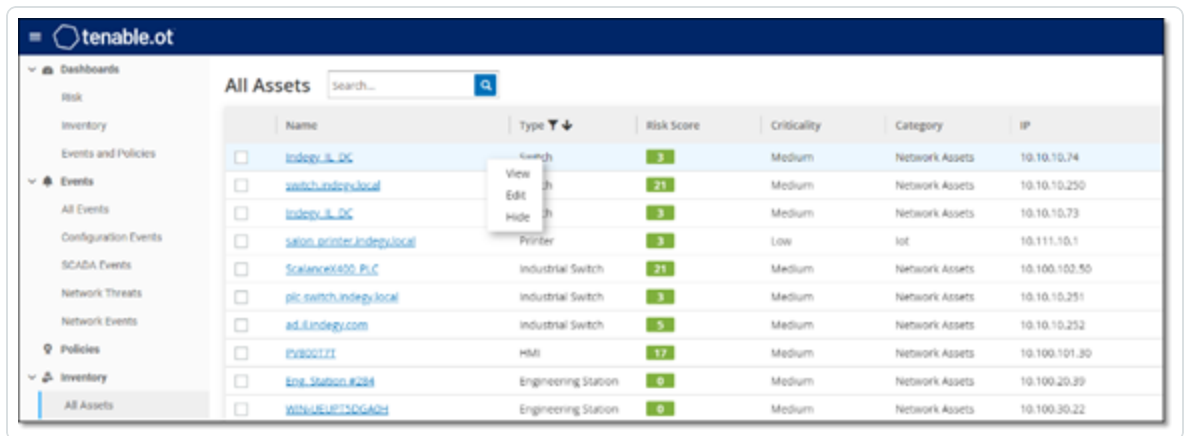
The image shows a dialog box titled "Create Network Segment" with a close button (X) in the top right corner. The dialog contains three input fields: "NAME" (with a red asterisk indicating it is required), "VLAN", and "DESCRIPTION". The "NAME" field contains the letter "I". At the bottom of the dialog, there are two buttons: "Cancel" and "Create".



3. In the **Name** box, type a name for the Network Segment.
4. (Optional) In the **VLAN** box, type a VLAN number for the Network Segment.
5. (Optional) In the **Description** box, type a description of the Network Segment.
6. Click **Create**.

OT Security creates the new Network Segment and shows it in the list of Network Segments.

7. To assign the assets to the newly created Network Segment:
 - a. Go to **Inventory > All Assets**.
 - b. Do one of the following:
 - Right-click the asset you want to assign to the newly created Network Segment and select **Edit**.
 - Hover over the asset you want to assign, then from the **Actions** menu, select **Edit**.



The **Edit Asset Details** window opens.

8. In the **Network Segments** drop-down box, select the required Network Segment.

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 required Network Segment for each one.

OT Security applies the Network Segment to the asset and shows it 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 triggered by specific Policies. For example, grouping by role, department, and so on enables you to send the notifications for specific Policy Events to the relevant parties.

View Email Groups

Name	Emails	Email Server	Used in Policies
Plant A Engineers	bob@gmail.com tim@gmail.com	Tenable	
Plant A Supervisors	laura@gmail.com juan@gmail.com	Tenable	



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

The Email Groups table shows the following information:

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

Parameter	Description
Name	The name used to identify the Group.
Emails	The list of emails included in the Group. Note: If there is no space to display all members of the Group, then click Actions > View > Members tab.
Email Server	The name of the SMTP server used to send emails to the Group.
Used in Policies	Shows the names of the Policies for which notifications are sent to this Group. Note: To view more details about the Policies in which the Group is used, click Actions > View > Used in Policies tab.

In addition, you can View, Edit, Duplicate, or Delete an existing Group. For more information, see [Actions on Groups](#).

Create 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. Go to **Groups > Email Groups**.
2. Click **Create Email Group**.



The **Create Email Group** panel appears.

The screenshot shows a 'Create Email Group' dialog box. It has a title bar with the text 'Create Email Group' and a close button (X). Below the title bar, there are three sections: 'Name' with a text input field, 'SMTP server' with a dropdown menu showing 'Select', and 'Emails' with a text area and the instruction 'One email per line'. At the bottom, there are 'Cancel' and 'Create' buttons.

3. In the **Name** box, type a name for the Group.
4. In the **SMTP server** drop-down box, select the server used for sending out the email notifications.

Note: If no SMTP server is 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** box, type the email of each member of the Group on a separate line.
6. Click **Create**.

OT Security creates the new Email Group and shows it on the **Email Groups** page. 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 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 cannot be edited or deleted but they can be duplicated.

The **User-defined** tab includes custom Groups created by the user. You can edit, duplicate, or delete these Groups.

View Port Groups

The screenshot shows a web interface titled 'Port Groups'. At the top, there is a search bar, an 'Actions' dropdown menu, and buttons for 'Create Port Group' and 'Export'. Below the header is a table with columns for 'Name', 'TCP Port', and 'Used in Policies'. A dropdown menu is open under 'Predefined port groups (39)', showing a list of groups. The 'ABB Open Ports' group is highlighted in green. Other groups listed include 'Any Port', 'Apogee Open Ports', 'Bachmann M1 Open Ports', 'CIP', 'Commonly Exploited Ports', and 'DeltaV Open Ports'.

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 View Port Groups table includes the following details:

Parameter	Description
Name	The name used to identify the Group.
TCP Port	The list of ports and/or ranges of ports that are included in the Group. Note: If the table does not display all members of the Group, you can view them on Actions > View > Members tab.
Used in Policies	Shows the name of each Policy that uses this Port Group in its configuration. Note: To view additional information about the Policies in which this Group is used, click Actions > View > Used in Policies tab.



Create Port Groups

You can create user-defined Port Groups that you can use 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. Go to **Groups > Port Groups**.
2. Click **Create Port Group**.

The **Create Port Group** panel appears.

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 red asterisk next to it, followed by an empty text input box. Below that is a "TCP Port" field with a red asterisk and the text "Port number or a range" below it. Underneath the "TCP Port" field is a blue plus sign followed by the text "Add port". At the bottom of the dialog, there are two buttons: "Cancel" and "Create".

3. In the **Name** box, type a name for the Group.
4. In the **TCP Port** box, type a single port or a range of ports to be included in the Group.
5. To add additional Ports to the Group:



- a. Click **+ Add Port**.

A new Port Selection box appears.

- b. In the new **Port number** box, type a single port or a range of ports to be included in the Group.

6. Click **Create**.

OT Security creates the new Port Group is created and shows it in the list of Port Groups. You can now use this Group when configuring Policies.

Protocol Groups

Protocol Groups are a set of protocols used for conversations between assets on a network. Protocol Groups are a Policy condition for Network Policies They also define what Protocols 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. You cannot edit or delete these Groups. 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, that is, Modbus, PROFINET, CIP and so on. You can also create your own user-defined Protocol Groups.

View Protocol Groups

Name	Protocols
Predefined protocol groups(57)	
ABB Allowed Protocols	MMS TCP1102 UDP12757 UDP12423 UDP1123 UDP12999 UDP1147 UDP1341 UDP124230 TCP180 TCP14818 MODBUS TCP502
Any Protocol	TCP UDP MODBUS UNITY CONCEPT PROFINET CIP PCCC ETHIP LLC S7 S7Plus P2 SRTF BROWSER DIG254 SICAM_PROFIBUS IEC1850 IEC104 YOKOGAWA_CENTUM BACNET LLDIP MELSEC
Apogee Allowed Protocols	P2 TCP15033 TCP169 TCP1100 TCP1135 UDP1161 - 162 TCP1001 - 3002 TCP15441 - 5442 UDP167 - 68
Bachmann M1 Allowed Protocols	PROFINET MODBUS DNP3 TCP21 TCP180 TCP1443 TCP1445 TCP502 UDP1000 TCP1050 IEC1
BACnet-IP	UDP14768 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. You cannot edit or delete these Groups, but you can duplicate them. The **User-defined** tab shows the custom Groups that you create. You can edit, duplicate, or delete these Groups.

The Protocol Groups table shows these details:

Parameter	Description
Name	The name to identify the Group.
Protocols	The list of protocols included in the Group. Note: If you are unable to view all members of the Group, then click Actions > View > Members tab.
Used in Policies	Shows the name of each Policy that uses this Protocol Group in its configuration. Note: To view additional details about the Policies in which this Group is used, click Actions > View > Used in Policies tab.

Create Protocol Groups

You can create custom Protocol Groups 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. Go to **Groups > Protocol Groups**.
2. Click **Create Protocol Group**.

The **Create Protocol Group** appears.

The screenshot shows a dialog box titled "Create Protocol Group". It features a "Name" field, a "Protocols" dropdown menu, and a "Port" field. Below the "Protocols" dropdown is a "+ Add Protocol" button. At the bottom of the dialog are "Cancel" and "Create" buttons.

3. In the **Name** box, type a name for the Group.
4. In the **Protocols** drop-down box, select a Protocol type.
5. If the selected Protocol is TCP or UDP, in the **Port** box, type a Port number or range of Ports.
For other Protocol types, you do not have to enter any value in the **Port** box.
6. To add additional Protocols to the Group:
 - a. Click **+ Add Protocol**.
A new **Protocol Selection** box appears.
 - b. Fill in the new **Protocol Selection** in the manner described in steps 4-5.
7. Click **Create**.

OT Security creates the new Protocol Group and shows 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.

View 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 schedule groups** tab includes Groups that are built into the system. You cannot edit, duplicate, or delete these Groups. The **User-defined schedule groups** tab shows the custom groups you created. You can edit, duplicate, or delete these Groups.

The Schedule Groups table shows the following details:

Parameter	Description
Name	The name to identify the Group.
Type	The Group type. Options are: <ul style="list-style-type: none">• Function – A predefined Schedule Group created to serve a particular function.• Recurring – A schedule that recurs on a daily or weekly basis. For example, a Work Hours schedule can be defined as Monday to Friday from 9 AM to 5 PM.• Interval – A schedule that occurs on a specific date or range of dates. For example, a Plant Renovation schedule can be defined by the period from June 1 to August 15.



Covers	A summary of the schedule settings. Note: If you are unable to view all members of the Group, then click Actions > View > Members tab.
Used in Policies	Shows the Policy ID of each Policy that uses this Schedule Group in its configuration. Note: To view additional details about the Policies in which this Group is used, click Actions > View > Used in Policies tab.

Create 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 with shared characteristics to highlight the events that happen during that time period.

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 9 AM to 5 PM.
- **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.

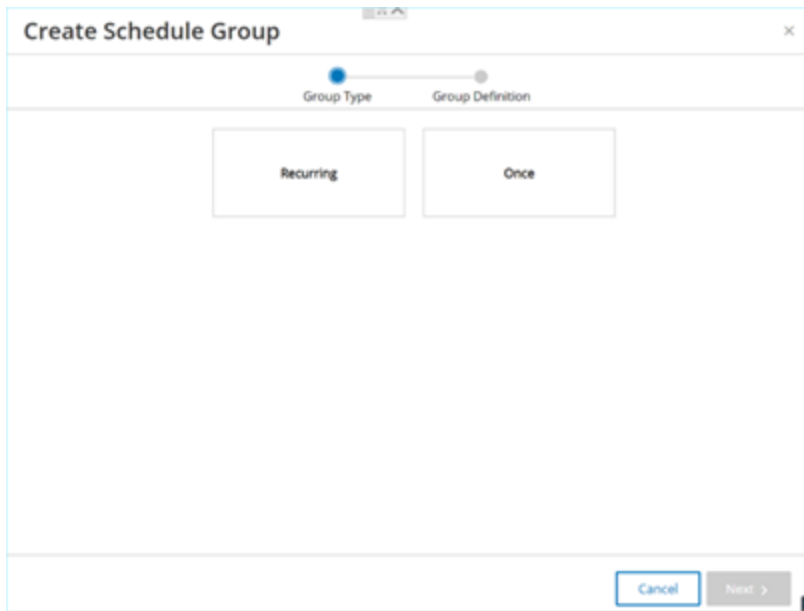
To create a Recurring Type Schedule Group:

1. Go to **Groups > Schedule Groups**.

The **Schedule Groups** page appears.

2. Click **Create Schedule Group**.

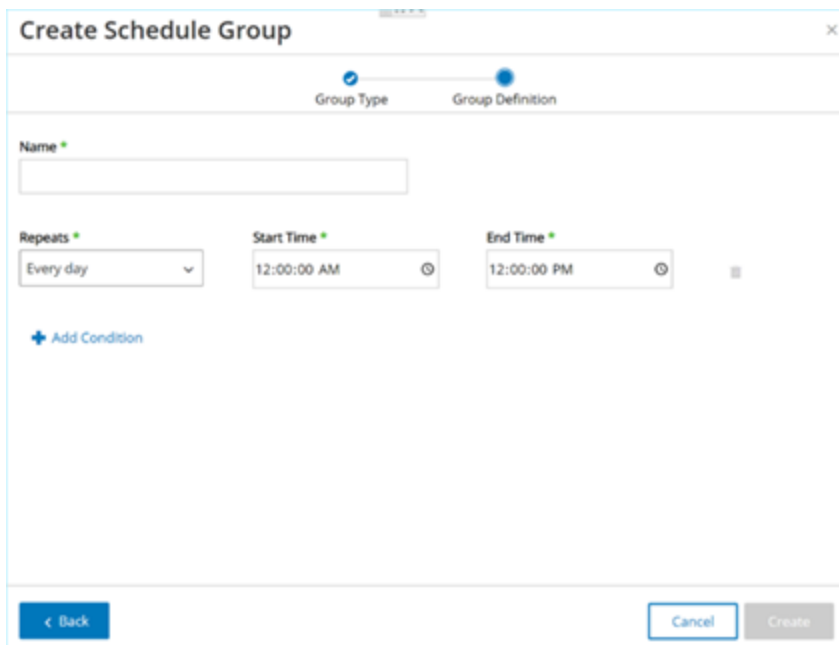
The **Create Schedule Groups** panel appears.



3. Click **Recurring**.

4. Click **Next**.

The parameters for defining a Recurring Schedule group appear.



5. In the **Name** box, type a name for the Group.

6. In the **Repeats** box, 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 want to include particular days of the week, for example Monday and Wednesday, then you need to add a separate condition for each day.

7. In the **Start Time** box, type the time of day (HH:MM:SS AM/PM) of the beginning of the time range included in the Schedule Group.
8. In the **End Time** box, type the time of day (HH:MM:SS AM/PM) of the end of the time range included in the Schedule Group.
9. To add additional Conditions (that is, additional time ranges) to the Schedule Group:
 - a. Click **+ Add Condition**.

A new row of Schedule selection parameters appears.
 - b. Fill in the schedule fields as described above in step 5-7.
10. Click **Create**.

OT Security creates the new Schedule Group and shows the list of Schedule Groups. You can now use this Group when configuring Policies.


To create a one-time Schedule Group:

1. Go to **Groups > Schedule Groups**.
2. Click **Create Schedule Group**.


The **Create Schedule Group** wizard appears.

3. Select **Time Range**.
4. Click **Next**.

The parameters for defining a time range schedule group appear.

5. In the **Name** box, type a name for the Group.
6. In the **Start Date** box, click 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** box, type 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** box, click 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** box, type the time of day (HH:MM:SS AM/PM) of the end of the time range included in the Schedule Group.
 12. Click **Create**.



OT Security creates the new Schedule Group and shows it 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 can be harmful to the furnaces.

View Tag Groups

Name ↑	Type	Controller	Tags	Used in Policies
User defined tag groups (2)				
demo1	Bool	Rouge	Rouge - MainTask/MainProgram/BR1(Bool) Rouge - MainTask/MainProgram/BR2(Bool) Rouge - ...	
demo2	Float	SIMATIC 300(1)	SIMATIC 300(1) - DB1/109(Float) SIMATIC 300(1) - DB1/111(Float) SIMATIC 300(1) - DB1/116(Float) SIMATIC...	

The **Tag Groups** page shows all tag groups currently configured in the system.

The Tag Groups table shows the following details:

Parameter	Description
Name	The name 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.

Note: If you are unable to view all Tags in this row, then click **Actions > View >**



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

You can View, Edit, Duplicate, or Delete an existing Group, see [Actions on Groups](#).

Create 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 cannot be set to detect specific values.

You can edit, duplicate, or delete Tag Groups.

To create a new tag group:

1. Go to **Groups > Tag Groups**.
2. Click **Create Tag Group**.

The **Create Tag Group** panel appears.



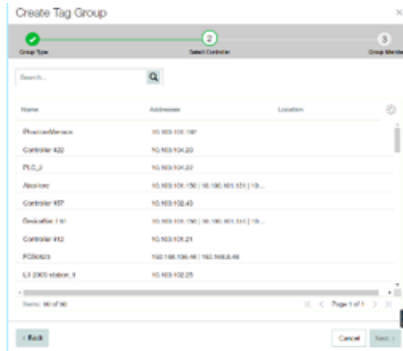
3. Select a Tag type.

Options are: Bool, Dint, Float, Int, Long, Short, or Any Type (which can include Tags of different Types).



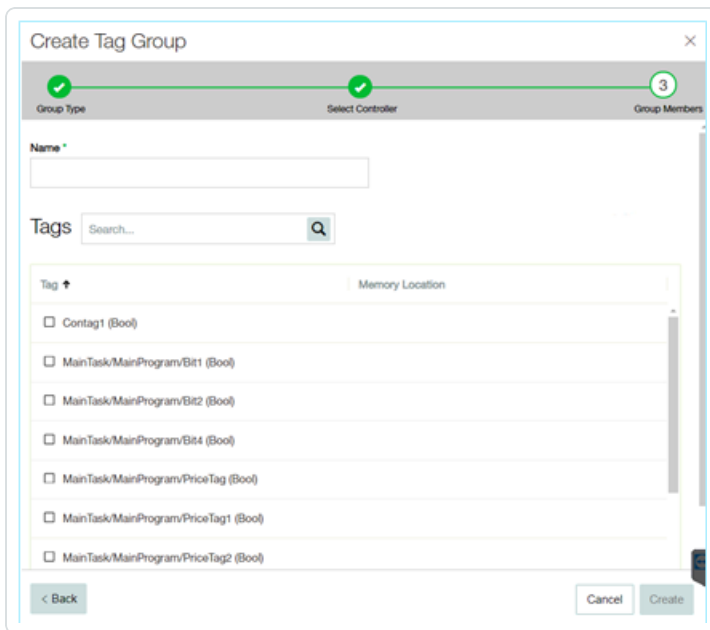
4. Click **Next**.

