Tenable OT Security 4.7 User Guide

Last Revised: June 24, 2026

Copyright © 2026 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Table of Contents

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.

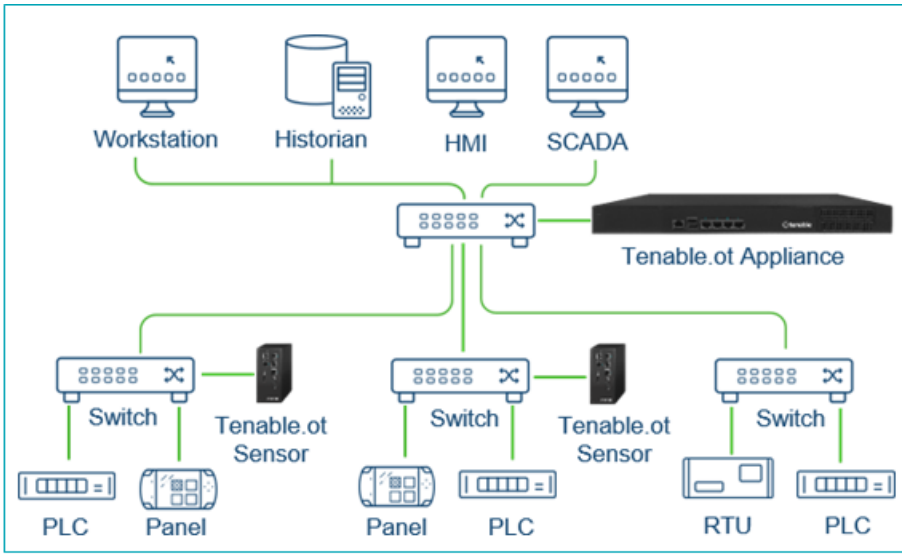
Solution Architecture

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 integrations[1].

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

Tenable OT Security Hardware Specifications

ICP and Sensor Specifications

The following are the specifications for the OT Security hardware appliances for Industrial Core Platform (ICP):

Regular ICP

Category	Regular ICP
CPU	Intel® Xeon™ D-218dIT, 2.0 GHz
Cores	14
RAM	64 GB
Storage	256 GB SSD 800 GB NVMe 2 TB HDD
Network (Copper Ethernet)	4 x 1 Gbps
Network (Fiber Ethernet)	N/A
Power Supply	Single 110-220v
Form Factor	1U Half Depth
Dimensions (LxWxH)	209 x 43 x 376 mm 8.2 x 1.7 x 14.8 in
Weight	3.6 Kg
Operating Temperature	5 ~ 45° C (41 ~ 113 F)
Relative Humidity	8% ~ 90% non-condensing
Max Span Throughput	500 Mbps

XL ICP

Category	XL ICP

CPU	2x Xeon® Silver 4314
Cores	2 x 16
RAM	256 GB
Storage	960 GB SSD SAS FIPS-140 SED 960 GB SSD SAS FIPS-140 SED 2X2.4TB SAS HDD FIPS-140 SED Note: The hardware supports full encryption and is FIPS-140 compliant.
Network (Copper)	6 x 1 Gbps
Network (Fiber)	2 x 10 GB SFP+
Power Supply	Redundant 110-220v, 165W
Form Factor	1U Full Depth
Dimensions (WxHxD)	Width*: 482.0mm (18.98”) x Height: 42.8mm (1.69”) x Depth*: 698 mm (27.5”) *Dimensions include bezel.
Weight	22 Kg
Operating Temperature	0 ~ 40° C (32 ~ 104 F)
Storage Temperature	-10 ~ 50° C (14 ~ 122° F)
Relative Humidity	5% ~ 90% non-condensing

Certifications	CE / FCC/ RoHS CB, CCC, UL, RCM, NOM
Max Span Throughput	1 Gbps

ICP-Mini

Category	ICP-Mini
CPU	Intel® Core™ i7-1185G7E, 1.8GHz
Cores	4
RAM	32 GB
Storage	480GB SSD
Network (Copper)	4 x 2.5 Gbps
Network (Fiber)	N/A
Power Supply	Terminal Block 12~28 VDC
Form Factor	DIN-Rail
Dimensions (mm)	150 x 190 x 81 mm
Weight	1.9 Kg
Operating Temperature	0 ~ 40° C (32 ~104° F)
Storage Temperature	-10 ~ 50° C (14 ~ 122° F)
Relative Humidity	10% ~ 95% non-condensing

Certification	CE / FCC / RoHS Class A CB, CCC, UL, ROM, NOM
Max Span Throughput	150 Mbps

Sensor

Category	Sensor
CPU	Intel® Core™ 13-8145UE, 2.2GHz
Cores	2
RAM	4 GB
Storage	128GB SATA M.2
Network (Copper)	2 x 1 Gbps
Network (Fiber)	N/A
Power Supply	Terminal Block 12~28 VDC
Form Factor	Extra Small Form Factor
Dimensions (WxHxD)	179 x 88 x 34.5 mm 7.05 x 3.46 x 1.36 in
Weight	0.72 Kg
Operating Temperature	0 ~ 50° C (32 ~ 122° F)
Storage Temperature	-40 ~ 60° C (-40 ~ 140° F)
Relative Humidity	20% ~ 80% non-condensing

Max Span Throughput	NA

System Elements

Assets

Assets are the hardware components in your network such as controllers, engineering stations, and servers. 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 and vulnerable open ports). 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.

Important! To purchase Tenable products, contact your Tenable Representative.

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.

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.

Note: While you can connect a standalone purchase of OT Security to your instance of Tenable One, that does not handle the licensing of those assets. Tenable One customers have a plethora of Tenable solutions that are licensed to them, including OT Security, but the licenses must be part of the Tenable One license first. You can work with your customer success managers (CSM) to update the account accordingly.

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
• Virtual Core Appliance. • Tenable Security Center.	• 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.

Operational Playbooks

Operational Playbooks are guides designed to help you achieve specific security outcomes by using actionable workflows. Irrespective of your role in the OT organization, these playbooks provide standardized procedures to secure your Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) environments.

These playbooks use the multi-engine detection capabilities of OT Security including asset inventory, vulnerability management, and threat detection to help you maintain a resilient posture.

Each workflow includes the following:

- An objective or a specific goal you are trying to achieve.
- The step-by-step paths within the OT Security interface.
- The measurable result after executing the workflow.

Prerequisites

Before executing these playbooks, ensure your network has the following:

- Asset Discovery: Make sure OT Security monitors at least one network segment using passive discovery or active querying to populate the inventory.
- User Permissions: Make sure that you have the necessary user roles to view dashboards and initiate scans.

Operational Workflows

To get started, see these workflows:

- Prioritize and Mitigate Vulnerabilities – Prioritize remediation based on actual threat levels (VPR) rather than just CVSS scores.
- Investigate and Respond to Network Threats – Detect and investigate anomalies, malware, or unauthorized network scans.

Prioritize and Mitigate Vulnerabilities

OT Security identifies threats including CVEs, vulnerable protocols, and open ports. It utilizes Vulnerability Priority Rating (VPR) to generate risk scores for each vulnerability, allowing teams to focus on high-risk vulnerabilities that are actively exploitable rather than just those with high Common Vulnerability Scoring System (CVSS) scores.

VPR is the Tenable-calculated score based on the technical impact and threat intelligence for a vulnerability. For more information about VPR and how it differs from CVSS, see this blog.

Objective

Move from a reactive "patch everything" approach to a risk-based strategy by identifying and remediating the vulnerabilities that pose the greatest actual threat to the operational environment.

Prerequisites

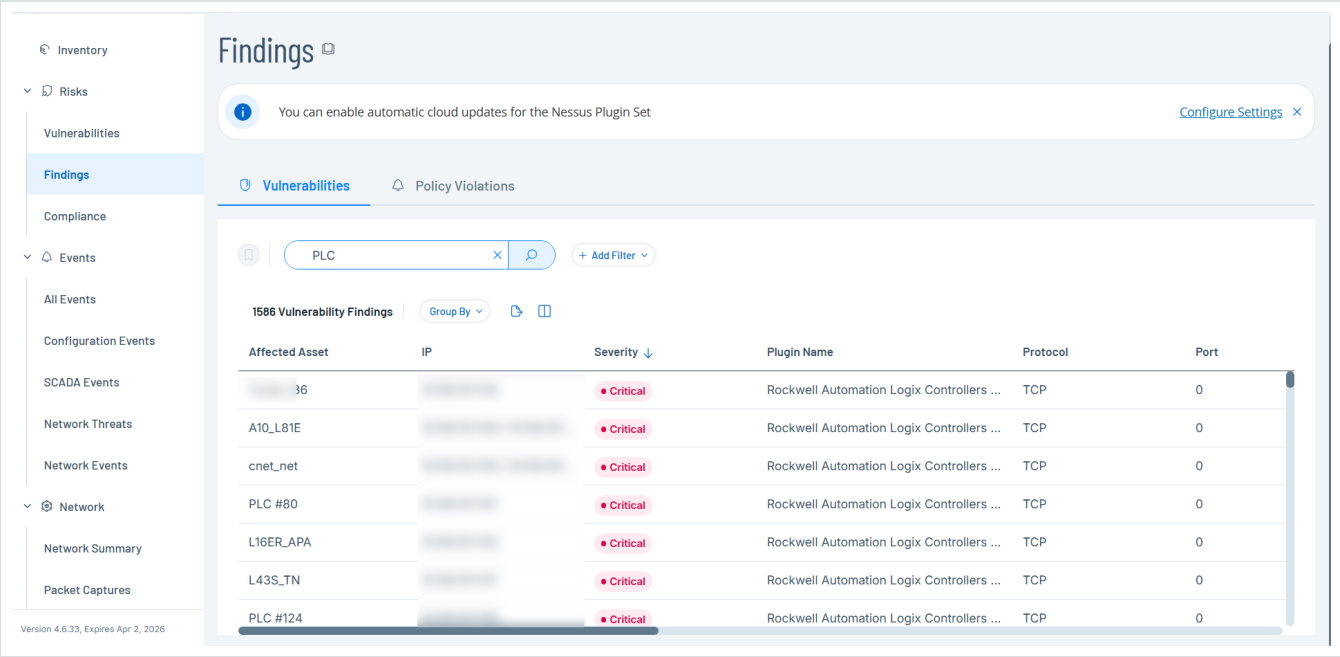
- OT Security must have identified assets via passive or active discovery.
- (Optional) Integration with Tenable Vulnerability Management or Tenable Security Center for unified scoring.

Step 1: View the Risk Dashboard

1. Log in to OT Security.
2. In the left navigation menu, click Risks > Findings.

   The Findings page appears with the default Vulnerabilities tab, displaying all network threats,

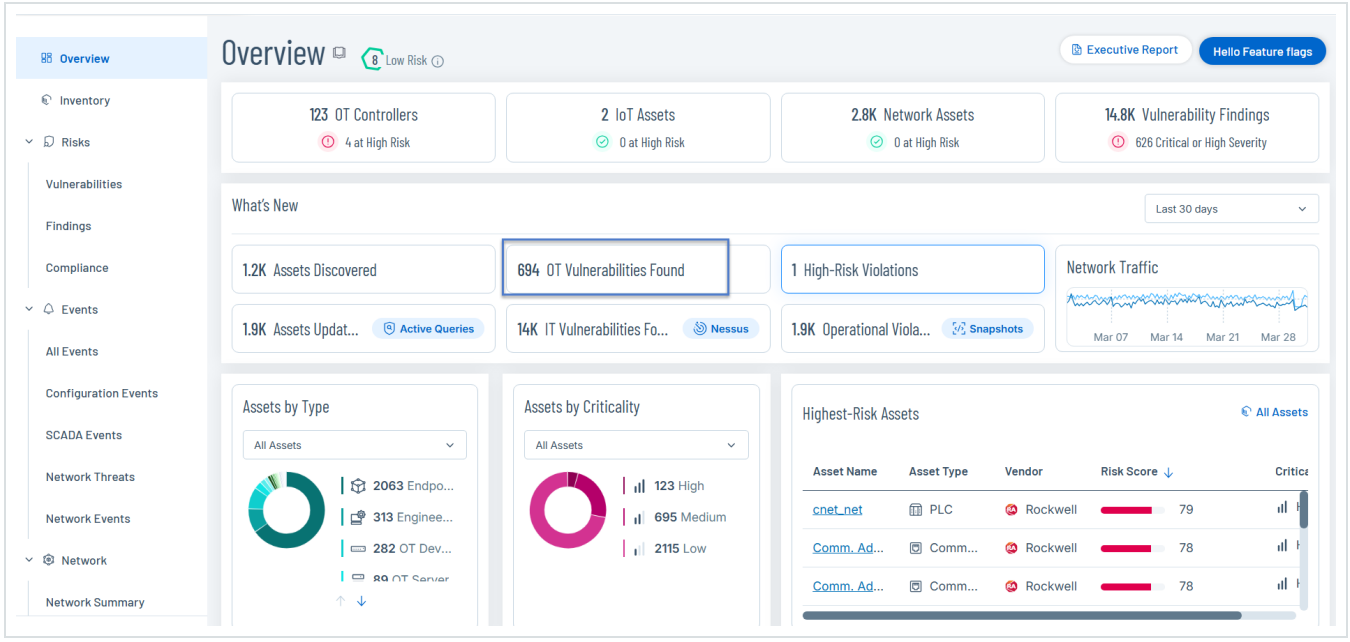
including CVEs and vulnerable protocols.