A list of controllers in your network appears.



5. Select a controller for which you want to include Tags in the Group.
6. Click **Next**.

A list of Tags of the specified type on the specified controller appears.



7. In the **Name** box, type a name for the Group.
8. Select the check box next to each of the Tags that you want to include in the Group.
9. Click **Create**.



OT Security creates the new Tag Group and shows in the list of Tag Groups. You can now use this Group when configuring SCADA Event Policies.

Rule Groups

Rule Groups comprise a group of related rules, 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.

View Rule Groups

The screenshot shows the 'Rule Groups' interface with a search bar and buttons for 'Actions', 'Create Rule Group', and 'Export'. The table below lists predefined rule groups with their names, the number of rules, and the policies they are used in.

Name ↑	Number of Rules	Used in Policies
Predefined rule groups (65)		
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. You cannot edit, duplicate, or delete these groups. The **User-defined** tab shows the custom Groups created by the user. You can edit, duplicate, or delete these groups.

The Rule Groups table shows the following details:

Parameter	Description
Name	The name used to identify the Group.



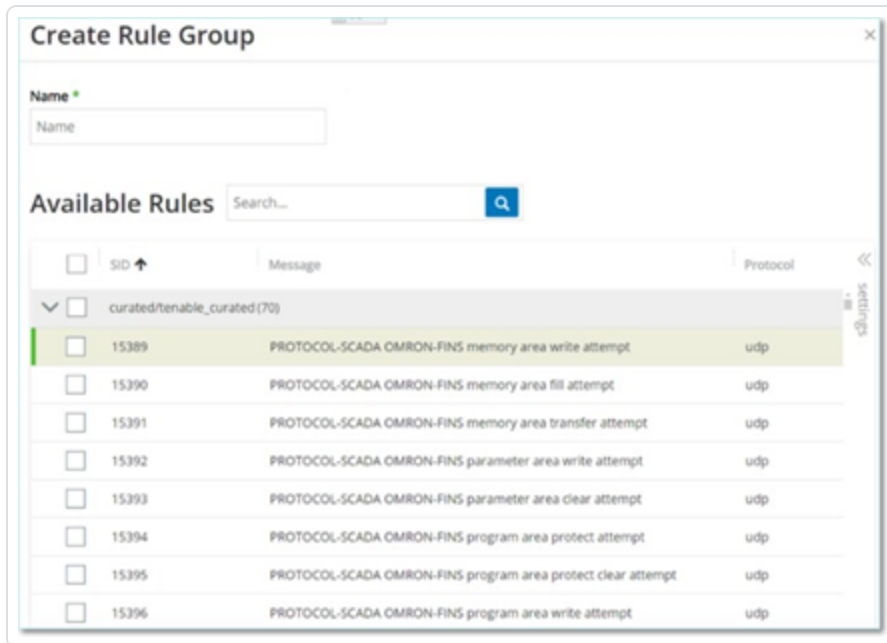
Number of Rules	The number of rules (SIDs) that comprise this Rule Group.
Used in Policies	Shows the Policy ID of each Policy that uses this Rule Group in its configuration. <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;">Note: To view additional details about the Policies in which this Group is used, click Actions > View > Used in Policies tab.</div>

Create Rule Groups

To create a new Rule Group:

1. Go to **Groups > Rule Groups**.
2. Click **Create Rule Group**.

The **Create Rule Group** panel appears.



3. In the **Name** box, type a name for the group.
4. In the **Available Rules** section, select the check box next to each of the rules you want to include in the group.



Note: Use the search box to find the desired rules.

5. Click **Create**.

OT Security creates the new Rule Group and shows it in the list of Rule Groups. You can now use this Group when configuring Intrusion Detection Policies.

Actions on Groups

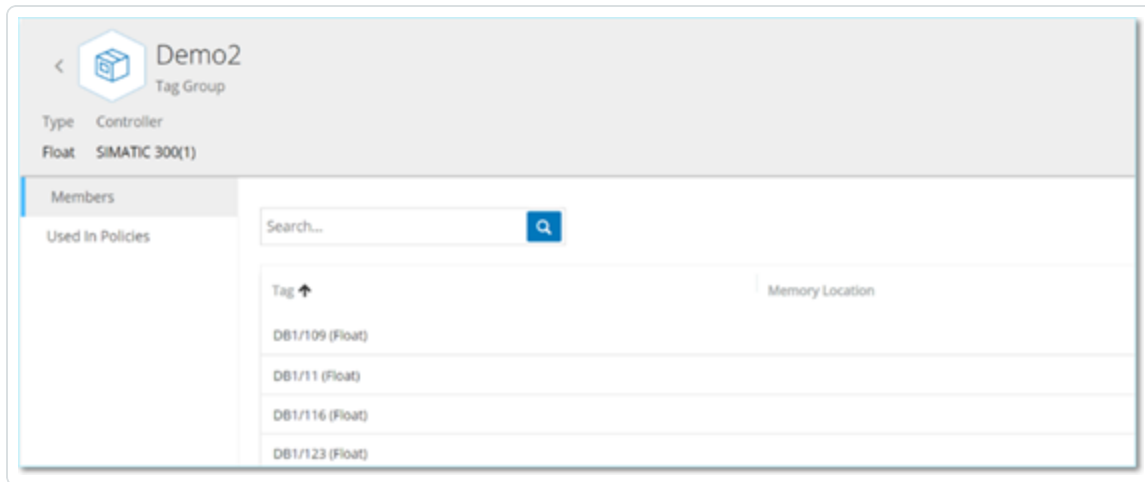
When you select a Group on any of the Group screens, you can do the following from the **Actions** menu on the top of the screen:

- **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. See [View Group Details](#)
- **Edit** – Edit details of the Group. See [Edit a Group](#)
- **Duplicate** – Create a new Group with a similar configuration to the specified Group. See [Duplicate a Group](#)
- **Delete** – Delete the Group from the system. See [Delete a Group](#)

Note: You cannot edit or delete predefined Groups. Some predefined Groups also cannot be duplicated. You can also access the **Actions** menu by right-clicking a Group.

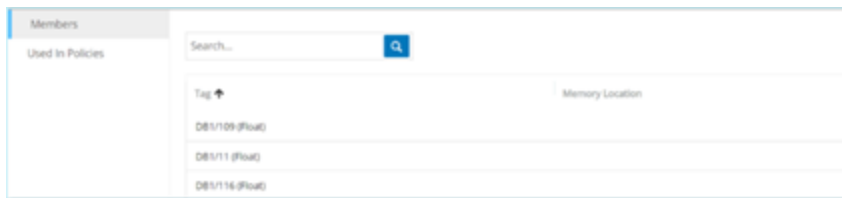
View Group Details

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



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

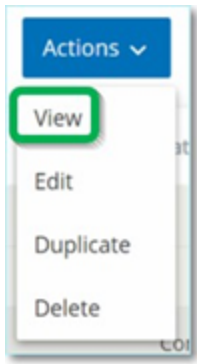
- **Members** – Shows a list of all members of the Group.



- **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. For more information, see [View Policies](#).

To view details of a Group:

1. In **Groups**, select the required type of Group.
2. Do one of the following:
 - Click **Actions**.
 - Right-click the required group.
A menu appears.
3. Select **View**.



The Group details screen appears.

Edit a Group

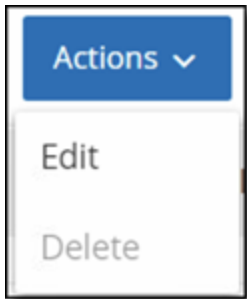
You can edit the details of an existing Group.

To edit details of a Group:

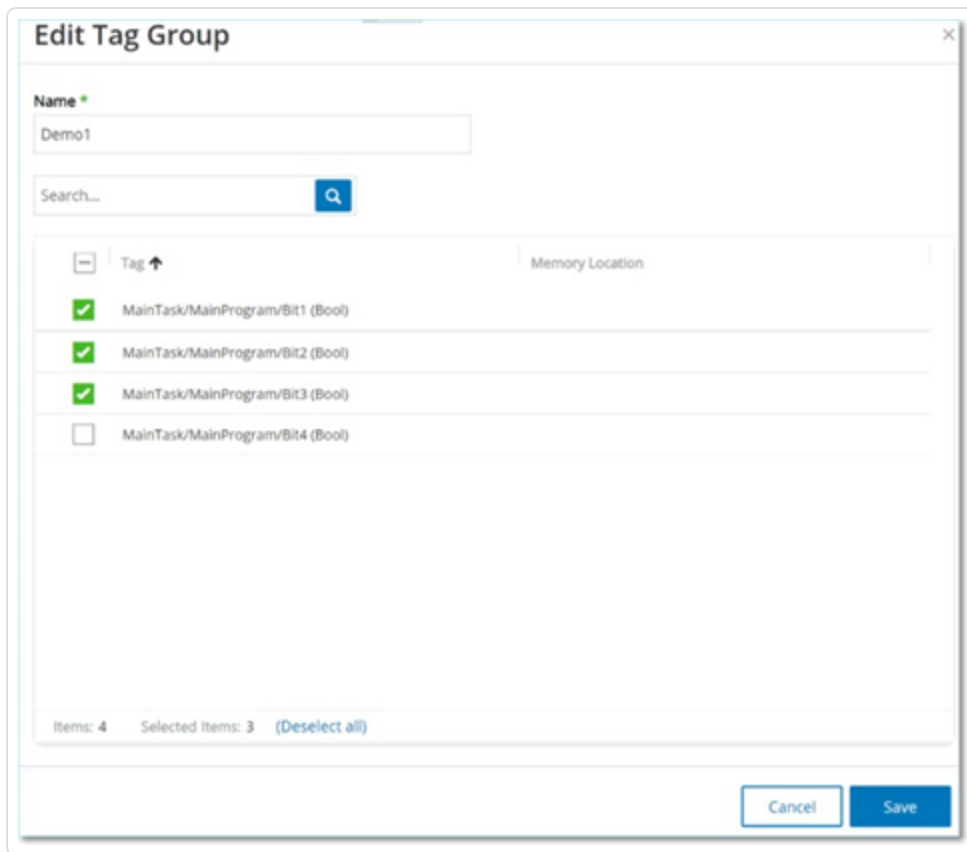
1. Under **Groups**, select the desired type of Group.
2. Do one of the following:
 - Click **Actions**.
 - Right-click the required group.

A menu appears.

3. Select **Edit**.



4. The **Edit Group** window appears, showing the relevant parameters for the specified Group type.



5. Modify as needed.

6. Click **Save**.

OT Security saves the group with the new settings.

Duplicate a Group

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.

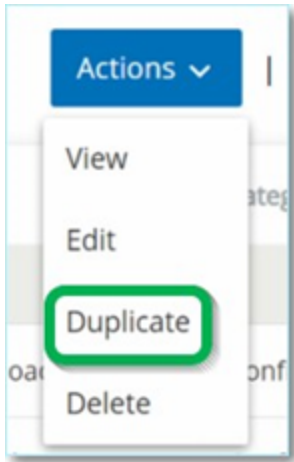
To duplicate a Group:

1. Under **Groups**, select the desired type of Group.
2. Select the existing Group on which you want to base the new Group.
3. Do one of the following:

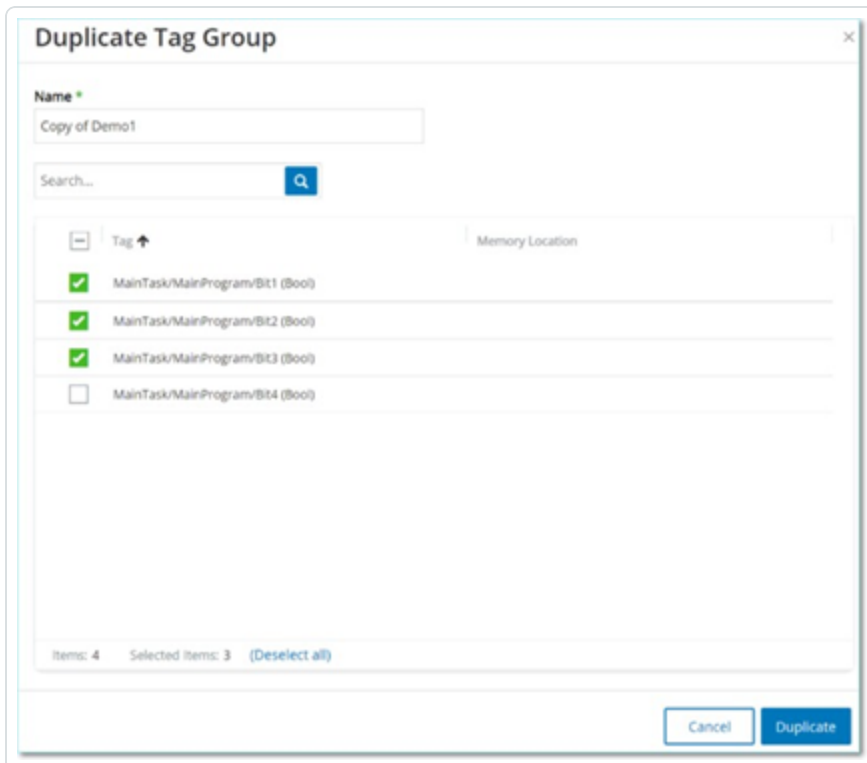
- Click **Actions**.
- Right-click the required group.

A menu appears.

4. Select **Duplicate**.



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





5. In the **Name** box, type 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**.

OT Security saves the new Group with the new settings, in addition to the existing Group.

Delete a Group

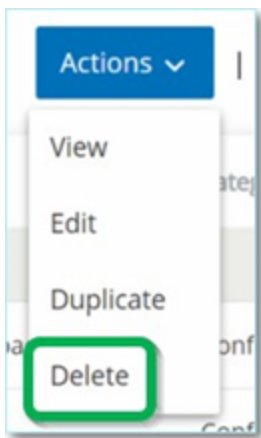
You can delete user-defined Groups but not predefined Groups. You cannot delete a user-defined policy, if it is being used as a policy condition for one or more Policies.

To delete a Group:

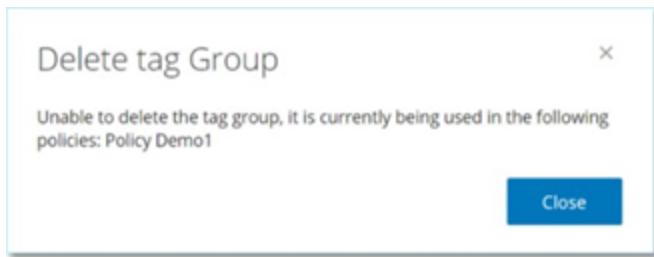
1. Under **Groups**, select the required type of Group.
2. Select the Group that you want to delete.
3. Do one of the following:
 - Click **Actions**.
 - Right-click the required group.

A menu appears.

4. Select **Delete**.



A confirmation window appears.



5. Click **Delete**.

OT Security permanently deletes the group from the system.



Local Settings

The **Local Settings** section in OT Security includes most of the configuration pages for OT Security. The following pages are available under **Local Settings**:

Active Queries – Activate/deactivate query functions and adjust their frequency and settings. See [Active Queries](#).

Sensors – View and manage sensors, approve or delete incoming Sensor pairing requests, and configure Active Queries performed by Sensors. See [Sensors](#).

System Configuration

- **Device** – View and edit device details and network information. For example, system time, automatic logout (that is, inactivity timeout).

Note: You can configure DNS servers in Tenable Core. For more information, see [Manually Configure a Static IP Address](#) in the Tenable Core + Tenable OT Security User Guide.

- **Port Configuration** – View how the ports on the device are configured. For more information on Port Configuration, see [Device](#).
- **Updates** – Perform updates of plugins either automatically or manually through the cloud, or offline.
- **Certificate** – View information about your HTTPS certificate and ensure a secure connection by either generating a new HTTPS certificate in the system or uploading your own. See [System Configuration](#).
- **API Keys** – Generate API keys to enable third-party apps to access OT Security via API. All users can create API keys. The API key has the same permissions as the user that created it, according to their role. An API key is shown once, when it is first generated; you 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. See [Monitored Networks](#).
- **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. See [Add Assets Manually](#).

Note: The maximum number of IP ranges that can be sent to the Tenable Nessus Network Monitor is 128, therefore Tenable recommends 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 is classified as an asset.

- **Hidden Assets** – View a list of hidden assets in the system. These are assets removed from the asset listings, see [Inventory](#). You can restore hidden assets from this page.
 - **Custom Fields** – Creates custom fields to tag assets with relevant information. The custom field can be plain text or it can be a link to an external resource.
 - **Event Clusters** – Allows you to cluster together multiple similar events that occur within a designated time range for monitoring them. See [Event Clusters](#).
 - **PCAP Player** – Allows 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 administrator user can create local user accounts for specific users and assign a role to the account, see [User Management](#).
 - **User Groups** – An administrator user can view, edit, add, and delete user groups. See [User Management](#).



- **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 [User Management](#).
- **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 available 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 you 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** – Starting in 3.18, you can take a backup and restore your OT Security using the **Backup/Restore** page in Tenable Core. For more information, see [Application Data Backup and Restore](#). To restore using CLI, see [Restore Backup Using CLI](#).
 - **Export Settings** – Export OT Security platform configuration settings as an .ndg file to the local computer. This serves 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 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.

Caution: This operation cannot be undone and all data in the system will be lost.

- **System Log** – Shows a log of all system events that occurred in the system. For example, Policy turned on, Policy edited, Event Resolved, and so on. You can export the log as a CSV file or send it to a Syslog server. See [System Log](#).