Step 2: Prioritize by Severity and Asset Criticality

1. Sort the vulnerability list by VPR or Severity (Critical or High) to identify top threats.
2. Use the Add Filter button to filter the view to focus on critical asset categories, such as Controllers (PLCs) or Engineering Stations.

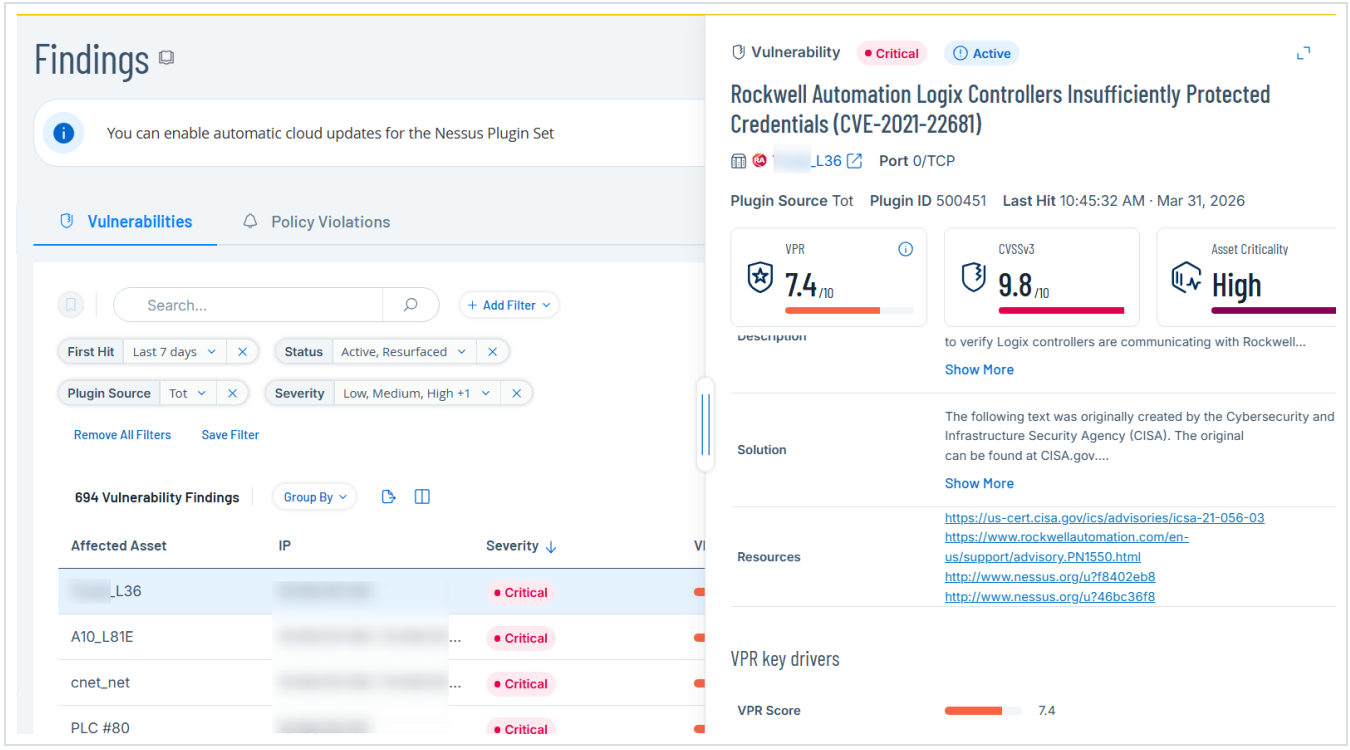
   The Vulnerabilities list displays the filtered results.
3. Alternatively, review the Vulnerabilities widget on the Overview dashboard to see the distribution of severity across asset types.



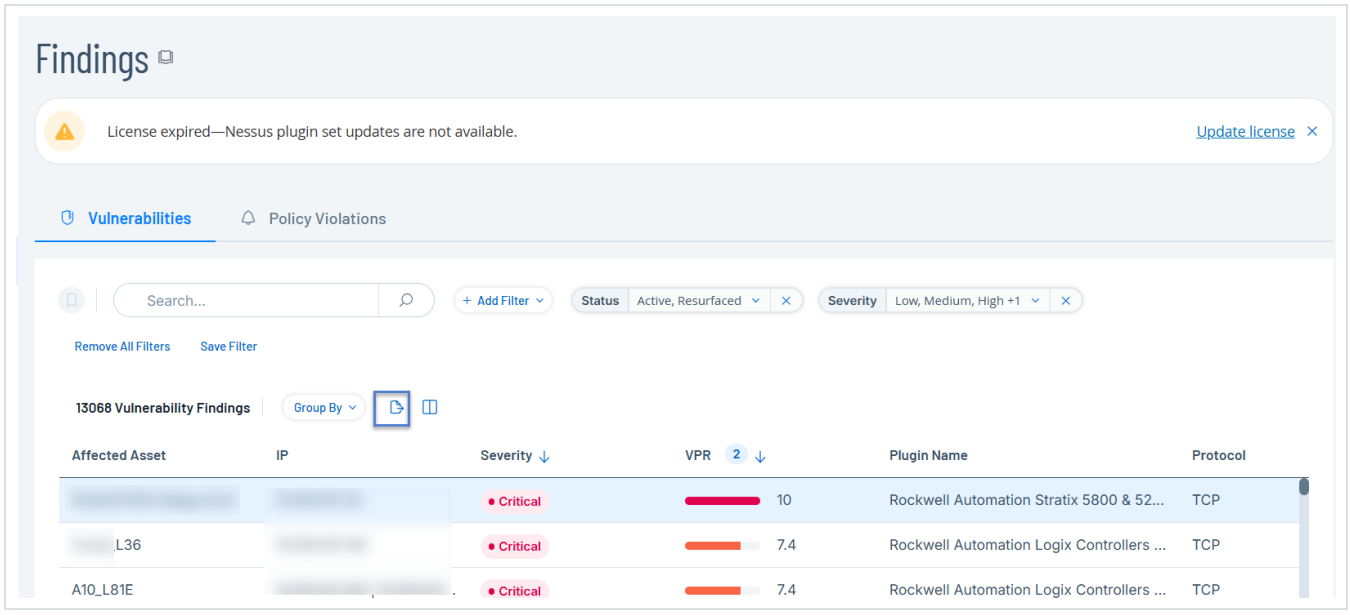
- Click the OT Vulnerabilities widget to drill down into the Findings page.

Step 3: Analyze Remediation Options

1. In the Findings page, click a specific asset to open the Asset Details panel.
2. Click a specific vulnerability to review the detailed insights and mitigation suggestions provided for the specific CVE or vulnerability.



3. On the Findings page, click the Export button to export the data to share with other teams and stakeholders.



Tip: If you integrated OT Security with Tenable One or Tenable Security Center, you can further analyze the findings within these applications. For more information about integrating Tenable One or Tenable Security Center, see Integrations.

Outcome

You have a prioritized list of vulnerabilities relevant to your exact environment, enabling the efficient allocation of maintenance resources to reduce the greatest risk.

Investigate and Respond to Network Threats

OT Security employs multiple detection engines, including behavioral anomalies, signature-based detection (Suricata), and policy-based rules to identify traffic indicative of cyberattacks.

Objective

Detect and investigate suspicious network activity, such as unauthorized scans, malware propagation, or protocol anomalies, to prevent operational disruption.

Prerequisites

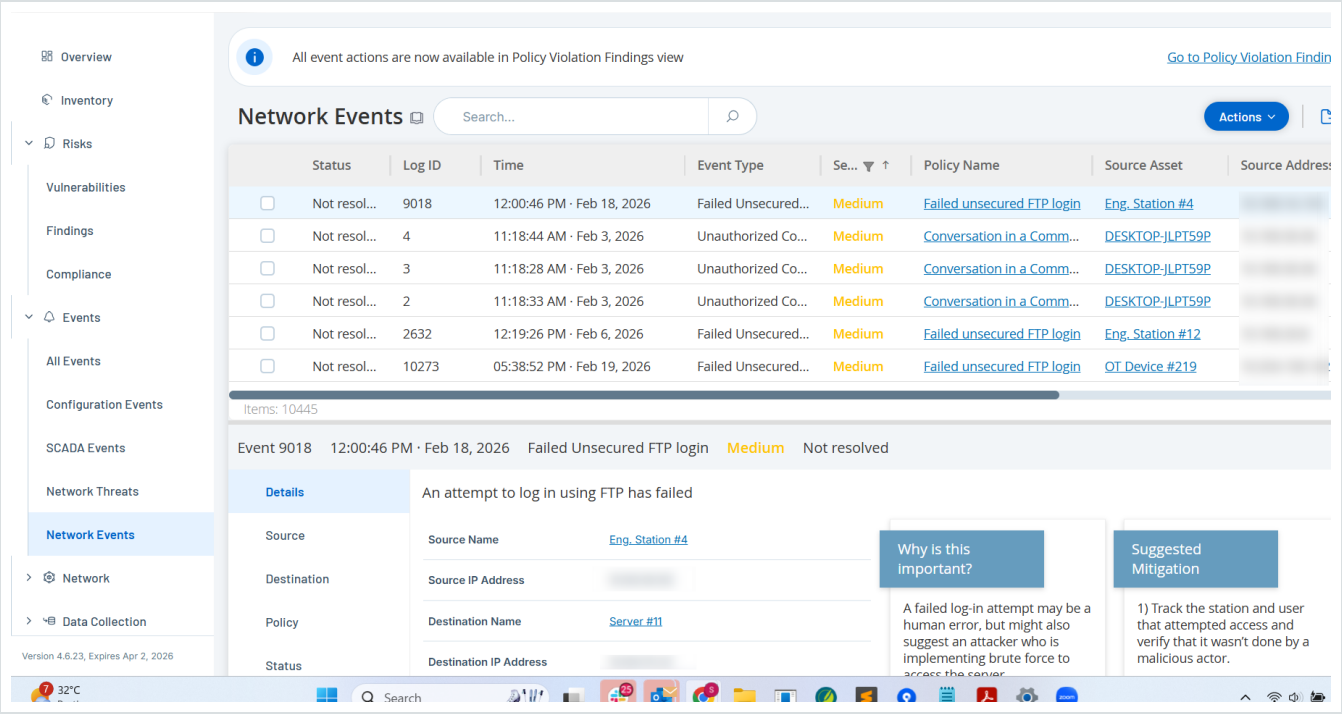
You must have the required permissions to view events.

Make sure that you configure the following:

- Configure network monitoring. See Monitored Networks.
- Enable detection policies. See Enable or Disable Policies.
- (Optional) Enable PCAP capture for forensic analysis. See Download Individual Capture Files.

Step 1: Monitor Event Alerts

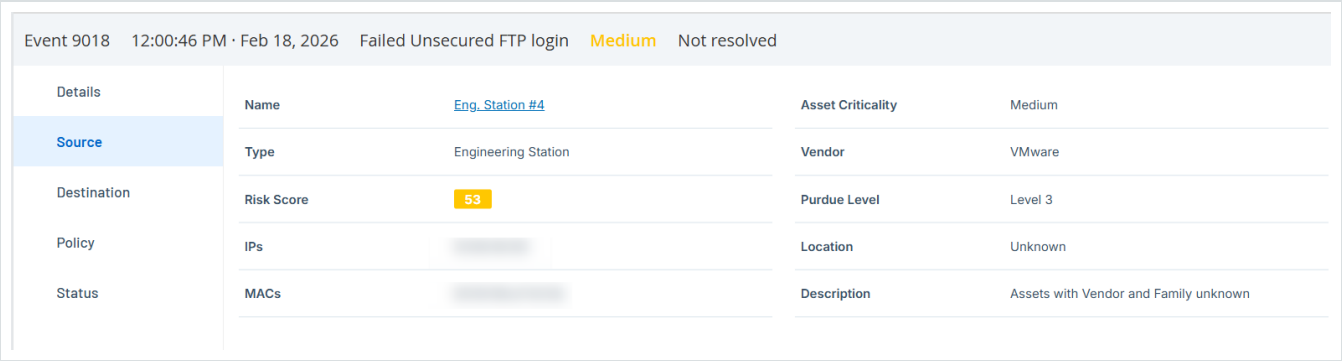
1. Log in to OT Security.
2. In the left navigation menu, click Events.
3. Select Network Threats or Network Events to view alerts related to intrusion attempts or abnormal traffic.