Sensors

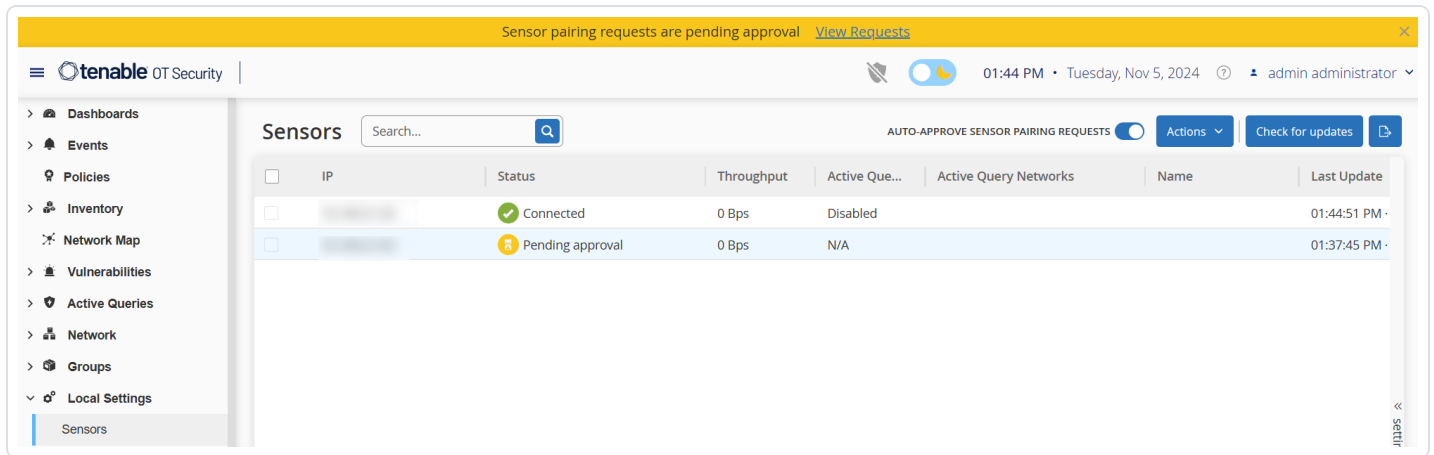
After sensors are paired using the Tenable Core user interface, you can approve new pairings, view, and manage sensors using the **Edit**, **Pause**, and **Delete** functions in the **Actions** menu. You can also choose to enable automatic approval for sensor pairing requests using the **Auto Approve Sensor Pairing Requests** toggle.

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

Note: You can pair an unlimited number of sensors with ICP, but there's a cap on the total combined SPAN (Switched Port Analyzer) traffic volume per appliance. For instance, you could have 10 sensors, each transmitting between 10 Mbps to 20 Mbps, but the overall traffic must not exceed the ICP's limit. For more information, see the [System and License Requirements](#) in the Tenable Core + OT Security User Guide.

View Sensors

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



The Sensors table includes the following details:

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

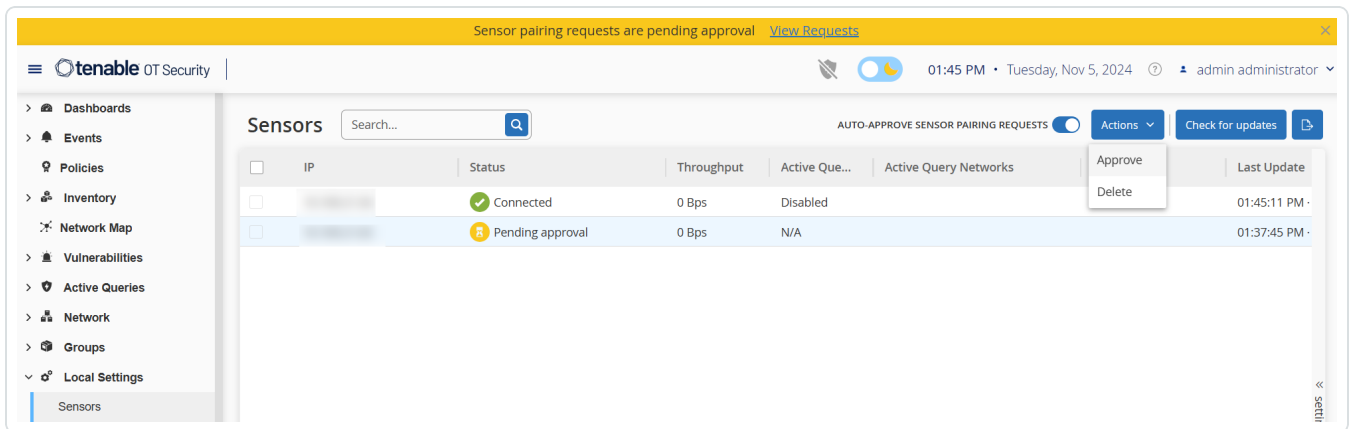
Manually Approve Incoming Sensor Pairing Requests



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 **Local Settings > Sensors**.
2. Click a row in the table with a status of **Pending Approval**.
3. Click **Actions > Approve**, or from the right-click menu, select **Approve**.



Note: To delete a sensor, click **Actions > Delete**, or right-click and select **Delete**.

Configure Active Queries

Once a sensor is connected in the 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 queries.

Note: Sensors 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 a row in the table with a status of **Connected**.
3. Click **Actions > Edit**, or right-click and select **Edit**.



The **Edit Sensor** panel is displayed.

Edit Sensor ×

NAME
Test3

Active Query Networks
ONE CIDR PER LINE

Sensor active queries

Cancel Save

4. To rename the Sensor, edit the text in the **Name** box.
5. In the **Active Query Networks** box, add or edit relevant network segments to which the Sensor sends 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. Click the **Sensor active queries** toggle to enable active queries.
7. Click **Save**.

The panel closes. In the **Sensors** table, in the **Active Queries** column, the enabled sensors now display **Enabled**.

Update Sensors



Starting from version 3.16, OT Security Sensor receives software and security updates from the ICP that manages it. Once a sensor is paired with authentication, it relies on the site to provide any OS and software updates necessary. The sensor only needs to reach OT Security for receiving software updates. OT Security allows you to update all your sensors from the centralized **Sensors** page.

If the sensor requires an update, you receive an alert during the following:

- Startup.
- Pairing completion between sensor and ICP.
- Periodic check.
- Using the **Check for updates** option.

Note: The sensor must be paired to OT Security with authentication for updating remote sensors. For more information on pairing, see [Pairing Sensors with ICP](#).

To update authenticated sensor version 3.16 or later with the ICP:

1. Go to **Local Settings > Sensors**.

The **Sensors** page appears.

2. Check the **Version** column to see if the version is up to date or if it needs an update.
3. If the version needs an update, do one of the following:

To update a single sensor:

- Right-click the required sensor and select **Update**.
- Select the checkbox next to the required sensor, then from the **Actions** menu, select **Update**.

To update multiple sensors:

- Select one or more sensors that requires an update, then from the **Actions** menu, select **Update**.

OT Security updates the selected sensors.

Note: During the update, the sensor may be unavailable.



System Configuration

The OT Security **System Configuration** pages allow 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

The **Device** page shows detailed information about your OT Security configuration. You can view and edit the configuration in this page.

The screenshot shows the 'Device' configuration page in a web interface. On the left is a navigation sidebar with categories: Dashboards, Events, Policies, Inventory, Network Map, Vulnerabilities, Active Queries, Network, Groups, Local Settings, and System Configuration. Under 'System Configuration', 'Device' is selected. The main content area is titled 'Device' and contains several configuration sections, each with an 'Edit' button:

- Device Name:** The name of Tenable OT Security management system. Input field contains 'DEVICE NAME'.
- Device URLs:** Device URLs allows you to set multiple URLs from which the system can be accessed (FQDN/IP) in addition to the locally configured IP addresses. (Change requires restart).
- System Time:** Determines the time of the Tenable OT Security 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). Input field shows 'MANUAL SYSTEM TIME' and 'Feb 9, 2024 06:21:14 AM'.
- Timezone:** Determines the time zone for the Tenable OT Security system. Time zone, together with the system time, determines the displayed time of alerts, activities, system log events and all other time-related features. Input field shows 'TIMEZONE' and 'Etc/UTC'.
- Maximum Login Session Timeout:** Determines the session period after which logged in users will be logged out automatically and required to log in again. (Requires logout). Input field shows 'LOGOUT AFTER' and '2 Weeks'.
- Maximum Inactivity Timeout:** (Partially visible at the bottom).

At the bottom left of the page, it says 'Version Mixed Build Expires Dec 29, 2993'.



Device Name

A unique identifier for the OT Security appliance.

Device URLs

Allows you to set the single URL from which the system can be accessed (FQDN).

Important: Editing the Device URL is a critical change. The new FQDN is not presented again. Failure to make note of the exact string makes the user interface inaccessible. Make sure to verify the resolution before proceeding.

System Time

The correct time and date are set automatically, but you can edit it.

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

Timezone

Select the local time zone at the site location from the drop-down list. To change the timezone, click **Edit**

Maximum Login Session Timeout

The session period after which users are logged out automatically and are required to log in again. To change the login session timeout period, click **Edit**. Available options for the time period: 2 weeks, 30 minutes, 1 hour, 4 hours, 12 hours, 1 day, 1 week, and 2 weeks.

Maximum Inactivity Timeout

The inactivity period after which logged in users are logged out automatically and required to log in again. To change the inactivity period, click **Edit**.

Open Ports Age Out Period

Determines the period after which Open Port listings are 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, click the **Ping Requests** toggle to enable ping requests.

Packet Capture

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 exceeds 1.8 TB, the system deletes older files. You can view and download available files from the **Network > Packet Captures** page, see section [Network](#).

To activate packet captures, click the **Packet Capture** toggle to enable packet captures.

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 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, click the **Auto Approve Incoming Sensor Pairing Requests** toggle to enable automatic approval.

Classification Banner

Add a banner to OT Security to indicate the data accessible via the software.

To add a banner, click **Edit**. After adding the banner, click to enable the **Classification Banner** toggle.

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 telemetry collection, click the **Enable Usage Statistics**.

Note: You can disable sharing of usage statistics at any time by clicking the toggle switch.

GraphQL Playground

An in-browser GraphQL IDE. Enable or disable this toggle to use the playground in production to test your API queries.

Port Configuration

The **Port Configuration** page shows how the ports on the device are configured. For more information on Port Configuration, see [Device](#).

The screenshot shows the 'Port Configuration' page. At the top, there is a title 'Port Configuration' and an 'Edit' button. Below the title, a note states: 'You can separate the Tenable.ot management interface from the Queries interface. (Change requires restart)'. The main content area is divided into four columns, each with a port icon and a label: 1. 'Queries + Management', 2. 'Mirror Port', 3. 'Reserved', and 4. 'Reserved'. Below this, there is a section for 'Queries IP configuration' with a table showing the following details:

Queries IP configuration	
IP	10.100.20.87
SUBNET MASK	255.255.255.0
GATEWAY	10.100.20.1

Set Compliance Dashboard Preferences

You can specify the security frameworks that the **Compliance** dashboard refers to when generating the data in the [widgets](#).

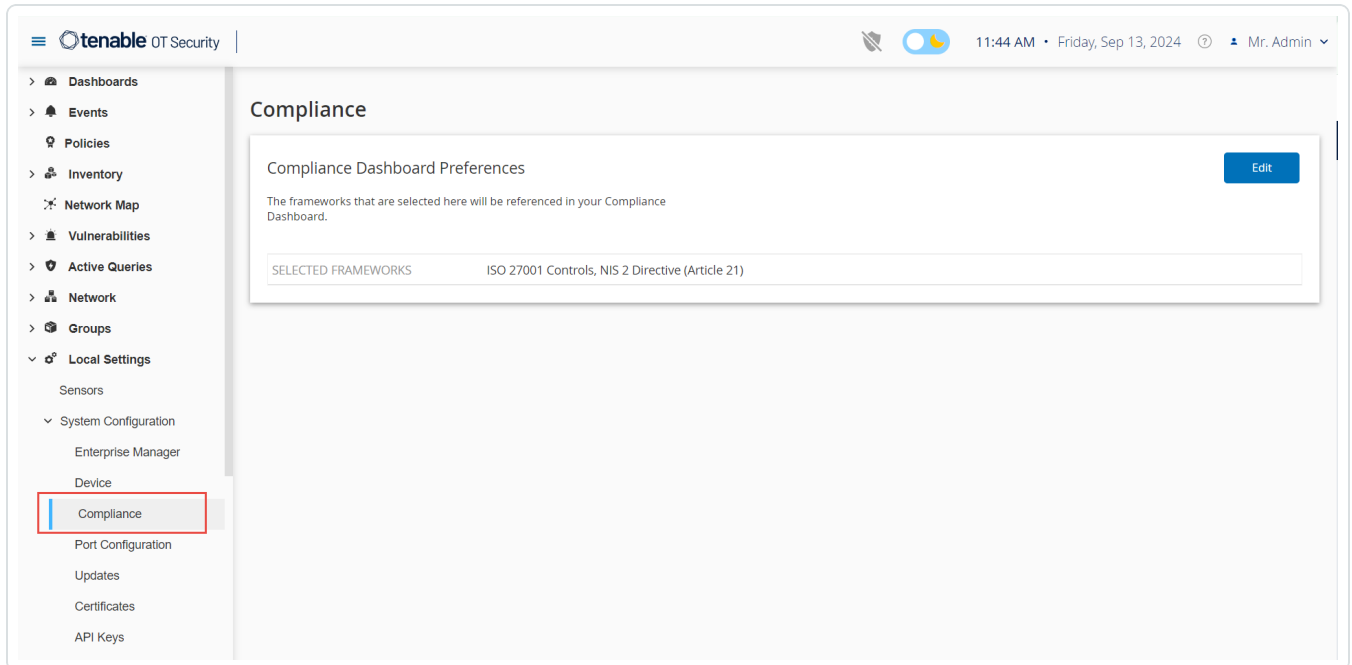
To set the compliance dashboard preferences:



1. Do one of the following:

- Go to **Local Settings > System Configuration > Compliance**.
- On the **Compliance** dashboard page, click the **Security Framework Preferences** link.

The **Compliance** preferences page appears.



2. In the **Compliance Dashboard Preferences** section, click **Edit**.

The **Edit Referenced Compliance Frameworks** pane appears.

3. Select the required compliance frameworks. You can choose from the following options.

- **ISO 27001 Controls**
- **CAF Principles**
- **OTCC Sub Domains**
- **NIS2 Directive (Article 21)**

4. Click **Save**.

OT Security saves the compliance framework preferences and checks your organization's compliance against the specified preferences. OT Security displays the results from the compliance checks on the [Compliance dashboard](#).



Updates

Updating Tenable Nessus plugins and Intrusion Detection System (IDS) Engine Ruleset to the latest versions ensures that OT Security monitors your assets for the all the latest known vulnerabilities. OT Security provides an option to update classification, family, coverage and so on through the Dynamic Fingerprinting Engine (DFE) Cloud Updates. You can perform updates through the cloud, both automatically and manually, and offline as well.

Note: For information about updating Tenable Core, see [Manage Updates](#) in the Tenable Core + OT Security User Guide.

Updates

Nessus Plugin Set Cloud Updates Update from File Edit Frequency Update Now

FREQUENCY	Every day at 02:00 AM
LAST UPDATED	
PLUGIN SET	202405270731

IDS Engine Ruleset Cloud Updates Update from File Edit Frequency Update Now

FREQUENCY	Every week on Monday and Thursday at 02:00 AM
LAST UPDATED	10:26:53 AM · May 29, 2024
RULE SET	202405282239

DFE Cloud Updates Update From File Edit Frequency Update Now

FREQUENCY	Every day at 04:36 PM
LAST UPDATED	10:11:59 AM · May 29, 2024
VERSION	202405170936

Note: You can also perform updates via **Vulnerabilities > Update plugins**.

Note: If the user license ages out, the option to download new updates are blocked, and plugins cannot be updated.

Tenable Nessus Plugin Set Updates

Set Automatic Cloud Updates of Plugins



If you have an internet connection, you can update plugins through the cloud. When you enable automatic updates, plugins update at the time and frequency that you set (Default: daily at 02:00 AM).

To enable automatic updates of plugins:

1. Go to **Local Settings > System Configuration > Updates**.

The **Updates** window appears. The **Nessus Plugin Set Cloud Updates** section shows the number of your Plugin Set, the date of the last update, and the update schedule.

2. Click the **Nessus Plugin Set Cloud Updates** toggle to enable automatic updates.

Edit Frequency of Plugin Updates

To edit the schedule of automatic updates of Plugins:

1. Go to **Local Settings > System Configuration > Updates**.

The **Updates** window appears. The **Nessus Plugin Set Cloud Updates** section shows the number of your Plugin Set, the date of the last update, and the update schedule.

2. Click **Edit Frequency**.

The **Edit Frequency** side panel appears.

Edit Frequency

REPEATS EVERY ^{*}

1 Days

AT ^{*}

02:00:00

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

Cancel Save

3. In the **Repeats Every** section, set the time interval at which you want to update the plugins by typing a number and selecting a unit of time (Days or Weeks) from the drop-down box.

If you select **Weeks**, select which days of the week you want to perform a weekly update on the plugins.

4. In the **At** section, set the time of day at which you want to update the Plugins (in HH:MM:SS) by clicking on the clock icon and selecting the time, or by typing the time manually.
5. Click **Save**.

A message appears confirming that the frequency update is successful.

Perform Manual Cloud Updates of Plugins

To update plugins manually:

1. Go to **Local Settings > System Configuration > Updates**.

The **Updates** page appears. The **Nessus Plugin Set Cloud Updates** section shows the number of your Plugin Set, the date of the last update, and the update schedule.



2. Click **Update Now**.

A message appears to confirm that the update is in progress. When the update is complete, the **Plugin Set** displays the number of the current Plugin Set.

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

Offline Updates

If you do not have an internet connection on your OT Security device, you can manually update the Plugins by downloading the latest Plugin set from the Tenable Community Portal and uploading the file.

To update plugins offline:

1. Go to **Local Settings > System Configuration > Updates**.

The **Updates** page appears. The **Nessus Plugin Set Cloud Updates** section shows the number of your Plugin Set, the date of the last update, and the update schedule.

2. Click **Update From File**.



The **Update From File** window appears.

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

Set Automatic Cloud Updates of the IDS Engine Ruleset

If you have an internet connection, you can update the IDS Engine Ruleset through the cloud. When you enable automatic updates, the IDS Engine Ruleset can update at the time and frequency that you set (Default: Repeats every week on Monday and Thursday at 02:00 AM).

To enable automatic updates of the IDS Engine Ruleset:

1. Go to **Local Settings > System Configuration > Updates**.

The **Updates** page appears. The **IDS Engine Ruleset Cloud Updates** shows the number of your Rule Set, the date of the last update, and the update schedule.