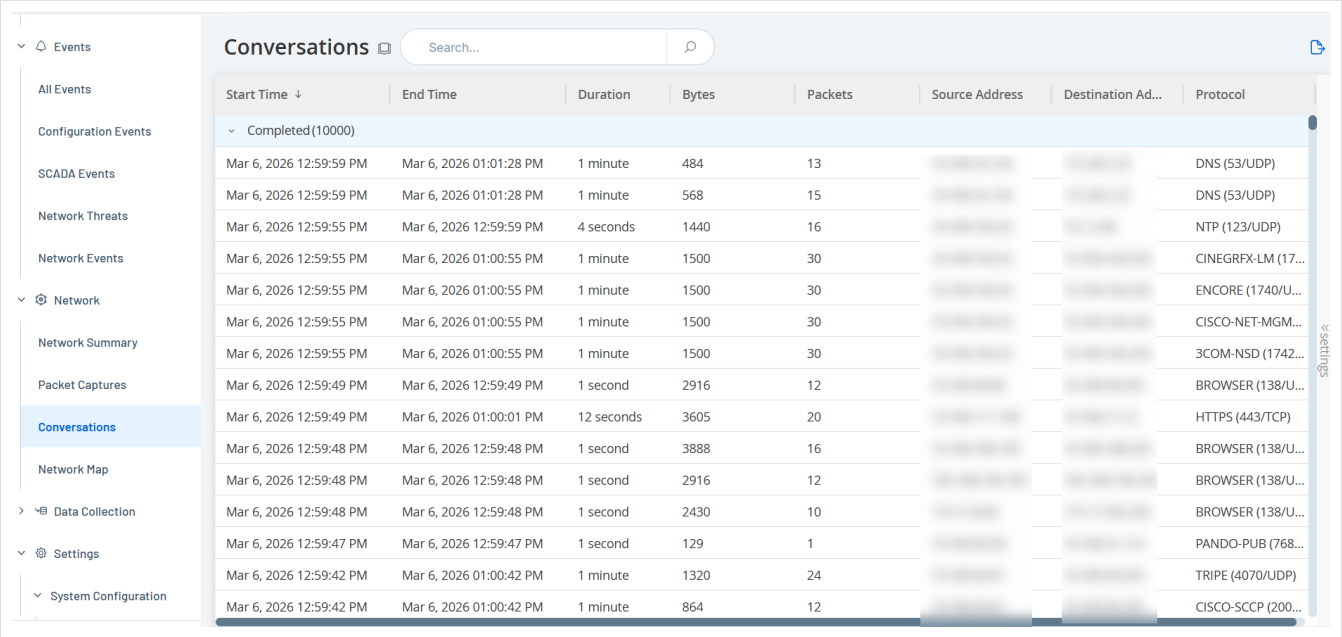
4. Sort events by Severity (High or Critical) to triage immediate threats.

Step 2: Analyze Conversation Data

1. Select a specific event to view the Event Details panel.
2. Identify the Source and Destination assets involved in the suspicious activity.



3. Navigate to the Network > Conversations page to view the specific traffic flows between these assets.



4. If available, use the Packet Captures (PCAP) view to analyze the raw traffic data for forensic evidence. See Download Individual Capture Files.

Step 3: Initiate Response

- Review the Suggested Mitigation in the Event details section and take action (e.g., isolate the compromised asset).

- If the event is a false positive, adjust the policy configuration to fine-tune detection and reduce noise. See Policies.
- In Findings > Policy Violations, mark the event as Resolved to clear it from the active queue. See Policy Violations.

Outcome

You can rapidly identify the "who, what, where, and when" of a security incident, minimizing the Mean Time to Respond (MTTR).

Error Messages

The following table describes the error messages that may appear in Tenable OT Security.

Category	Error Category Name	Error Description	User Interface Message	Recommended Action
Active Query Management	NoRoutesForClient	A query received a routing error from the network.	There may be a network connectivity issue. Please check network connectivity and retry the query.	Check your network connectivity and retry the active query.
Active Query Management	InternalError	An internal	An	Retry the

		error occurred in the query attempt.	unexpected error occurred. Try again later, and if the issue persists, contact Technical Support.	query after some time. If the issue persists, contact Tenable Support.
Active Query Management	DnsError	A DNS hostname not found for the target IP.	A DNS hostname could not be found for the target IP. Please ensure that reverse DNS is enabled and a PTR record is defined for the IP.	Verify if the reverse DNS Lookup is enabled and the DNS pointer record (PTR) is defined for the IP.
Active Query Management	HostUnreachableError	A query target cannot be reached. Check your routing.	Could not reach the device. This might be due to a network connectivity	Check your network connectivity and firewall settings and retry the

			issue. Please check your network or firewall settings and try again.	active query.
Active Query Management	TimeoutError	A query has received no response from the target and reached timeout.	Network Timeout. This may be due to temporary network issues or a slow response from the device. Please try the query again later.	Retry the query after some time.
Active Query Management	NetworkError	A query has received an error response from the network.	A network error has occurred. This may be due to temporary network issues or	Check your network connectivity and retry the query.

			firewall restrictions. Please check your network connectivity and retry the query.	
Active Query Management	ProtocolError	A query has received an unexpected response from the target.	Unsupported response format from the destination. This could be due to an incompatible protocol version on the device or a temporary network issue. Please check device compatibility or try the query again later.	Check whether the destination device is compatible with or retry the query after some time.

Active Query Management	AuthenticationError	Invalid authenticati on credentials were used in the query.	Failed to authenticate to the device. Credentials may be incorrect or missing, Please verify your credentials.	Verify your credentials and retry the query.
Active Query Management	LimitExceededError	OT Security has reached the limit for failed queries against the target.	Active queries to this device are paused due to too many failed queries. Try again later and If the issue persists, contact support	There are several failed queries to the device. Retry the query after some time, and if the issue persists, contact Technical Support.
Active Query Management	NoPotentialClients	No valid clients exist in the target query range (CIDR	Active query found no accessible devices in the target	The target devices may not be accessible because of

		block, asset list, or IP range).	range. User-applied restrictions might block some devices (CIDR block, asset list, or IP range). Please review your selection and access controls.	user-applied restrictions. Review your access control settings and retry the query.
Active Query Management	NoAllowedClients	No allowed clients exist in the target query range (CIDR block, asset list, or IP range).	Active query found no compatible devices in the target range (CIDR block, asset list, or IP range). Please review your selection and access controls.	The target devices may not be compatible with OT Security settings. Review your access control settings and retry the query.
IoT	ServiceUnavailable	Service is	The IoT	Retry the

		unavailable, may be and issue with startup or after reset.	Connector Service is not available or has encountered an issue, try again later and if the issue persists, contact support.	query after some time as the IoT Connector service may be temporarily down. If the issue persists, contact Technical Support.
IoT	IotConnectorSecureModeError	The IoT connector cannot connect with a remote installed IoT agent.	IoT connector secure mode error. The IoT Agent on the remote system must be reinstalled to allow connections again.	Reinstall the IoT Agent on the remote system and retry the connection.
IoT	IotConnectorIpAlreadyExists	The user is trying to add a connector with an IP	Connector creation failed. The provided IP	Provide a unique IP address and try to add the

		that already exists.	address is already in use by another connector. Please provide a unique IP address and try again.	connector.
Server Pairing: (Enterprise Manager (EM), External Server, FW)	WrongCertificate	The user is trying to pair ICP to EM with an invalid certificate.	The pairing server presented an invalid security certificate. Please verify the server certificate and try again. If this persists, consult the server administrator.	Generate a new security certificate and try pairing the ICP to EM. If the issue persists, contact the server administrator.
Server Pairing: (EM, External Server, FW)	MissingEmAddress	Only via API	No server address was provided for	Provide the IP address or hostname of

			pairing. Please enter the IP address or hostname of the server you want to connect to and try again.	the server you want to connect and try again.
Server Pairing: (EM, External Server, FW)	MissingPassword	Only via API	The provided credentials are incomplete. Please enter a password for the pairing server and try again.	Provide a username and password for the server and try again.
Server Pairing: (EM, External Server, FW)	MissingCredentials	Only via API	Missing connection credentials for the pairing server. Please provide the	Provide valid credentials for the server and try again.

			required credentials (e.g., username and password) and try again.	
Server Pairing: (EM, External Server, FW)	BothApiKeyAndUserCredentials	Only via API	Only one authentication method is allowed for pairing with this server. Please remove either the API key or user credentials and try again.	Use either API key or user credentials for pairing.
OT Feeds: PII/Suricata/Nessus	NessusNotReady	Service is unavailable, may be an issue with startup or after reset.	The Nessus service is not yet available or has encountered an issue, try	The Nessus service may be down, so try reaching the service after some time, or if the

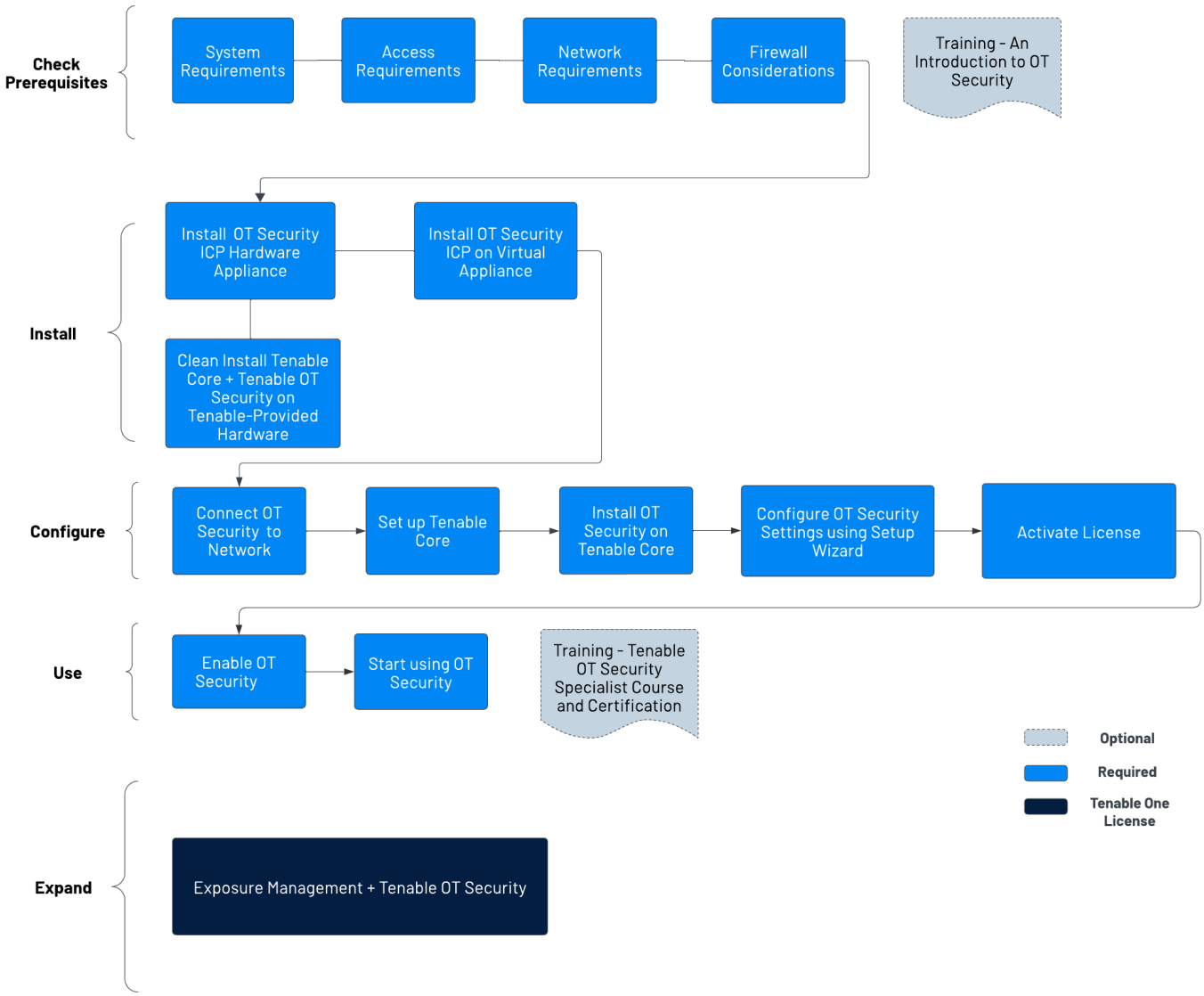
			again later, and If the issue persists, contact support.	issue persists, contact Tenable Support.
OT Feeds: PII/Suricata/Nessus	MissingFile	Only via API	No configuration file attached. Please upload a valid configuration file in the supported format to proceed.	Upload a valid configuration file.
OT Feeds: PII/Suricata/Nessus	InvalidFile	The uploaded file is invalid.	The uploaded file is invalid. It may be due to an unsupported format or missing version information. Please	Check whether the format or version of the uploaded file is valid before uploading the file.