2. Click the **IDS Engine Ruleset Cloud Updates** toggle to enable automatic updates.

Edit Frequency of IDS Engine Ruleset Updates

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

1. Go to **Local Settings > System Configuration > Updates**.

The **Updates** page appears. The **IDS Engine Ruleset Cloud Updates** shows the number of your Rule Set, the date of the last update, and the update schedule.

2. Click **Edit Frequency**.

The **Edit Frequency** side panel appears.

3. In the **Repeats Every** section, set the time interval at which you want to update the Ruleset, by typing a number and selecting a unit of time (Days or Weeks) from the drop-down box.

If you select **Weeks**, select which days of the week you want to perform a weekly update on the Ruleset.

4. In the **At** section, set the time of day at which you want to update the IDS Engine Ruleset (in HH:MM:SS) by clicking the clock icon and selecting the time, or by entering the time manually.

5. Click **Save**.

A message appears to confirm the frequency update is successful.

Perform Manual Cloud Updates of the IDS Engine Ruleset

To update the IDS Engine Ruleset manually:

1. Go to **Local Settings > System Configuration > Updates**.

The **Updates** page appears, with **IDS Engine Ruleset Cloud Updates**, showing the number of your Rule Set, the date of the last update and the update schedule.



2. Click **Update Now**.

A message appears confirming that the update is in progress. When the update is complete, the **Ruleset** box displays the number of the current IDS Engine Ruleset.

Offline Updates

If you do not have an internet connection on your OT Security device, you can manually update your IDS Engine Ruleset by downloading the latest Ruleset from the Tenable Customer Portal and uploading the file.

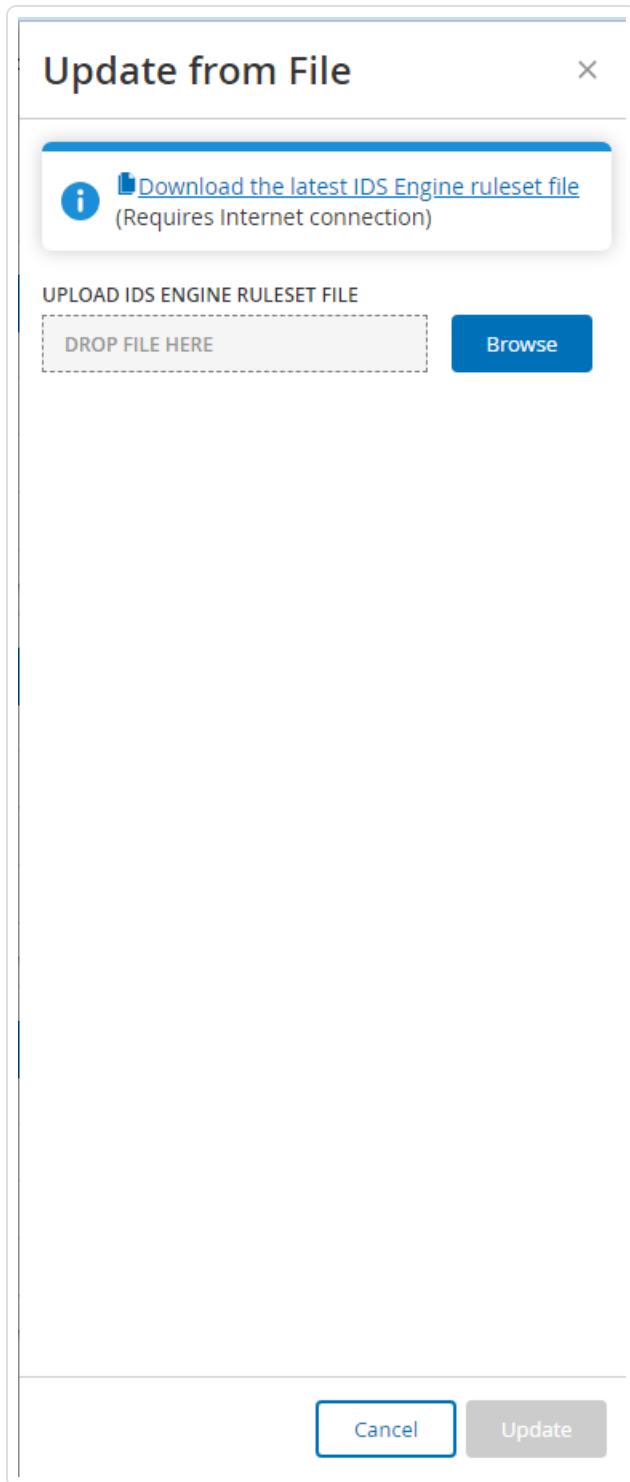
To update the IDS Engine Ruleset offline:

1. Go to **Local Settings > System Configuration > Updates**.

The **Updates** window appears. The **IDS Engine Ruleset Cloud Updates** shows the number of your Rule Set, the date of the last update, and the update schedule.

2. Click **Update From File**.

The **Update From File** window appears.



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 file you downloaded from the OT Security Customer portal.
5. Click **Update**.

DFE Cloud Updates

You can use the **Dynamic Fingerprinting Engine (DFE) Updates** section to update changes or add new classification to your OT Security system.

Set Automatic Cloud DFE Updates

Using an internet connection, you can update the IDS Engine Ruleset through the cloud. When you enable automatic updates, the IDS Engine Ruleset can update at a set time and frequency (Default: Repeats every week on Monday and Thursday at 02:00 AM).

To enable automatic DFE updates:

1. Go to **Local Settings > System Configuration > Updates**.

The **Updates** page appears. The **DFE Cloud Updates** section shows the frequency set for automatic updates, the date of the last update, and the current version of the update.

2. To enable automatic updates, click the **DFE Cloud Updates** toggle.

Edit Frequency of DFE Updates

To edit the schedule of automatic DFE updates:

1. Go to **Local Settings > System Configuration > Updates**.

The **Updates** page appears. The **DFE Cloud Updates** section shows the frequency set for automatic updates, the date of the last update, and the current version of the update.

2. Click **Edit Frequency**.

The **Edit Frequency** side panel appears.

3. In the **Repeats Every** section, set the time interval for the DFE update by typing a number and selecting a unit of time (Days or Weeks) from the drop-down box.

If you select **Weeks**, select the days of the week for the weekly DFE update.



4. In the **At** section, set the time of day for the DFE update (in HH:MM:SS) by clicking the clock icon and selecting the time, or by entering the time manually.
5. Click **Save**.

A message appears to confirm that the frequency update is successful.

Perform Manual Cloud DFE Updates

To update DFE manually:

1. Go to **Local Settings > System Configuration > Updates**.

The **Updates** page appears. The **DFE Cloud Updates** section shows the frequency set for automatic updates, the date of the last update, and the current version of the update.

2. Click **Update Now**.

A message appears confirming that the update is in progress. When the update is complete, the **Version** box displays the current DFE version.

Offline Updates

If you do not have an internet connection on your OT Security device, you can manually update DFE by downloading the latest version from the Tenable Customer Portal and uploading the file.

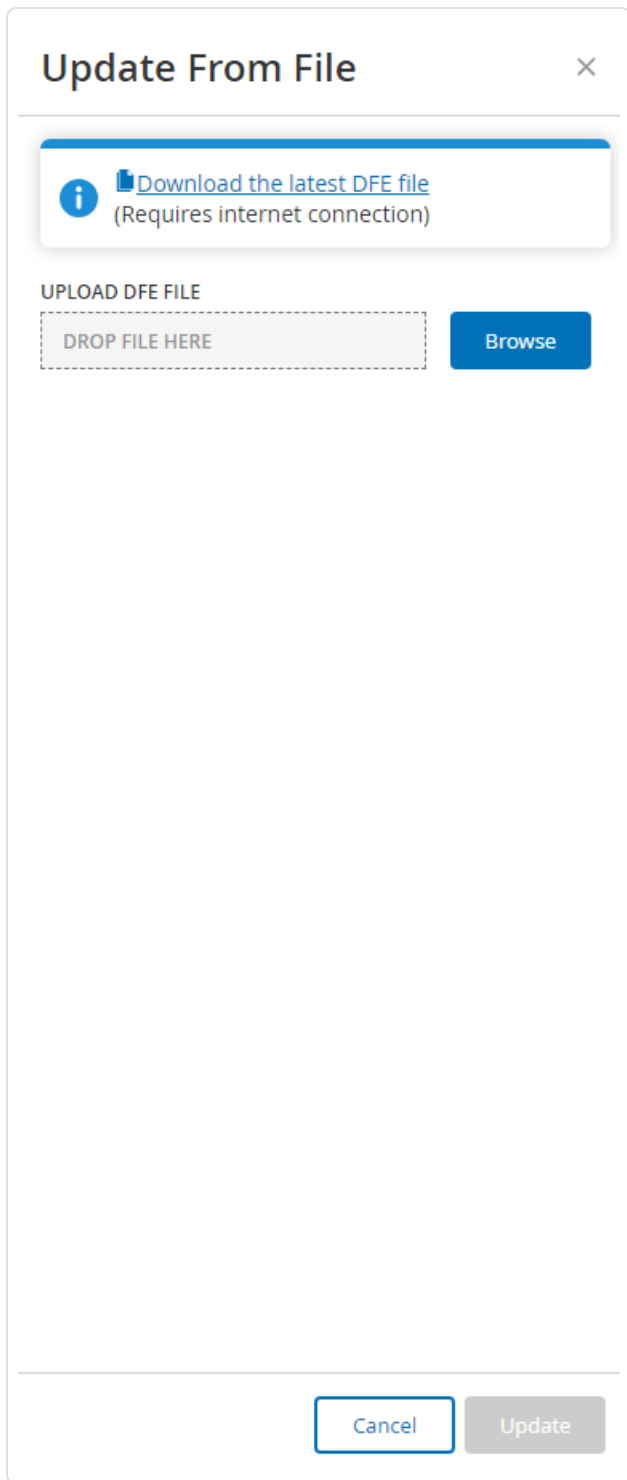
To perform an offline DFE update:

1. Go to **Local Settings > System Configuration > Updates**.

The **Updates** window appears. The **DFE Cloud Updates** section shows the frequency set for automatic updates, the date of the last update, and the current version of the update.

2. Click **Update From File**.

The **Update From File** window appears.



3. If you have not yet done so, click the link to download the latest Device Signatures file.

Note: Downloading the latest Device Signatures 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 Device Signatures file you downloaded from the OT Security Customer portal.
5. Click **Update**.

Certificate

Generate an HTTPS Certificate

The HTTPS certificate ensures the system is using a secure connection to the OT Security appliance and server. The initial certificate ages out 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 overrides the current certificate.

To generate a self-signed certificate:

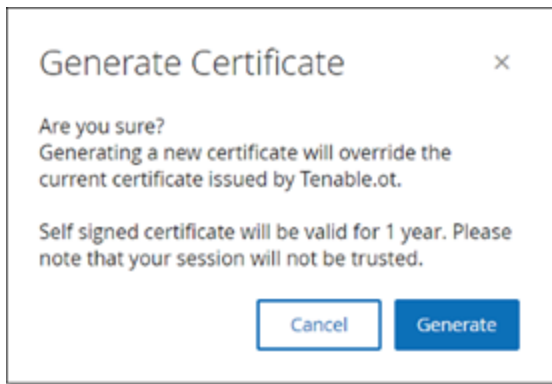
1. Go to **Local Settings > System Configuration > Certificates**.

The **Certificates** window appears.

2. From the **Actions** menu, select **Generate Self-Signed Certificate**.



The Generate Certificate confirmation window appears.



3. Click **Generate**.

OT Security generates the self-signed certificate and you can view the certificate in the **Local Settings > System Configuration > Certificate** page.

Upload an HTTPS Certificate

To upload an HTTPS Certificate:

1. Go to **Local Settings > System Configuration > Certificates**.

The **Certificates** window appears.

2. From the **Actions** menu, select **Upload Certificate**.



The **Upload Certificate** side panel appears.

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. In the **Certificate File** section, click **Browse** and navigate to the certificate file you want to upload.
4. In the **Private Key File** section, click **Browse** and navigate to the Private Key file you want to upload.
5. In the **Private Key Passphrase** box, type the private key passphrase.
6. Click **Upload** to upload the files.

The side panel closes.

Note: After replacing the certificate, Tenable recommends that you reload the browser tab to ensure the HTTP Certificate update is successful. If the upload is unsuccessful, OT Security displays a warning message.

Pair ICP with Enterprise Manager



Note: This flow is available for OT Security 3.18 and later.

You can pair your Industrial Core Platform (ICP) with OT Security EM and manage all your sites.

Before you Begin

Make sure that:

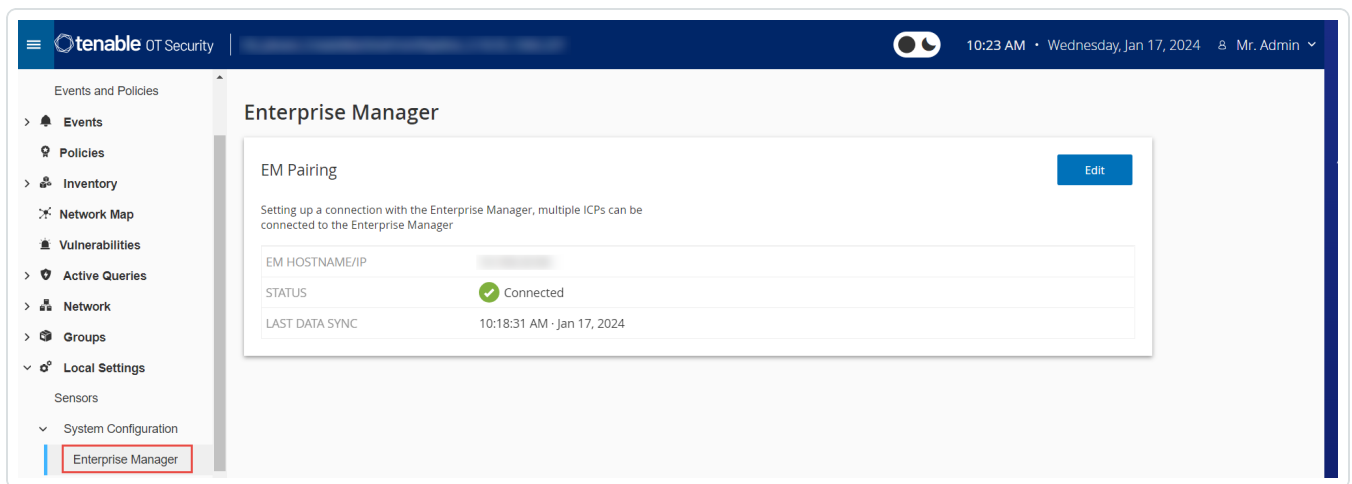
- OT Security EM can connect via API to the ICP.
- Make sure TCP 443 and TCP 28305 are open for communication from ICP to OT Security EM.
- HTTPS connections exist between ICP and OT Security EM.
- (Optional) Generate an API Key in OT Security EM.

Note: This is required only when pairing using the API key option.

To pair ICP with OT Security EM:

1. In OT Security, go to **Local Settings > System Configuration > Enterprise Manager**.

The **Enterprise Manager** page appears.



2. In the **EM Pairing** section, click **Start Pairing**.

The **EM Pairing Configuration** panel appears.

3. Select one of the following:



- **Pair using username and password**
- **Pair using API secret**

If you select...	Action
Pair using username and password	<ol style="list-style-type: none">1. In the Hostname/IP box, type the hostname or the IP address of the EM.2. In the Username box, type the administrator username of the EM.3. In the Password box, type the password of the EM.4. In the EM Certificate Fingerprint, paste the certificate that you copied from the EM Certificates page. <div data-bbox="716 816 1479 932" style="border: 1px solid green; padding: 5px;">Tip: You can skip this step and manually approve the certificate from the EM Pairing page.</div> <div data-bbox="716 957 1479 1073" style="border: 1px solid blue; padding: 5px;">Note: You can access the Certificates page from Local Settings > System Configuration in OT Security EM.</div>
Pair using API Key	<ol style="list-style-type: none">1. In the Hostname/IP box, type the hostname or the IP address of the EM.2. In the API Secret box, paste the API key that you copied from the EM.3. In the EM Certificate Fingerprint, paste the certificate that you copied from the EM Certificates page. <div data-bbox="716 1465 1479 1581" style="border: 1px solid green; padding: 5px;">Tip: You can skip this step and manually approve the certificate from the EM Pairing page.</div> <div data-bbox="716 1606 1479 1722" style="border: 1px solid blue; padding: 5px;">Note: You can access the Certificates page from Local Settings > System Configuration in OT Security EM.</div>

4. Click **Pair**.



OT Security displays the **EM Pairing** page with the pairing status.

Note: The status can show as **Waiting for certificate approval** (if certificate is not provided) or **Pending EM approval** (if automatic approval of pairing requests is disabled).

5. (Optional) If the status shows **Waiting for certificate** approval:

a. Click **Show Certificate**.

The **Approve Certificate** panel appears.

b. Verify if the fingerprint on the panel is the same as that on the EM **Certificates** page.

Click **Approve**.

OT Security approves the certificate and displays the EM pairing page with the status changed to **Pending EM approval**.

6. If the status shows **Pending EM approval**, it indicates that **Auto Approve ICP Pairing Requests** is disabled, then proceed as follows:

Tip: To approve pairing requests automatically in OT Security EM, enable the **Auto Approve ICP Pairing Requests** in the OT Security EM **ICPs** page.

a. In OT Security EM, in the left navigation bar, select **ICPs**.

The **ICPs** page appears.

b. Hover over the row of the system you want to pair, do one of the following:

- Right-click the **Status** column and select **Approve**.
- In the upper-right corner, click **Actions > Approve**.

OT Security EM approves the pairing and shows the status as **Connected**.

Tip: After the pairing is complete, OT Security EM shows the following:

- Shows the data from the ICP on the EM **Dashboards**.
- Newly paired ICP appears on the **ICPs** page.
- Access to the ICP by clicking the ICP name from the **ICPs** page. The ICP instance



accessed from the EM shows the **ICP** label in the header. For more information, see [ICPs](#) in the Tenable OT Security Enterprise Manager User Guide.

In OT Security, the **Enterprise Manager** page shows the status as **Connected**. You can click **Edit** to modify the EM pairing configuration.

Disconnect ICP Pairing with Enterprise Manager

You can disconnect the ICP pairing from the EM or the ICP when the pairing is no longer needed.