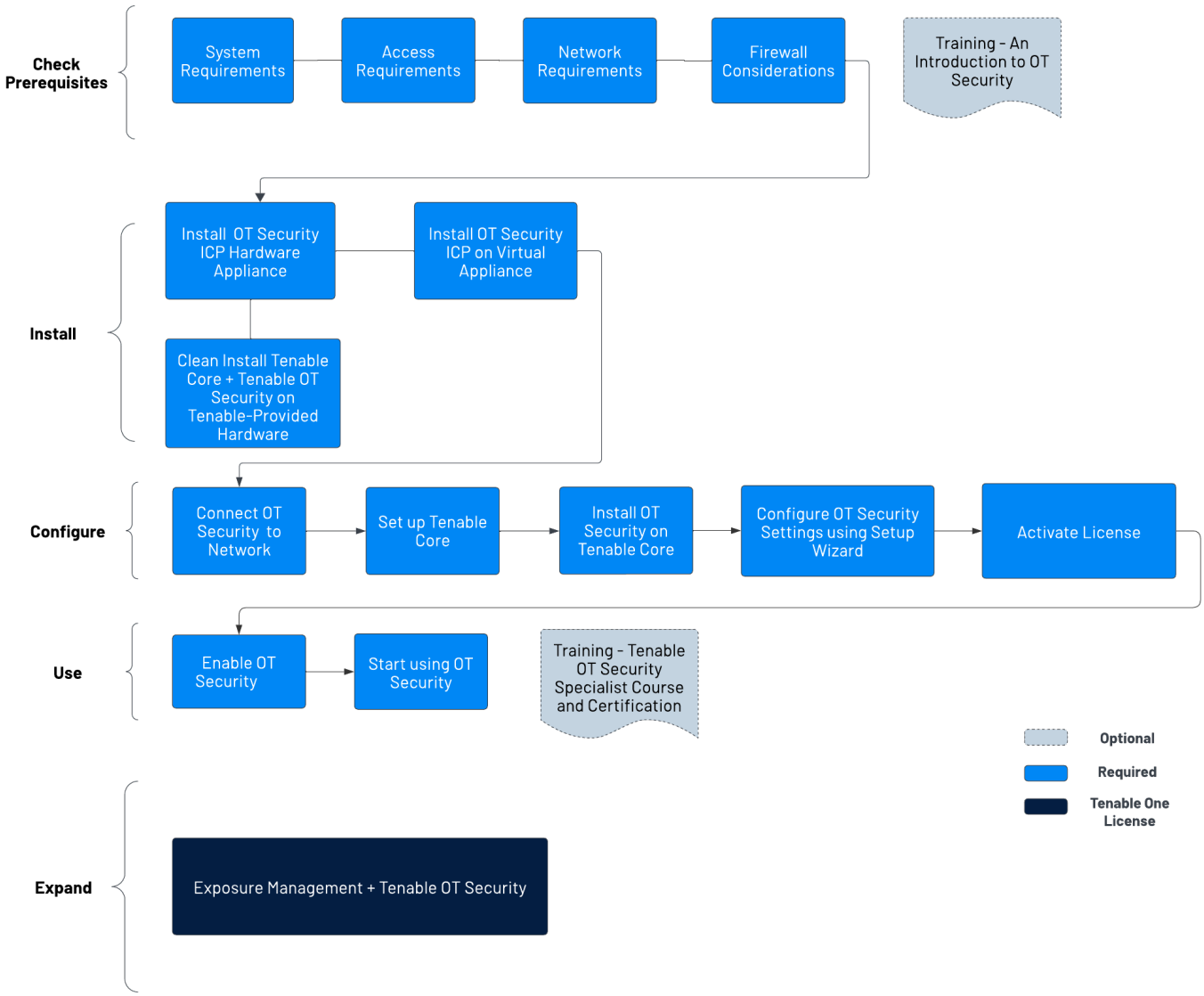
			review the documentation for supported formats and required fields, and try again.	
OT Feeds: PII/Suricata/Nessus	NoSpaceLeftOnDevice	Uploading a file during online or offline mode while there is no space left on the device for the new one.	The device does not have enough storage space to accommodate the new configuration file. Please free up some space on the device and try again.	Free up space on the device and try uploading the configuration file.
OT Feeds: PII/Suricata/Nessus	OldLicense	The user is using a license without valid credentials.	Action not allowed due to an outdated version format. Please	Upgrade your OT Security license in the supported format.

			obtain a new license in the supported format and try again.	
OT Feeds: PII/Suricata/Nessus	UpdateAlreadyInProgress	The user is currently running an update while there is already one job in progress, and only one update can run at a time.	An update is already in progress for this device. Please wait for the current update to finish before attempting another one.	Wait for the current update to complete before you try again.
OT Feeds: PII/Suricata/Nessus	OlderVersionUpdateAttempt	The user is attempting to downgrade to an earlier version.	File upload failed due to an active newer version. Ensure you have the latest updated file and try uploading again.	Ensure the file you are trying to upload is the latest version.

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, and authentication servers 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:

- Access the **Exposure View** page, where you can 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:
    - View and manage cyber exposure cards.
    - View CES and CES trend data for the Global and Operational Technologies exposure cards.
    - View Remediation Service Level Agreement (SLA) data.
    - View Tag Performance data.
- Access the **Exposure Signals** page, where you can generate exposure signals that use queries to search for asset *violations*. Simply put, if an asset is impacted by a weakness related to the query, then the asset is considered a *violation*. Using this, you can gain visibility into your most critical risk scenarios.
    - Find top active threats in your environment with up-to-date feeds from Tenable Research.
    - View, generate, and interact with the data from queries and their impacted asset violations.
    - Create custom exposure signals to view business-specific risks and weaknesses
- Access the **Inventory** page, 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:

- View and interact with the data on the **Assets** tab:
  - Review your AD assets to understand the strategic nature of the interface. This should help set your expectations on what features to use within Tenable Exposure Management, and when.
  - Familiarize yourself with the Global Asset Search and its objects and properties. Bookmark custom queries for later use.
  - Find devices, user accounts, software, cloud assets, SaaS applications, networks, and their weaknesses.
  - Drill down into the **Asset Details** page to view asset properties and all associated context views.
- View and interact with the data on the **Weaknesses** tab:
  - View key context on vulnerability and misconfiguration weaknesses to make the most impactful remediation decisions.
- View and interact with the data on the **Software** tab:
  - Gain full visibility of the software deployed across your business and better understand the associated risks.
  - Identify what software may be out of date, and which pieces of software may soon be End of Life (EoL).
- View and interact with the data on the **Findings** tab:
  - View instances of weaknesses (vulnerabilities or misconfigurations) appearing on an asset, identified uniquely by plugin ID, port, and protocol.
  - Review insights into those findings, including descriptions, assets affected,

criticality, and more to identify potential security risks, visibility on under-utilized resources, and support compliance efforts.

- Access the **Attack Path** page, where you can optimize risk prioritization by exposing risky attack paths that traverse the attack surface, including web apps, IT, OT, IoT, identities, ASM, and prevent material impact. Streamline mitigation by identifying choke points to disrupt attack paths with mitigation guidance, and gain deep expertise with AI insights (Not supported in FedRAMP environments).
    - View the **Dashboard** tab 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 attack techniques 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 paths leading to 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.
    - On the **Top Attack Techniques** tab, 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 attack techniques, which allow you to understand and act on the unknowns that enable and amplify threat impact on your assets and information.
    - On the **Top Attack Paths** tab, generate attack path queries to view your assets as part of potential attack paths:

        - Generate an Attack Path with a Built-in Query
        - Generate an Attack Path Query with the Attack Path Query Builder
        - Generate an Asset Query with the Asset 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.

    - Interact with the **MITRE ATT&CK Heatmap** tab, select the ICS heatmap option to focus on ICS (Industrial Control Systems) tactics and techniques

- View and interact with the data in the **Tags** page:
    - Create a new dynamic tag for your OT assets, where:
        - Operator = Host System Type
        - Value = PLC
    - Create and manage tags to highlight or combine different asset classes.
    - View the **Tag Details** page to gain further insight into the tags associated with your assets.