To disconnect an ICP pairing from OT Security EM:

1. In OT Security EM, in the left navigation bar, select **ICPs**.

The **ICPs** page appears.

2. Hover over the row of the ICP you want to delete, do one of the following:
 - Right-click the **Status** column and select **Delete**.
 - Click the ICP row. This highlights the row and enables the **Actions** button.

3. Click **Delete**.

OT Security EM disconnects the pairing with OT Security.

To disconnect an ICP pairing from OT Security:

1. In OT Security, go to **Local Settings > System Configuration > Enterprise Manager**.

The **Enterprise Manager** page appears.

2. In the EM Pairing section, click **Edit**.

The **EM Pairing** panel appears.

3. Click **No Pairing**.

4. Click **Pair**.

OT Security disconnects the pairing with OT Security EM.

License



When you need to update or reinitialize your OT Security license, reach out to your Tenable account manager. Once your Tenable account manager updates your license, you can [update](#) or [reinitialize](#) your license. For more information, see the [OT Security License Activation](#).

Environment Configuration

Monitored Networks

The Monitored Network configuration contains a set of IP ranges (CIDRs / subnets) that define the monitoring boundaries for OT Security. OT Security ignores assets outside of the configured ranges.

By default, OT Security configures three default public ranges: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16, as well as the link-local range of 169.254.0.0/16 (APIPA).

Monitored Network Edit

The Assets Network is an aggregation of IP ranges in which assets are located. Use these settings in order to configure these IP ranges. Please note that in addition to these settings, any host within tenable.ot's sensors subnets or any activity performing device will be classified as an asset.

DEFAULT IP RANGES	192.168.0.0/16
	172.16.0.0/12
	169.254.0.0/16
	10.0.0.0/8
ADDITIONAL IP RANGES	

To disable any of the default ranges or add ranges appropriate for your network:

1. Go to **Local Settings > Environment Configuration > Asset Settings**.

The **Asset Settings** window appears.

2. Click **Edit**.



The Monitored Network panel appears.

Monitored Network ×

i IDS engine will only monitor the first 400 subnet definitions (CIDRs).

Default IP ranges:

- 192.168.0.0/16
- 172.16.0.0/12
- 169.254.0.0/16
- 10.0.0.0/8

Additional IP ranges:

IP RANGES ONE CIDR PER LINE

e.g 10.10.10.10/8

Cancel Save



3. Select the required **Default IP ranges** and/or add **Additional IP ranges** (one IP range per line) in the designated text box.
4. Click **Save**.

OT Security saves the monitored network configuration.

Add Assets Manually

To track your inventory, you may want to view some additional assets you possess, even though OT Security has not yet detected these assets. You can manually add these assets to your inventory by downloading and editing a CSV file, and then uploading the file to the system. You 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 uses the information retrieved about the detected asset and overwrites the previously uploaded information. The system begins 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 display a risk score of 0 until OT Security detects these assets.

Note: When assets are added manually, events are not detected for those assets until OT Security detects their communication in the network.

To add assets manually:

1. Go to **Local Settings > Environment Configuration > Asset Settings**.
The **Asset Settings** screen appears.
2. In **Add Assets Manually**, from the **Actions** menu, select **Download CSV template**.
OT Security downloads the tot_Assets template document.
3. Open the tot_Assets template document.
4. Edit the tot_Assets template precisely in accordance with the instructions found in the file, leaving only the column headers (Name, Type, and so on.) and the values you enter.
5. Save the edited file.



- Return to the **Assets Settings** screen.
- From the **Actions** menu, select **Upload CSV** and navigate to and open the desired CSV file to upload it.
- In **Add Assets Manually**, click **Download Report**.

A CSV file with report appears, 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	Pfc	High	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	10.200.30.30		VMware			Windows Server 2012				Success	
4	CCC	Switch			AA:bb:cd	Catalyst	C2960	12.3		Level3			Success	
5	DDDD	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 (that is, events that share the same policy), source, and destination assets, and so on.

To cluster events, 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 are not 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 is not part of the cluster.

To enable clustering:

- Go to **Local Settings**, go to **Environment Configuration > Event Clusters**.

The **Event Clusters** screen appears.



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

2. Click the toggle to enable desired categories for clustering.

3. To configure the time intervals for a category, click **Edit**.

The **Edit Configuration** window appears.

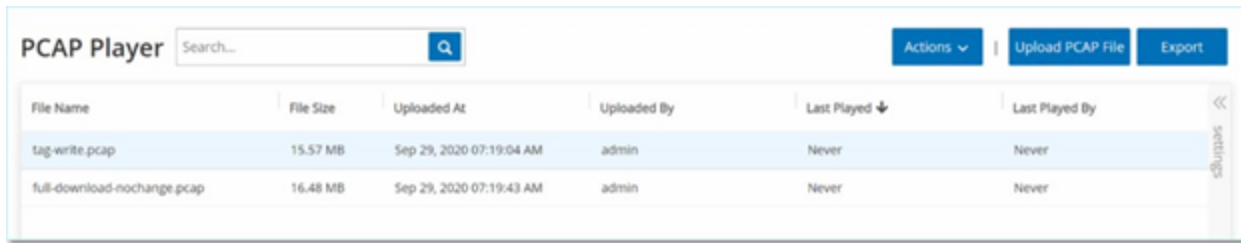
4. Type the required number value in the number box and select the unit of time using the drop-down box.

Note: For more information about clustering and time intervals, click the  icon.

5. Click **Save**.



PCAP Player



The screenshot shows the PCAP Player 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 three buttons: "Actions" with a dropdown arrow, "Upload PCAP File", and "Export". Below the search bar is a table with the following columns: "File Name", "File Size", "Uploaded At", "Uploaded By", "Last Played" (with a downward arrow), and "Last Played By". The table contains two rows of data:

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 (Packet Capture) 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 occurred within your network. You can use this feature for simulation purposes or in order to analyze traffic that occurs outside of the network that OT Security monitors. For example, remote plants.

Note: PCAP Player supports these file types: .pcap, .pcapng, .pcap.gz, .pcapng.gz. You can use files that are recorded by an instance of OT Security or other network monitoring tools.

Upload a PCAP File

To upload a PCAP file:

1. Go to **Local Settings > Environment Configuration > PCAP Player**.
2. Click **Upload PCAP File**.

The **File Explorer** opens.

3. Select the required PCAP recording.
4. Click **Open**.

OT Security uploads the PCAP file to the system.

Play a PCAP File

To play a PCAP file:



1. Go to **Local Settings >Environment Configuration > PCAP Player**.
2. Select the PCAP recording you want to play.
3. Click **Actions > Play**.

The **Play PCAP** wizard appears.

4. In the **Play Speed** drop-down box, select the speed at which you want the system to play the file.

Options are: 1X, 2X, 4X, 8X or 16X.

Note: Playing a PCAP file injects data into the system, you cannot undo or stop this operation once it runs.

5. Click **Play**.

The system plays the PCAP file. 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.

User Management

Access to the OT Security Console is controlled by user accounts that designate the permissions that are available for that user. The user's permissions are determined by the User Groups to which they are assigned. Each User Group is assigned a role, which defines the set of permissions that are 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 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** and so on. 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 that define their roles.



- **Authentication Servers** – Use your organization’s authentication servers (for example, 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 (for example, Microsoft Entra ID) and assign users to your OT Security application.

[Local Users](#)

[User Groups](#)

[User Roles](#)

[Zones](#)

[Authentication Servers](#)

[SAML](#)

Local Users

An administrator user can create new user accounts and edit existing accounts. Each user is assigned to one or more User Groups which determine the roles assigned to the user.

Note: You can add users to the User Groups either during the creation or editing of the user’s account or the User Group.

View Local Users

The **Local Users** window 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 **Local Users** window shows the following details:

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



Full Name	The full name of the user.
Username	The username of the user, used for login.
User Groups	The User Groups to which the user is assigned.

Add 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. Go to **Local Settings > User Management > Local Users**.
2. Click **Add User**.

The **Add User** pane appears.

The screenshot shows a dialog box titled "Add User" with a close button (X) in the top right corner. It contains the following fields:

- FULL NAME ***: A text input field with the placeholder "Full Name".
- USERNAME ***: A text input field with the placeholder "Username".
- PASSWORD ***: A password input field with the placeholder "Password" and a visibility toggle icon.
- RETYPE NEW PASSWORD ***: A password input field with the placeholder "Retype New Password" and a visibility toggle icon.
- USER GROUPS ***: A dropdown menu with the placeholder "Select multiple".

At the bottom of the dialog are two buttons: "Cancel" and "Create".

3. In the **Full Name** box, type the first and last name.



Note: The name that you enter appears in the header bar when the user is signed in.

4. In the **Username** box, type a user name to be used for logging in to the system.
5. In the **Password** box, type a password.
6. In the **Retype Password** box, type the identical password.

Note: This is the password that the user uses for the initial login. The user can change the password in the **Settings** window after logging into the system.

7. In the **User Groups** drop-down box, select the check box for each User Group to which you want 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** and so on. For an explanation of the available roles, see [Local Users](#).

8. Click **Create**.

OT Security creates the new user account in the system and adds to the list of users in **Local Users**.

Additional Actions on User Accounts

Edit 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. Go to **Local Settings > User Management > Local User**.

The **Local Users** screen appears.

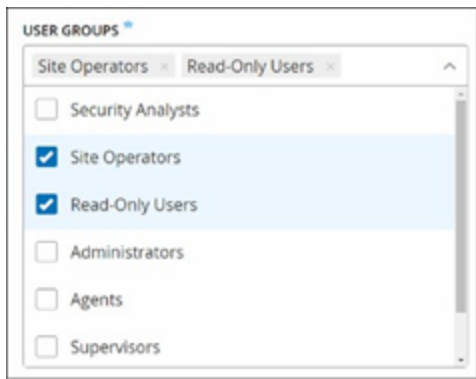
2. Right-click the required user and select **Edit User**.

Note: Alternatively, you can select a user and then from the **Actions** menu, select **Edit User**.

3. The **Edit User** pane appears, showing the User Groups to which the user is assigned.



4. In the **User Groups** drop-down box, select or clear the required user groups.



5. Click **Save**.

Change a User's Password

Note: This procedure is for an administrator user to change the password for any account in the system. Any user can change their own password by going to **Local Settings > User**.

To change a user's password:

1. Go to **Local Settings > User Management > Local User**.

The **Local Users** screen appears.

2. Right-click the required user and select **Reset Password**.

Note: Alternatively, you can select a user and from the **Actions** menu, select **Reset Password**.

The **Reset Password** window appears.



Reset Password ×

Reset password for Bob Smith.

PASSWORD *

Password

RETYPE NEW PASSWORD *

Retype New Password

3. In the **New Password** box, type a new password.
4. In the **Retype New Password** box, re-type the new password.
5. Click **Reset**.

OT Security applies the new password to the specified user account.

Delete Local Users

To delete a user account:

1. Go to **Local Settings > User Management > Local User**.

The **Local Users** screen appears.

2. Right-click the required user and select **Delete User**.

Note: Alternatively, you can select a user and from the **Actions** menu, select **Delete User**.

A confirmation window appears.

3. Click **Delete**.

OT Security deletes the user account from the system.

User Groups



An administrator user can create new User Groups and edit existing groups. Each user is assigned to one or more User Groups, which determine the roles 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, and so on. For an explanation of the available roles, see [User Roles](#).

Viewing User Groups

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

Name	Members	Role
Administrators	Mr. Adman	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 following details are available in the User Groups page:

Parameter	Description
Name	The name of the User Group.
Members	A list of all members assigned to the group.
Role	The role given to this group. For an explanation of the permissions associated with each role, see User Roles Table .

Add User Groups

You can create new User Groups and assign users to that Group.

To create a user group:

1. Go to **Local Settings > User Management > User Groups**.

The **User Groups** screen appears.

2. Click **Create User Group**.



The **Create User Group** pane appears.

Create User Group ×

NAME *

ROLE *
LOCAL MEMBERS
ZONES
AUTHENTICATION SERVERS



3. In the **Name** box, type a name for the group.
4. In the **Role** drop-down box, select from the drop-down list the role that you want to assign to this group. Available roles are:
 - Read Only
 - Security Analyst
 - Security Manager
 - Site Operator
 - Supervisor
5. In the **Local Members** drop-down box, select the user accounts that you want to assign to the group.
6. In the **Zones** drop-down box, select the zones you want to assign to the user group.
7. In the **Authentication Servers** drop-down box, select the servers that you want to assign to the user group.
8. Click **Create**.

OT Security creates the new User Group and adds to the list of groups shown in the **User Groups** screen.

Additional Actions on User Groups

Edit 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 from the **Actions** menu, select **Delete User**.

To edit a User Group:

1. Go to **Local Settings > User Management > User Groups**.

The **User Groups** screen appears.



2. Do one of the following:

- Right-click the required user group and select **Edit**.
- Select the user group you want to edit. The **Actions** menu appears. Select **Actions > Edit**.

The **Edit User Group** panel appears, showing the group's settings.

3. Change the **Name**, **Role**. You can also select or clear users to add or remove users to the group.

The screenshot shows a dialog box titled "Edit User Group". It has three main sections: "NAME" with a text input field containing "Security Analysts"; "ROLE" with a dropdown menu showing "Security Analyst"; and "USERS" with a multi-select list containing "Bob Smith" and "Mr. Admin", and a plus icon to add more users.

4. Modify the parameters as needed.
5. Click **Save**.

Delete 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 need to first remove the users from the group before you can delete the group.

To delete a user group:

1. Go to **Local Settings > User Management > User Groups**.

The **User Groups** screen appears.

2. Do one of the following:



- Right-click the required User Group and select **Delete**.
- Select the user group you want to delete. The **Actions** menu appears. Select **Actions > Delete**.

A confirmation window appears.

3. Click **Delete**.

OT Security deletes the **User Group**.

User Roles

The following are the available roles:

- **Administrator** – Has maximum privileges to do all operational as well as administrative tasks in the system, including creating new user accounts.
- **Read-Only** – Can view data (asset inventory, events, network traffic), but cannot act in the system.
- **Security Analyst** – Can view data in the system and resolve security events.
- **Security Manager** – Can manage security-related capabilities, including configuring policies, viewing data in the system, and resolving events.
- **Site Operator** – Can view data in the system and manage the asset inventory.
- **Supervisor** – Has full privileges to do all operational tasks in the system and some limited administrative tasks excluding creating new users and other sensitive activities.

User Roles Table

The following table gives a detailed breakdown of precisely which permissions are enabled for each role.

Permission	Admin (Local)	Admin (External/AD)
Events		
View events	✓	✓
Resolve	✓	✓



Download capture file	✓	✓
Exclude from policy	✓	✓
Resolve all	✓	✓
Export	✓	✓
Create Policy on FortiGate	✓	✓
Refresh	✓	✓
Policies		
View policies	✓	✓
Enable/Disable	✓	✓
View action	✓	✓
Edit	✓	✓
Duplicate	✓	✓
Delete	✓	✓
Create policy	✓	✓
Export	✓	✓
Assets		
View assets	✓	✓
View action	✓	✓
Edit	✓	✓
Delete	✓	✓
Import (upload new assets by csv)	✓	✓
Hide	✓	✓



Export	✓	✓
Resync	✓	✓
Nessus scan	✓	✓
Take snapshot (single asset)	✓	✓
Update open ports (single asset)	✓	✓
Update port state (single asset)	✓	✓
View in browser (single asset)	✓	✓
View in main asset map (single asset)	✓	✓
Generate attack vector (single asset)	✓	✓
Vulnerabilities (Plugins)		
View plugin hits	✓	✓
View action	✓	✓
Edit comment	✓	✓
Update plugin set	✓	✓
Export	✓	✓
Network		
Turn on packet capture	✓	✓
Close ongoing captures	✓	✓
Download PCAP file	✓	✓
Export conversations table	✓	✓
Set as baseline	✓	✓
Generate map	✓	✓



Refresh map	✓	✓
Groups		
View groups	✓	✓
View action	✓	✓
Edit	✓	✓
Duplicate	✓	✓
Delete	✓	✓
Create group	✓	✓
Export	✓	✓
Report		
View reports	✓	✓
Generate	✓	✓
Download	✓	✓
Export	✓	✓
Network Segments		
View Network Segments	✓	✓
Edit	✓	✓
Delete	✓	✓
Create	✓	✓
Export	✓	✓
Learn More	✓	✓
Local Settings		



Queries	✓	✓
System Configuration - Device Details	✓	✓
System Configuration - Sensors	✓	✓
System Configuration - Port Configuration	✓	✓
System Configuration - Updates	✓	✓
System Configuration - Certificate (HTTPS)	✓	✓
System Configuration - API Keys	✓	✗
System Configuration - License	✓	✓
Environment Configuration - Asset Settings	✓	✓
Environment Configuration - Hidden Assets	✓	✓
Environment Configuration - Custom Fields	✓	✓
Environment Configuration -Event Clusters	✓	✓
Environment Configuration - PCAP Player	✓	✓
Users and Roles - User Settings	✓	✓
Users and Roles - Local Users	✓	✗
Users and Roles - User Groups	✓	✗
Users and Roles - Active Directory	✓	✗
Integrations	✓	✓
Servers	✓	✓
System Actions	✓	✓ without factory reset
System log	✓	✓
Enable (on setup and after disable)	✓	✓



Delete Assets	✓	✓
----------------------	---	---

Permission	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
Events					
View events	✓	✓	✓	✓	✓
Resolve	✓	✓	✓	✗	✗
Download capture file	✓	✓	✓	✓	✓
Exclude from policy	✓	✓	✗	✗	✗
Resolve all	✓	✓	✓	✗	✗
Export	✓	✓	✓	✓	✓
Create Policy on FortiGate	✓	✓	✗	✗	✗
Refresh	✓	✓	✓	✓	✓
Policies					
View policies	✓	✓	✓	✓	✓
Enable/Disable	✓	✓	✗	✗	✗
View action	✓	✓	✓	✓	✓
Edit	✓	✓	✗	✗	✗
Duplicate	✓	✓	✗	✗	✗
Delete	✓	✓	✗	✗	✗
Create policy	✓	✓	✗	✗	✗



Export	✓	✓	✓	✓	✓
Assets					
View assets	✓	✓	✓	✓	✓
View action	✓	✓	✓	✓	✓
Edit	✓	✗	✗	✓	✗
Delete	✓	✗	✗	✓	✗
Import (upload new assets by csv)	✓	✗	✗	✓	✗
Hide	✓	✗	✗	✓	✗
Export	✓	✓	✓	✓	✓
Resync	✓	✓	✓	✓	✗
Nessus scan	✓	✓	✓	✓	✗
Take snapshot (single asset)	✓	✓	✓	✓	✗
Update open ports (single asset)	✓	✓	✓	✗	✗
Update port state (single asset)	✓	✓	✓	✗	✗
View in browser (single asset)	✓	✓	✓	✓	✓
View in main asset map (single asset)	✓	✓	✓	✓	✓



Generate attack vector (single asset)	✓	✓	✓	✓	✓
Vulnerabilities (Plugins)					
View plugin hits	✓	✓	✓	✓	✓
View action	✓	✓	✓	✓	✓
Edit comment	✓	✓	✓	✗	✗
Update plugin set	✓	✓	✗	✗	✗
Export	✓	✓	✓	✓	✓
Network					
Turn on packet capture	✓	✗	✗	✗	✗
Close ongoing captures	✓	✓	✓	✓	✗
Download PCAP file	✓	✓	✓	✓	✓
Export conversations table	✓	✓	✓	✓	✓
Set as baseline	✓	✓	✗	✗	✗
Generate map	✓	✓	✓	✓	✓
Refresh map	✓	✓	✓	✓	✓
Groups					
View groups	✓	✓	✓	✓	✓



View action	✓	✓	✓	✓	✓
Edit	✓	✓	✗	✗	✗
Duplicate	✓	✓	✗	✗	✗
Delete	✓	✓	✗	✗	✗
Create group	✓	✓	✗	✗	✗
Export	✓	✓	✓	✓	✓
Report					
View reports	✓	✓	✓	✓	✓
Generate	✓	✓	✓	✓	✓
Download	✓	✓	✓	✓	✓
Export	✓	✓	✓	✓	✓
Network Segments					
View Network Segments	✓	✓	✓	✓	✓
Edit	✓	✓	✗	✗	✗
Delete	✓	✓	✗	✗	✗
Create	✓	✓	✗	✗	✗
Export	✓	✓	✓	✓	✓
Learn More	✓	✓	✓	✓	✓
Local Settings					
Queries	✓	✗	✗	✗	✗
System Configuration -	✓	✗	✗	✗	✗



Device Details					
System Configuration - Sensors	✓	✓ (No Actions)	✓ (No Actions)	✓ (No Actions)	✓ (No Actions)
System Configuration - Port Configuration	✓	✗	✗	✗	✗
System Configuration - Updates	✓	✗	✗	✗	✗
System Configuration - Certificate (HTTPS)	✗	✗	✗	✗	✗
System Configuration - API Keys	✓ (Only Local Users)	✓ (Only Local Users)	✓ (Only Local Users)	✓ (Only Local Users)	✓ (Only Local Users)
System Configuration - License	✗	✗	✗	✗	✗
Environment Configuration - Asset Settings	✓	✗	✗	✗	✗
Environment Configuration - Hidden Assets	✓	✓ - no restore	✓ - no restore	✓	✓ - no restore
Environment Configuration - Custom Fields	✓	✗	✗	✗	✗



Environment Configuration - Event Clusters	✓	✗	✗	✗	✗
Environment Configuration - PCAP Player	✓	✗	✗	✗	✗
Users and Roles - User Settings	✓	✗	✗	✗	✗
Users and Roles - Local Users	✗	✗	✗	✗	✗
Users and Roles - User Groups	✗	✗	✗	✗	✗
Users and Roles - Active Directory	✗	✗	✗	✗	✗
Integrations	✗	✗	✗	✗	✗
Servers	✓	✓ (No Actions)	✓ (No Actions)	✓ (No Actions)	✓ (No Actions)
System Actions	✓ only backup and diagnostics	✓ only diagnostics	✗	✗	✗
System log	✓	✓	✓	✓	✓ no syslog
Enable (on setup and after disable)	✗	✗	✗	✗	✗
Delete Assets	✓	✗	✗	✗	✗

Zones



Zones control which assets, events, and vulnerabilities a particular user group can view. A specific user group can only view assets and associated vulnerabilities, events, and connections that fall within its zone. You can assign non-admin accounts to a specific group and zone to limit their visibility to relevant assets.

Create Zones

To create zones:

1. Go to **Local Settings > Users Management > Zones**.

The **Zones** page appears.

2. In the upper-right corner, click **Create**.

The **Create Zone** panel appears.

3. In the **Name** box, type a name for the zone.

4. In the **Asset Groups** box, select the groups you want to assign to the zone. You can use the Search box to search for a specific asset group.

5. In the **User Groups** box, select the user groups you want to assign to the zone.

6. (Optional) In the **Description** box, type a description for the zone.

7. Click **Create**.

OT Security creates the zone and it appears on the **Zones** page.

View Zones

1. Go to **Local Settings > Users Management > Zones**.

The **Zones** page appears. The **Zones** page displays the zones in a table and includes the following details.

Column	Description
Name	The name of the zone.



Asset Groups	The asset groups assigned to the zone.
User Groups	The user groups assigned to the zone.
Description	A description for the zone.
Last Modified by	The user who last modified the zone.
Last Modified on	The date when the zone was last modified.

Edit a Zone

1. Go to **Local Settings > Users Management > Zones**.

The **Zones** page appears.

2. Click the row of the zone you want to edit and do one of the following:
 - Right-click the zone, then select **Edit**.
 - In the header bar, click **Actions > Edit**.

The **Edit Zone** panel appears.

3. Modify the configuration as needed.
4. Click **Save**.

OT Security updates the zone.

Duplicate Zone

1. Go to **Local Settings > Users Management > Zones**.

The **Zones** page appears.

2. Click the row of the zone you want to duplicate and do one of the following:
 - Right-click the zone, then select **Duplicate**.
 - In the header bar, click **Actions > Duplicate**.

The **Duplicate Zone** panel appears.

3. In the **Name** box, type a name for the zone.



The default value is the original zone name with the prefix "Copy of".

4. Modify the configuration as needed.
5. Click **Duplicate**.

OT Security creates a duplicate of the zone.

Delete Zone

You can delete zones you no longer require.

Note: You cannot delete a zone if there are associated user groups.

1. Go to **Local Settings > Users Management > Zones**.

The **Zones** page appears.

2. Click the row of the zone you want to delete and do one of the following:
 - Right-click the zone, then select **Delete**.
 - In the header bar, click **Actions > Delete**.

OT Security deletes the zone.

Authentication Servers

The **Authentication Servers** page shows your existing integrations with authentication servers. You can add a server by clicking 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



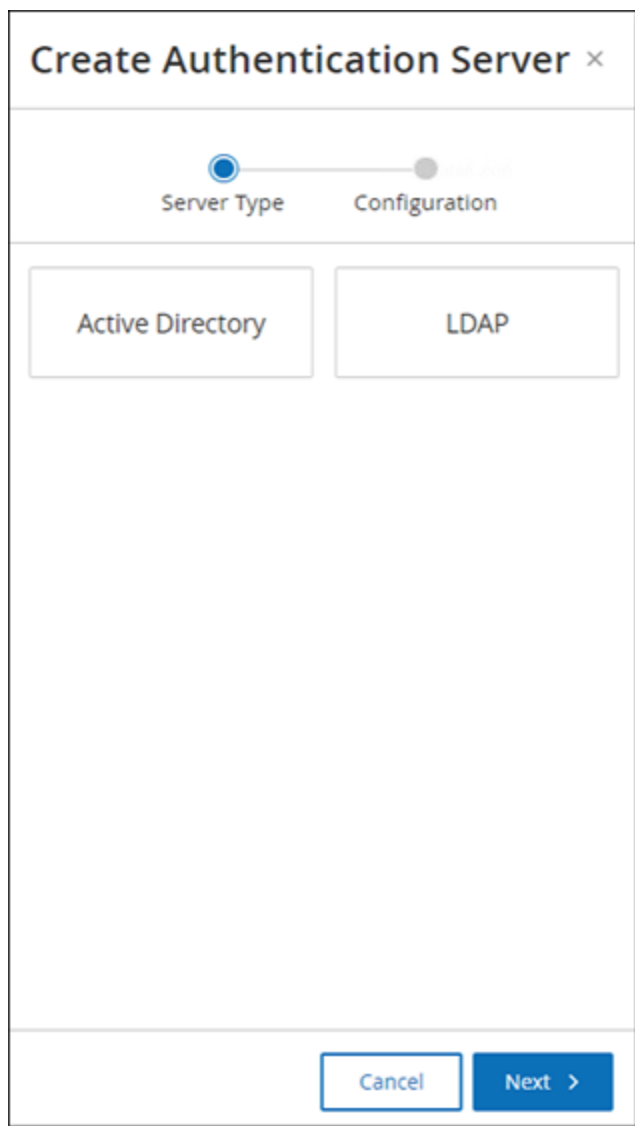
You can integrate OT Security with your organization's Active Directory (AD). This enables users to log in to OT Security using their Active Directory credentials. The configuration involves setting up the integration and then mapping groups in your AD to User Groups in OT Security.

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**, and so on. 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.
2. Go to **Local Settings >Users Management > Authentication Servers**.
The **Authentication Servers** window appears.
3. Click **Add server**.

The **Create Authentication Server** panel opens with the **Server Type**.



4. Click **Active Directory**, then click **Next**.

The **Active Directory** configuration pane appears.

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

5. In the **Name** box, type the name to be used in the login screen.
6. In the **Domain** box, type the FQDN of the organizational domain (for example, company.com).



Note: If you are not aware of your Domain, you can find it by entering the command “set” in Windows CMD or Command Line. The value given for the “USERDNSDOMAIN” attribute is the Domain Name.

7. In the **Base DN** box, type the distinguished name of the domain. The format for this value is ‘DC={second-level domain},DC={top-level domain}’ (for example DC=company,DC=com).
8. For each of the Groups that you want to map from an AD group to a OT Security User Group, type the DN of the AD group in the appropriate box.

For example, to assign a group of users to the Administrators User Group, type the DN of the Active Directory group to which you want to assign administrator privileges in the **Administrators Group DN** box.

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 or Command Line. Type the name of the group that you want to assign in the identical format in which it is shown (for example “CN=IT_Admins,OU=Groups,DC=Company,DC=Com”). The Base DN must also be included at the end of each DN.

Note: These fields are optional. If a field is empty, no AD users are assigned to that User Group. You can set up an integration with no groups mapped, but in that case no users can access the system until you add at least one group map ping.

9. (Optional) In the **Trusted CA** section, click **Browse** and navigate to the file that contains your organization’s CA Certificate (which you obtained from your CA or Network Administrator).
10. Select the **Enable Active Directory** check box.
11. Click **Save**.

A message prompts you to restart the unit to activate the Active Directory.



Active directory changes are pending a restart

Restart

12. Click **Restart**.

The unit restarts. Upon reboot, OT Security activates the Active Directory settings. Any user assigned to the designated groups can access the OT Security platform using their organizational credentials.



Note: To log in using Active Directory, the User Principal Name (UPN) must be used on the login page. In some cases, this means simply adding @<domain>.com to the username.

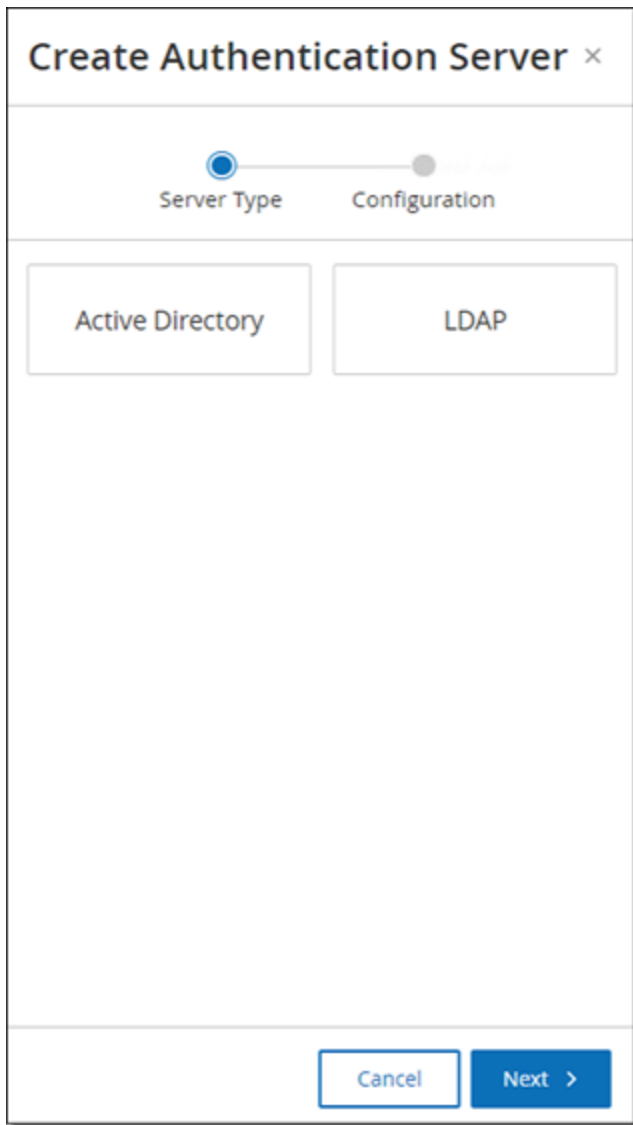
LDAP

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. Go to **Local Settings > User Management > Authentication Servers**.
2. Click **Add Server**.

The **Add Authentication Server** panel opens with the **Server Type**.



3. Select **LDAP**, then click **Next**.

The **LDAP Configuration** pane appears.

4. In the **Name** box, type the name to be used in the login screen.

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

5. In the **Server** box, type the FQDN or the login address.



Note: If using a secure connection, Tenable recommends using the FQDN and not an IP address to ensure that the secure Certificate provided is 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** box, type 389 to use a non-secure connection, or 636 to use a secure SSL connection.

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

7. In the **User DN** box, type the DN with parameters in DN format. For example, for a server name of adsrv1.tenable.com, the user DN can be
CN=Administrator,CN=Users,DC=adsrv1,DC=tenable,DC=com.
8. In the **Password** box, type the password of the User DN.

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

9. In the **User Base DN** box, type the base domain name in DN format. For example, for a server name of adsrv1.tenable.com, the User Base DN is
OU=Users,DC=adsrv1,DC=tenable,DC=com.
10. In the **Group Base DN** box, type the Group base domain name in DN format. For example, for a server name of adsrv1.tenable.com, the Group Base DN is
OU=Groups,DC=adsrv1,DC=tenable,DC=com.
11. In the **Domain append** box, type the default domain that is 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 boxes, type 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**.



OT Security starts the Server in **Disabled** mode.

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

The **System Restart** dialog appears.

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 is not 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 (for example, Microsoft Azure). This enables users to authenticate using 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 – SAML Integration for Microsoft Entra ID](#)

To configure SAML:

1. Go to **Local Settings >Users Management > SAML**.
2. Click **Configure**.

The **Configure SAML** panel appears.

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

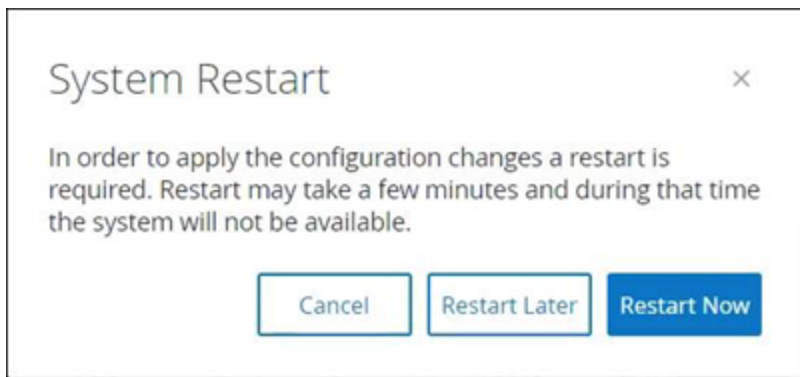
[Cancel](#) [Save](#)

3. In the **IDP ID** box, type the Identity Provider's ID for the OT Security application.
4. In the **IDP URL** box, type the Identity Provider's URL for the OT Security application.
5. In **Certificate Data**, click **Drop File Here**, 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** box, type the username attribute from the Identity Provider for the OT Security application.



7. In the **Groups Attribute** box, type the groups attribute from the Identity Provider for the OT Security application.
8. (Optional) In the **Description** box, type a description.
9. For each group mapping that you want 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** window, click the **SAML single sign on login** toggle to enable single sign-on login.

The **System Restart** notification window appears.



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, OT Security shows following banner until the restart is done:



Upon reboot, the settings are 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 to allow OT Security to sync with your other cybersecurity platforms.

Tenable Products

You can integrate OT Security with Tenable Security Center and Tenable Vulnerability Management. OT Security shares data with the other platforms through these integrations. The synced data includes OT vulnerabilities as well as data discovered by IT-type Tenable Nessus scans initiated from OT Security.

Note: OT Security does not send data for **Hidden** assets to Tenable Security Center and Tenable Vulnerability Management via the integration.

Note: To integrate the platforms, OT Security must be able to reach Tenable Security Center and/or Tenable Vulnerability Management via port 443. Tenable recommends that you 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 **Universal Repository** in Tenable Security Center to store OT Security data and take a note of the repository ID. For more information, see [Universal Repositories](#).

Note: Tenable recommends creating a specific user on Tenable Security Center that is 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.

To integrate Tenable Security Center:

1. Go to **Local Settings > Integrations**.

The **Integrations** page appears.

2. In the upper-right corner, click **Add Integration Module**.

The **Add Integration Module** panel appears.

3. In the **Module Type** section, select Tenable Security Center.



4. Click **Next**.

The **Module Definition** panel with the relevant fields appears.

5. In the **Hostname/IP** box, type the hostname or IP of your Tenable Security Center.
6. In the **Username** box, type the account user ID.
7. In the **Password** box, type the password of your account.
8. In the **Repository ID**, provide the Universal Repository ID.
9. In the **Sync Frequency** drop-down box, set the frequency to sync the data.
10. Click **Save**.

OT Security creates the integration and shows the new integration on the Integrations page.

11. Right-click the new integration and click **Sync**.

Tenable Vulnerability Management

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

To integrate Tenable Vulnerability Management:

1. Go to **Local Settings > Integrations**.

The **Integrations** page appears.

2. In the upper-right corner, click **Add Integration Module**.

The **Add Integration Module** panel appears.

3. In the **Module Type** section, select Tenable Vulnerability Management.
4. Click **Next**.

The **Module Definition** panel with the relevant fields appears.

5. In the **Access Key** box, provide the access key.



6. In the **Secret Key** box, provide the secret key.
7. In the **Sync Frequency** drop-down box, select the frequency to sync the data.

Tenable One

To integrate with Tenable One, follow the steps in [Integrate with Tenable One](#).

Palo Alto Networks – Next Generation Firewall

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

To integrate OT Security with your Palo Alto Networks Next Generation Firewalls (NGFW):

1. Go to **Local Settings > Integrations**.

The **Integrations** page appears.

2. In the upper-right corner, click **Add Integration Module**.

The **Add Integration Module** panel appears.

3. In the **Module Type** section, select Palo Alto Networks NGFW.

4. Click **Next**.

5. In the **Hostname/IP** box, type the hostname or IP address of your Palo Alto NGFW account.

6. In the **Username** box, type the username of your NGFW account.

7. In the **Password** box, type the password of your NGFW account.

8. Click **Save**.

OT Security saves the integration.

Aruba – ClearPass Policy Manager

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

To integrate OT Security with your Aruba ClearPass account:



1. Go to **Local Settings > Integrations**.

The **Integrations** page appears.

2. In the upper-right corner, click **Add Integration Module**.

The **Add Integration Module** panel appears.

3. In the **Module Type** section, select Aruba Networks ClearPass.

4. Click **Next**.

5. In the **Hostname/IP** box, type the hostname or IP address of your Aruba Networks ClearPass account.

6. In the **Username** box, type the username of your Aruba Networks ClearPass account.

7. In the **Password** box, type the password of your Aruba Networks ClearPass account.

8. In the **Client ID** box, type the client ID of your Aruba Networks ClearPass account.

9. In the **API Client Secret** box, type the API Client Secret of your Aruba ClearPass account.

10. Click **Save**.

OT Security saves the integration.

Integrate with Tenable One

You can integrate OT Security with Tenable One to send assets and risk scores data to Tenable Vulnerability Management. To integrate with Tenable One, you must first generate a linking key in Tenable Vulnerability Management and provide it to OT Security. Tenable One gets updated periodically with any asset changes since the previous synchronization.

Before you begin

- Ensure that you have the linking key generated in Tenable Vulnerability Management. For more information, see [OT Connectors](#) in the Tenable Vulnerability Management User Guide.

Note: A linking key generated within Tenable Vulnerability Management can only be used for a single OT Security site.

To integrate with Tenable One:



1. Go to **Local Settings > Integrations**.

The **Integrations** page appears.

2. In the upper-right corner, click **Add Integration Module**.

The **Add Integration Module** panel appears.

3. In the **Module Type** section, click **Tenable One**.

4. Click **Next**.

The **Module Definition** section appears.

5. In the **Cloud Site** box, type the cloud site name.

Note: The cloud site name appears on the **Add OT Connector** window in Tenable Vulnerability Management after you generate the linking key.

6. In the **Linking Key** box, provide the linking key that you generated from Tenable Vulnerability Management.

7. Click **Save**.

OT Security displays a message that the integration is successful. Once the integration is complete, you can view the linked site in the **Integrations** page. In Tenable One, the **Sensors > OT Connectors** page shows the device name configured for that site in OT Security.

For the device name for a site, see the **Device Name** section in the **System Configuration > Device** page.

Note: If you change the name of your site in OT Security after it is already paired, you can manually modify the sensor name within Tenable Vulnerability Management to match the new site name. Alternatively, you can delete the integration on both OT Security and Tenable Vulnerability Management, and pair it again to automatically update the site name change.

For information about the complete procedure for deploying and licensing Tenable OT Security for Tenable One, see the [Tenable One Deployment Guide](#).

IoT Connectors



OT Security allows you to map all managed Internet of Things (IoT) devices to their respective application server by configuring the IoT Connector engine and synchronizing assets from the specific application server.

In the example of an IP camera, you can see the Video Management System (VMS) server that manages it. On the OT Security **Inventory** page, navigating to the VMS application server shows all the cameras that it manages on the **Inventory > Related Assets** page.

Name	IP	Connection Method	Connector Type	Status	Assets
Exacq VMS - Site A		Via Remote API	Exacq Edge	N/A	
Mobotix Camera - Site B		Via Remote API	Mobotix Camera	N/A	
VMS Agent - Site C		Via Agent	Agent	N/A	

Note: By default, when importing assets from an IoT connector, OT Security imports the IP address along with the MAC address of the devices. To import only the MAC address, go to **Local Settings > Environment Configuration > Assets Settings** and disable the **Fetch IP Address for IoT Assets** option.

IoT Connectors Engine

OT Security includes an IoT Connector engine that you can integrate with your IoT/VMS servers.

This engine supports two connection methods: authenticating with a remote application API service or connecting via an agent. After integrating your application servers with the engine, OT Security imports all managed devices such as cameras, badge access systems, and fire panels.

Add IoT Connectors

You can integrate your IoT connectors with OT Security either using a remote API service or an agent.



Before you Begin

- **(Only for connections via Agent)** Make sure you install the OT Security IoT Connector Agent on your application servers. For more information, see [Install IoT Connector Agent on Windows](#).

1. In the left navigation bar, go to **Local Settings > IoT Connectors**.

The **IoT Connectors** page appears.

2. In the upper-right corner, click **Add IoT Connector**.

A drop-down menu appears.

3. Select one of the following options:

- **Via Agent**

1. In the **Connector Name** box, type a name for the connector.
2. In the **IP** box, type the IP address of the connector to add.
3. Click **Save**.

Note: If your application server does not have the [OT Security IoT Connector Agent](#) installed, the connection fails and OT Security displays an error message.

- **Via Remote API**

1. In the **Connector Type** section, select the IoT connector to add.
2. Click **Next**.
The **Connector Details** section appears.
3. In the **Connector Name** box, type a name for the connector.
4. In the **IP** box, type the IP address of the connector.
5. In the **Port** box, type the port number through which OT Security can connect. The default port number is 22609.
6. In the **Username** box, type the username to log in to the connector.



7. In the **Password** box, type the password for the connector.
8. Click **Save**.

OT Security saves the connector and it appears on the **IoT Connectors** page.

Name	IP	Connection Method	Connector Type	Status	Assets
Lab Milestone		Via Remote API	Milestone	Connected	3
Sallent Agent		Via Agent	Agent	Disconnected	1
Lab Exacq		Via Remote API	Exacq Edge	Connected	1

View Assets Linked to the IoT Connector

After you connect to the application server, you can view the related assets or services managed by the application server.

To view all devices managed by the server:

1. Go to **Inventory > All Assets**.

The **All Assets** page appears.

2. Use the **Search** box to search for the application server.

The selected application server page appears with the list of devices that it manages.

Partner Asset	Family	Relationship Type	Access Direction	Details	First Seen	Last Updated
Arecont Single Camera (SingleCam	IoTConnectors	To Partner		01:43:36 PM · Jun 17, 2024	02:56:17 AM · Aug
Hanwha Vision QNV-8080R (Hanwha Vision QNV-8080R	IoTConnectors	To Partner		01:43:02 PM · Jun 17, 2024	02:55:14 AM · Aug
axis-accc8ef5210e	M3046-V	IoTConnectors	To Partner		01:43:03 PM · Jun 17, 2024	02:55:15 AM · Aug

Test the IoT Connection

After adding an IoT connector, you can test if OT Security can reach it.



1. In the IoT Connectors table, do one of the following:

- In the row of the IoT connector you want to test, right-click and select **Test Connection**.
- Select the IoT connector you want to test, then click **Actions > Test Connection**.

OT Security runs the test to verify if it can reach the connector.

Edit IoT Connector

1. In the IoT Connectors table, do one of the following:

- In the row of the IoT connector you want to edit, right-click and select **Edit**.
- Select the IoT connector you want to edit, then click **Actions > Edit**.

The **Edit IoT Connector via Agent/Remote API** panel appears.

2. Modify the details as needed.

3. Click **Save**.

OT Security saves the updates to the IoT Connector.

Delete IoT Connector

1. In the IoT Connectors table, do one of the following:

- In the row of the IoT connector you want to delete, right-click and select **Delete**.
- Select the IoT connector you want to delete, then click **Actions > Delete**.

OT Security deletes the IoT connector.

Note: After you delete an IoT connector, OT Security uninstalls the IoT Connector Agent from the application server. If you want to connect to the same application server via Agent, you must reinstall the [OT Security IoT Connector Agent](#).

Install IoT Connector Agent on Windows

Required Role: Administrator



OT Security allows you to map all managed Internet of Things (IoT) devices to their respective application server by configuring the IoT Connector engine and synchronizing assets from the specific application server. To connect your application server via Agent, you must install the OT Security IoT Connector Agent.

To install OT Security IoT Connector Agent:

1. Log in to the [Tenable Downloads](#) page.
2. Navigate to the **OT Security** page.
3. From the **Advanced IoT Visibility** section, download the **Windows IoT Connector Agent** package.

Advanced IoT Visibility			
Windows IoT Connector Agent	Tenable IoT Connector Agent for Windows Server 2012, Server 2016, Server 2019, Server 2022, 7, 8, 10, and 11(64-bit)(v341)	190 MB	Checksum
Ubuntu IoT Connector Agent	Tenable IoT Connector Agent for Ubuntu 20.x, 22.x, 24.x(amd64)(v341)	212 MB	Checksum

4. Copy the downloaded **Windows IoT Connector Agent** package to the application server where you want to install it.
5. Run the **Tenable IoT Connector Agent** wizard.

A message appears that the connector agent wizard is initializing and the **Welcome to the Tenable IoT Connector Agent Setup Wizard** window appears.

6. Click **Next**.

The **License Agreement** window appears.

7. Select **I accept the agreement** and click **Next**.

The **Select Destination Directory** window appears.

8. Specify the directory to install the IoT Connector Agent (or use the default directory) and click **Next**.

The Tenable IoT Connector Agent installation starts.



9. After the installation completes, verify that the Tenable IoT Connector Agent service is running.

- a. In the **Run** command window, type `services.msc`.

The **Services** window opens.

- b. Confirm that the **OT Security IoT Connector Agent** appears in the list of services currently running.

Once the installation is complete, you can connect your application server to OT Security. For more information about how to connect to the application server via a remote agent, see [Add IoT Connectors via Agent](#).

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

To enable sending event notifications via email to the relevant parties you need to set up an SMTP Server in the system. If you do not set up an SMTP server, the system cannot send out email notifications whenever events are generated. Under any circumstances, all events can be viewed in the Management Console (user interface) on the **Events** screen.

To set up an SMTP server:

1. Go to **Local Settings > Servers > SMTP Servers**.
2. Click **Add SMTP Server**.

The **SMTP Servers** configuration window appears.

SMTP Servers

Tenable	Hostname / IP:	10.0.0.12	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) <input type="password"/>				

3. In the **Server Name** box, type the name of an SMTP server you want to use for email notifications.
4. In the **Hostname\IP** box, type a hostname or an IP address of the SMTP server.
5. In the **Port** box, type the port number on which the SMTP server listens for the Events (Default: 25).
6. In the **Sender Email Address** box, type an email address that is shown as the sender of the Event notification email.
7. (Optional)In the **Username** and **Password** boxes, type a username and password that is used to access the SMTP server.
8. To send a test email to verify that the configuration was successful, click **Send Test Email**, then type 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.

Syslog Servers

To enable collection of log events on an external server you 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 are saved only on the OT Security platform.

To set up a Syslog server:

1. Go to **Local Settings >Servers > Syslog Servers**.
2. Click **+ Add Syslog Server**. The **Syslog Servers** configuration window appears.

Syslog Servers

SERVER NAME *

HOSTNAME / IP *

PORT *

TRANSPORT *

Send keep alive message every 10m0s
 Allow syslog message caching

[+ Add Syslog Server](#)



3. In the **Server Name** box, type the name of a Syslog Server you want to use for logging system events.
4. In the **Hostname\IP** box, type a hostname or an IP address of the Syslog server.
5. In the **Port** box, type the port number on the Syslog server to which the events are sent.
Default: 514
6. In the **Transport** drop-down box, select the transport protocol to be used. Options are TCP or UDP.
7. 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. (Optional) Select the **Send keep alive message every 10m0s** option to check the connection at frequent intervals.
9. (Optional) For TCP syslog, select the **Allow syslog message caching** option to cache events when the connection is disrupted and to send them once the connection is restored.

Note: UDP syslog messages do not have any state awareness and may be lost if the connection is interrupted.

10. Click **Save**.

You can set up additional Syslog Servers by repeating the procedure.

FortiGate Firewalls

To set up a FortiGate server:

1. Go to **Local Settings > Servers > FortiGate Firewalls**.
2. Click **Add Firewall**.

The **Add FortiGate Firewall** configuration window appears.

Add FortiGate Firewall ×

i 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** box, type the name of a FortiGate Server you want to use.
4. In the **Host/IP** box, type a hostname or an IP address of the FortiGate server.
5. In the **API Key** box, type the API token you generated from FortiGate.

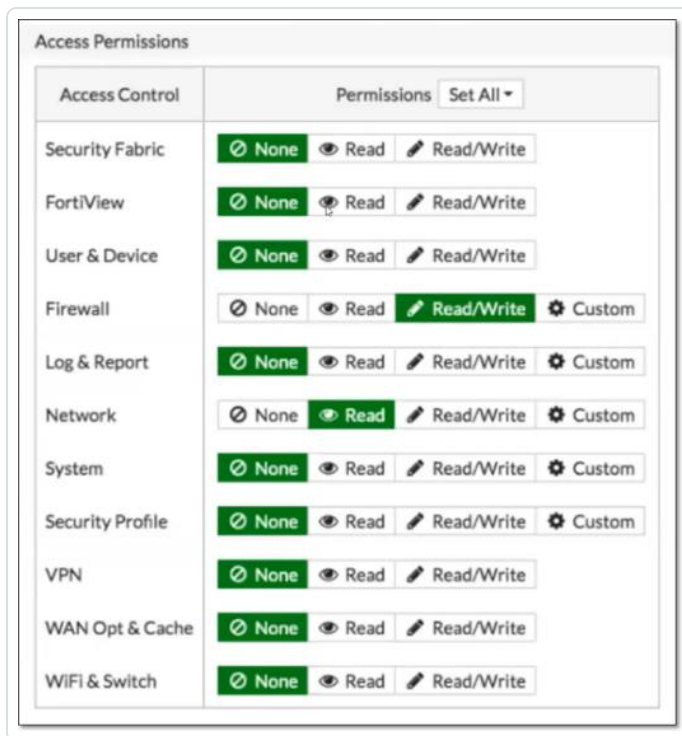
Note: For instructions on generating a FortiGate API token, see: https://registry.terraform.io/providers/fortinetdev/fortios/latest/docs/guides/fgt_token.

6. Click **Add**.

OT Security creates the FortiGate Firewall server.

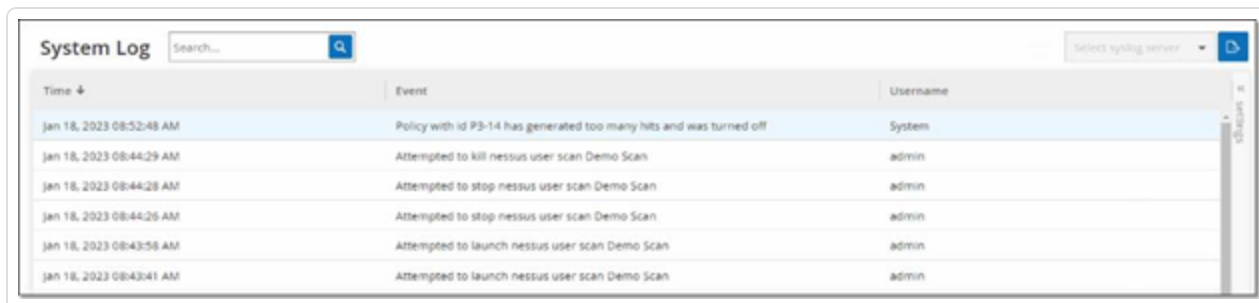
Note: For the source address (which is needed to ensure the API token can only be used from trusted hosts), use your OT Security unit IP address.

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



System Log

The **System Log** screen shows a list of all system events (for example, Policy turned on, Policy edited, Event Resolved, and so on.) that occurred in the system. This log includes both user-initiated events as well as automatically occurring system events (for example, Policy turned off automatically because of too many hits). This log does not include policy-generated events, which you can view on the **Events** screen. You can export the logs as a CSV file. You can also configure the system to send the System Log events to a Syslog server.



Each logged event includes the following details:

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



Time	The time and date when 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 **Local Settings > System Log**.
2. In the upper-right corner, click the drop-down box to display the list of servers.

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

3. Select the desired server.

OT Security sends the System Log events to the specified Syslog server.

Appendix – 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.

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 - Create the Tenable Application in Microsoft Entra ID



To create the Tenable application in Microsoft Entra ID:

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 appears.

2. In the **What's the name of your app?** field, enter a name for the application (for example 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.

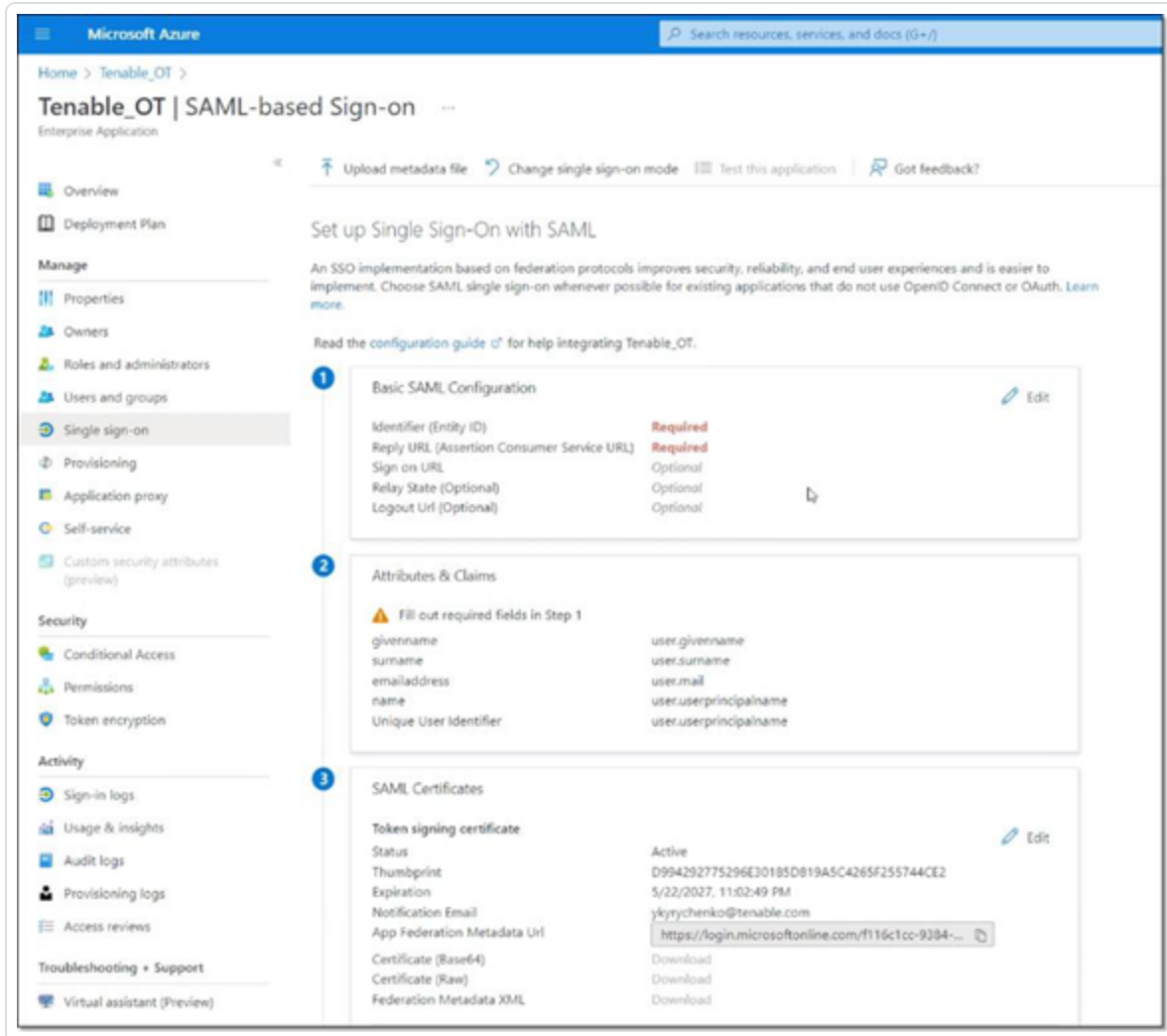
Note: Only fields specified in this procedure must be configured. Other fields may be left with their default values.



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 appears.



2. In section 1 – **Basic SAML Configuration**, click on Edit .

The **Basic SAML Configuration** side panel appears.



Basic SAML Configuration

Save | Got feedback?

Want to leave this preview of the SAML Configuration experience? Click here to leave the preview. →

Identifier (Entity ID) * ⓘ
The unique 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.
Add identifier

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.
Add reply URL



Sign on URL (Optional)
Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in 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 ✓

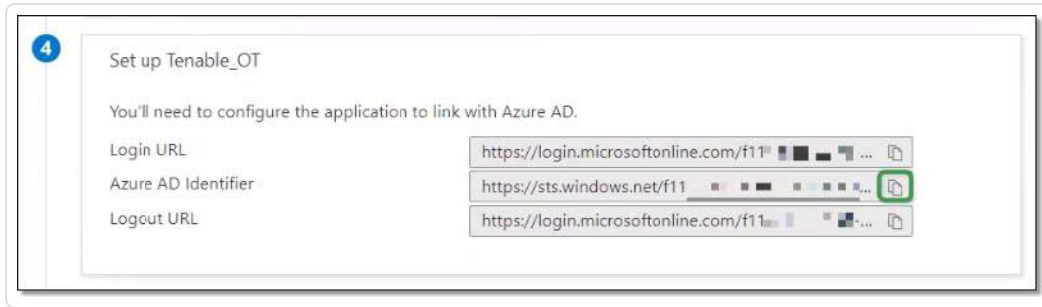
Relay State (Optional) ⓘ
The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.
Enter a relay state

Logout Url (Optional)
This URL is used to send the SAML logout response back to the application.
Enter a logout url ✓

3. In the **Identifier (Entity ID)** field, enter a temporary ID for the Tenable application (for example tenable_ot).
4. In the **Reply URL (Assertion Consumer Service URL)** field, enter a valid URL (for example https://OT Security).

Note: Both the Identifier and Reply URL is 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**.



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 *

IDP URL *

CERTIFICATE DATA *
 PEM format only
 Replace Current Certificate

USERNAME ATTRIBUTE *

GROUPS ATTRIBUTE *


DESCRIPTION

ADMINISTRATORS GROUP OBJECT ID

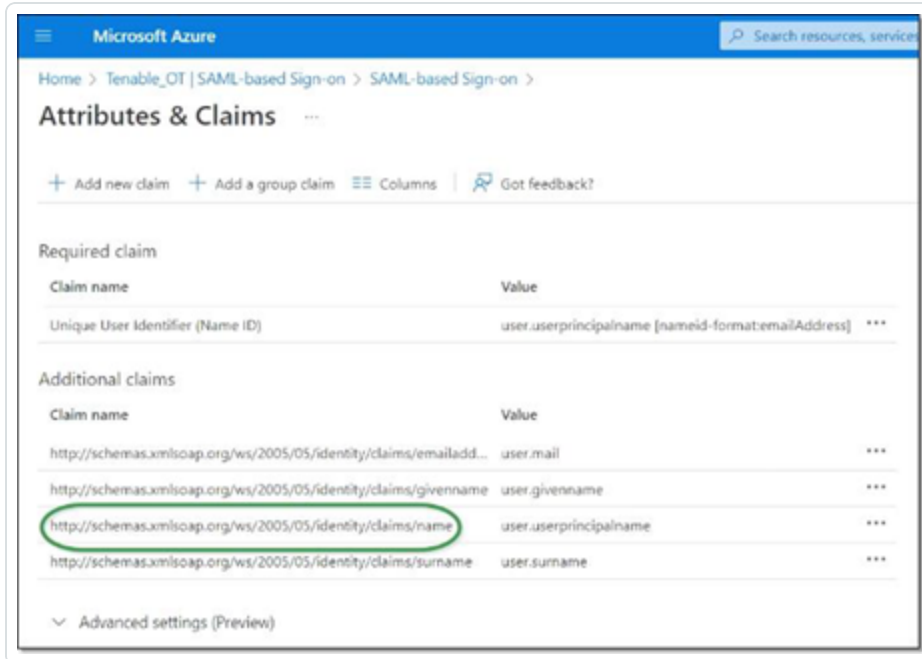
Cancel Save

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.



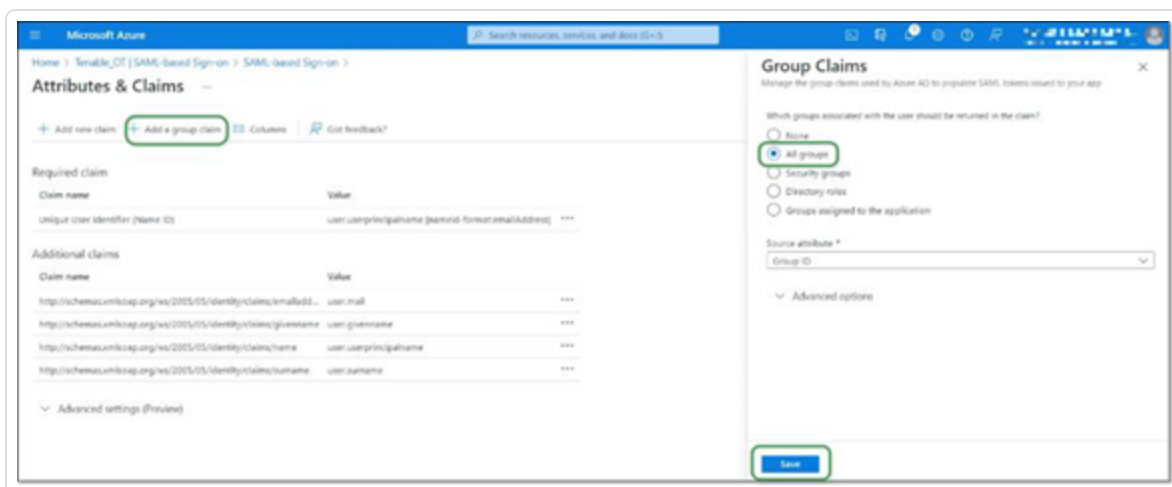
13. In the **Azure** console, in section 2 – **Attributes & Claims**, click  **Edit**.

14. Under **Additional claims**, select and copy the **Claim name** URL corresponding to the Value **user.userprincipalname**.



15. Return to the **Tenable** console and paste this URL in the **Username Attribute** field.

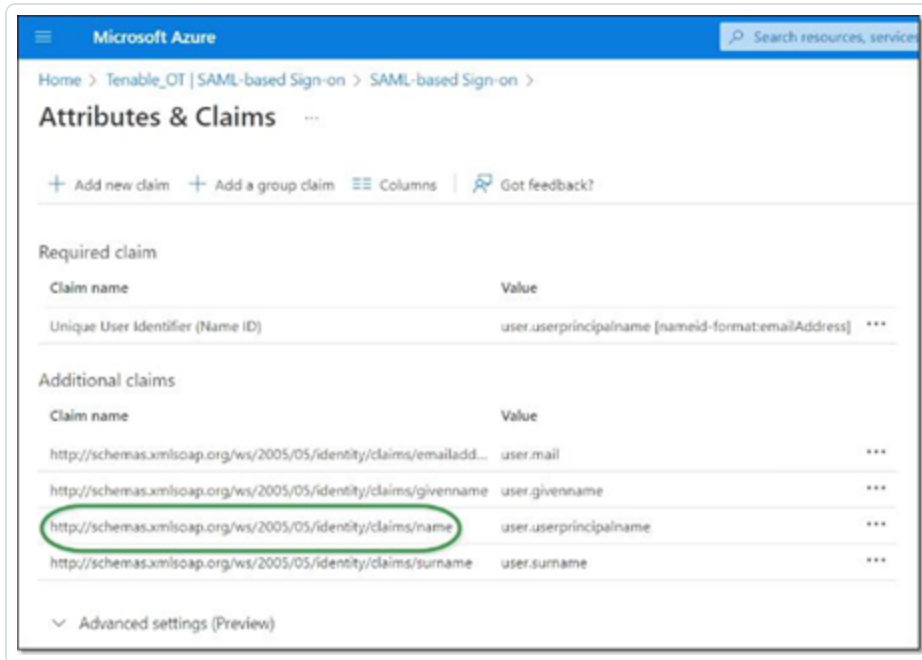
16. In the Azure console, click on **+ Add a group claim** to display the **Group Claims** side panel, and under **Which groups associated with the user should be returned in the claim?** Choose **All Groups** and click **Save**.





Note: If you have groups setting enabled in Microsoft Azure, you may choose Groups assigned to the application instead of All Groups, and Azure provides only the user groups that are assigned to the application.

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



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

Step 3 - Map Azure Users to Tenable Groups

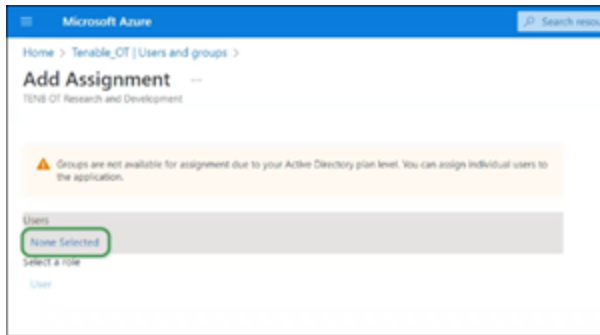
In this step, Microsoft Entra ID users are assigned to the OT Security application. The permissions granted to each user are designated by mapping between the Azure groups to which they are assigned and a pre-defined OT Security User Group, which has an associated role and set of permissions. The OT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

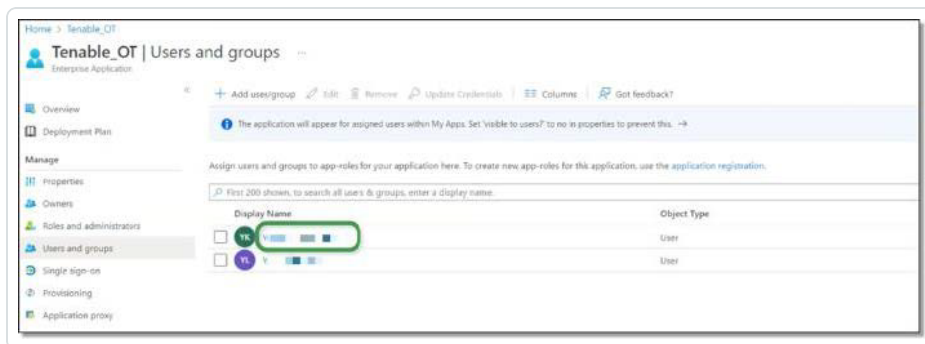
Note: If you have groups setting enabled in Microsoft Azure and have previously selected **Groups assigned to the application** instead of All Groups, you may choose to assign groups instead of individual users.

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

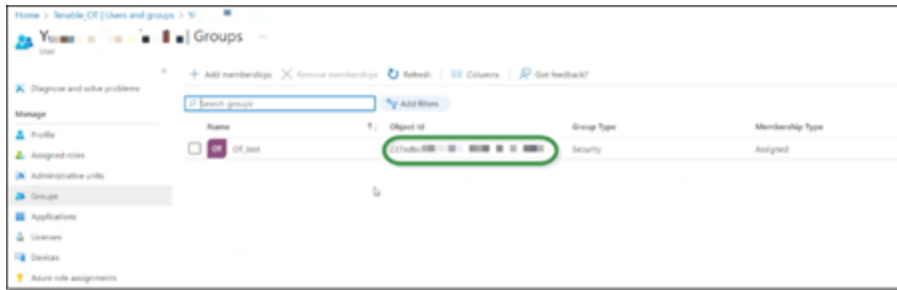


The **Users and groups** page appears.

- Click on the **Display Name** of a user (or group) to display that user's (or group's) Profile.



- In the **Profile** screen, in the left-side navigation bar, select **Groups** to display the **Groups** screen.
- 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 (for example 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 [X]

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

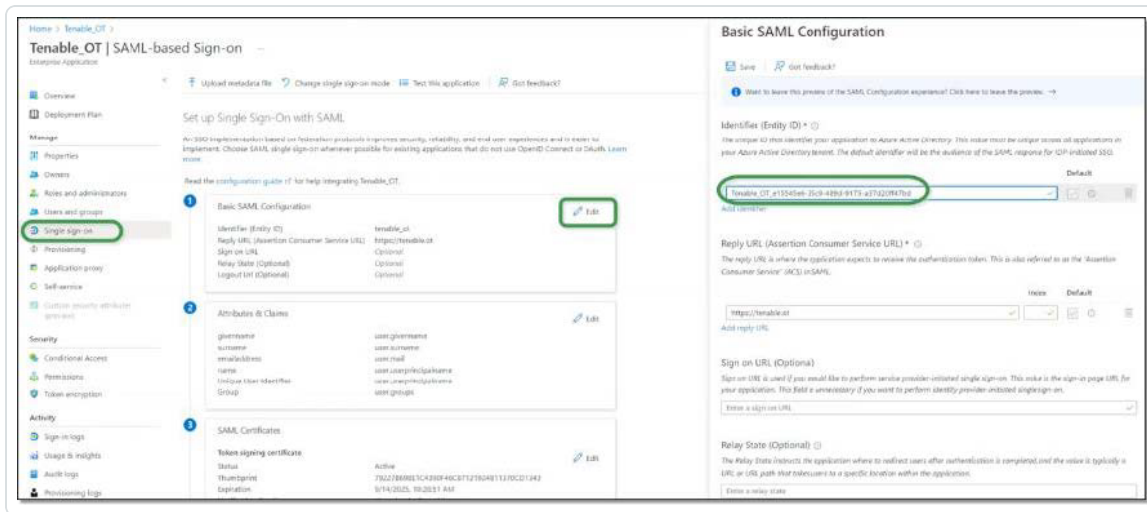
SITE OPERATORS GROUP OBJECT ID


SUPERVISORS GROUP OBJECT ID

Cancel Save

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

- 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.



- Return to the OT Security **SAML** screen, and under **URL**, click the copy icon.
- 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.
- Click  **Save** to save the configuration, and close the side panel.

The configuration is complete, and the connection appears on the **Azure Enterprise applications** screen.

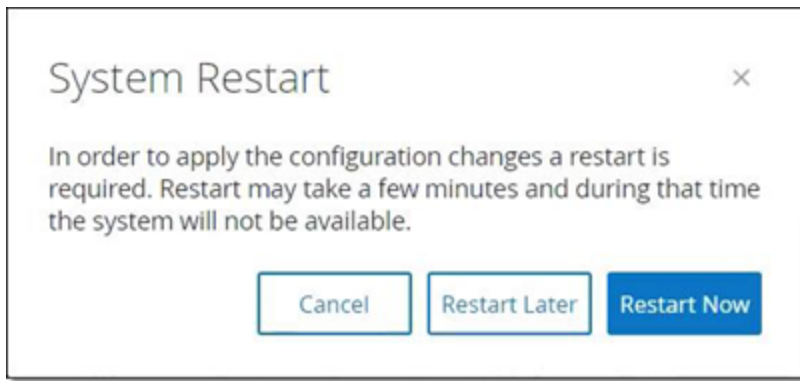
Step 5 – Activate the Integration

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:

- 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 appears.



2. Click **Restart Now** to restart the system and apply the SAML configuration immediately, or click **Restart Late** 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 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
2.9	July 25, 2023	Updated for version 3.16
3.0	September 11, 2023	Updated for version 3.17
3.1	March 15, 2024	Updated for version 3.18
3.2	July 30, 2024	Updated for version 3.19