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

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.

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

Tip: OT Security offers turnkey appliances that ship directly that come pre-imaged. This option is much easier to use and deploy, with a faster time to value. However, you can also source your own hardware and apply our ISO image to it. If you supply your own or choose to use ours, please refer to our Tenable OT hardware specs as a guideline or best practice. All components of OT Security, the ICP EM and Sensor can be ran on any hardware that meets the specs.

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.

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	Deploy Tenable Core in VMware
	Microsoft Hyper-V	`.zip` file	
Hardware Tenable-provided hardware		`.iso` image	Install Tenable Core on Hardware

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

OT Security Hardware Requirements

For more information about hardware requirements specifically for OT Security or OT Security Sensor, see Tenable OT Security Hardware Specifications in the *General Requirements Guide*.

OT Security Virtual Hardware 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.

The following chart outlines basic guidelines for operating Tenable Core + OT Security in a virtual environment.

Tenable Core + OT Security requires CPUs with AVX and AVX2 (for example, Intel Haswell or newer).

Installation Scenario	CPU Cores	Memory	Disk Space
Virtual Machine	8 cores	16 GB RAM	205 GB

OT Security Virtual Sensor Requirements

Installation Scenario	CPU	Memory	Disk Space
Sensor	2 virtual CPUs	4 GB RAM	60 GB HDD

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.

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 are heavily based 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

Maximum SPAN/TAP	CPU	Memory	Storage	Network

Throughput (Mbps)	Cores[1]	(DDR4)	Requirements	Interfaces
50 Mbps or less	4	16 GB RAM	Minimum 205 GB	Minimum two network interfaces
50-150 Mbps	16	32 GB RAM	Minimum 205 GB	Minimum two network interfaces
150-300 Mbps	32	64 GB RAM	Minimum 205 GB	Minimum two network interfaces
300 Mbps to 1 GB	32-64	128 GB RAM or more	Minimum 205 GB	Minimum two network interfaces

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 install 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 moved from a few seconds to less than a second.

Network Interface Requirements

You must have two (or more) 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 are installing the ISO (such as Hyper-V).

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

- OT Security requires only one NIC for EM.
- OT Security requires a minimum of two NICs for the ICP and Sensors.
- OT Security requires static IP addresses to be used for ICP/EM/Sensors.
- Both the sensor and ICP can be configured to monitor multiple SPAN interfaces.

Note: Starting from OT Security 4.1, the profile names for network interfaces are as follows:

- nic0 – System port 1
- nic1 – System port 2

- nic2 – System port 3
- nic3 – System port 4

nic0 or System port 1 (192.168.1.5) and nic3 or System port 4 (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 or System port 4 (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 + OT Security nic1 or System port 2 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*.

---

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

Access Requirements

Your Tenable Core + OT Security Sensor 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 need to be able to 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	You do not need internet access to deploy or update Tenable Core.
	Microsoft Hyper-V	`.zip` file	
Cloud	Amazon Web Services (AWS)	n/a	Requires internet access to deploy or update Tenable Core.
Cloud	Microsoft Azure	n/a	
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 Tenable Core + Tenable OT Security Sensor 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. OT Security also requires application-specific port access. For more information, see Firewall Considerations.

Inbound Traffic

Allow inbound traffic to the following ports listed.

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	(Default) Inbound HTTPS communications to the Tenable Core interface.
TCP 8090	Inbound HTTPS communications for restoring backups. Inbound communications with the file upload server.

Outbound Traffic

Allow outbound traffic to the following ports listed.

Port	Traffic
TCP 22	Outbound SSH connections, including remote storage connections.
TCP 443	Outbound communications to the `appliance.cloud.tenable.com` and `sensor.cloud.tenable.com` 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) requires a few network connections, referred to as Interface Roles.

Management and Active Query Interface

This is an interface configured with an IP address that allows network reachability to manage and configure the appliance. This interface allows the appliance to reach assets on the network for active querying (recommended, but optional).

Management and Active Query Roles Separation (Split-Port)

You can split the Management and Active Query roles between two separate interfaces. This enables, for instance, a connection to an IT network for management purposes and a separate connection to an OT network to access the OT assets using Active Query.

For this purpose, prepare and connect two separate interfaces each dedicated to one of the roles.

Basic management connectivity to the ICP through the Active Query interface is allowed and operational as long as the ICP system allows network connectivity.

To finalize the OT Security setup, you require management connectivity. You can configure Split-Port and Active Query connectivity later.

On Tenable-provided hardware appliances, OT Security is automatically installed, with the default interface roles (combined management and Active Query roles).

> Note: When configuring the IP address for both interfaces, Tenable recommends to only configure a Default-Gateway for the interface dedicated to the Management role. You can specify a dedicated gateway for Active Query when configuring Split Port.

Monitoring Interfaces

One or more network interfaces can be used for passive network monitoring. Passive monitoring (SPAN) interfaces:

- Monitor and collect traffic for analysis
- Must be connected to a Mirroring, Switch Port Analyzer (SPAN), or Remote Switch Port Analyzer (RSPAN) destination interface of a switch.

Note: Traffic that cannot be directly monitored by the appliance interfaces can be collected using OT Sensors or Encapsulated Remote SPAN (ERSPAN) configuration.

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.

Note: For the EM centralized updates to work, the ICP must be able to reach ports 28305 and 8000 (TCP).

Flow Direction	Port	Communicates With	Purpose
Inbound	TCP 443	Web interface for OT Security Appliance	Browser access to OT Security
Inbound	TCP 8000	Web interface for Tenable Core	Browser access to Tenable Core
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

Flow Direction	Port	Communicates With	Purpose
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	IoT Connector	Connects ICP to IoT connector

Flow Direction	Port	Communicates With	Purpose
	(secure port)		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	Unauthenticated / passive

Flow Direction	Port	Communicates With	Purpose
		Sends communication from sensor, receives on ICP/ OT Security	only sensor connection
Outbound	TCP 28304 (SSH) TCP 443 (HTTPS)	ICP/ OT Security SSH connections for sensor pairing. Sends communication from sensor, receives on ICP/ OT Security	Authenticated / secure tunnel between sensor and ICP

*Optional services

Active Query

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

> Note: OT Security supports queries across these protocols, but not all of them may apply to your environment. For optimal results, ensure that you open as many of the listed ports as possible between OT Security (or the OT Security sensors) and the nearby remote devices. This action enables accurate identification and querying.

Protocol	Port	Communicates With	Purpose
ICMP		Generic / Various	Network-level asset discovery / ping
TCP	21	Generic / Various	FTP file transfer
TCP / UDP	53	DNS Servers	Domain Name System (DNS)

Protocol	Port	Communicates With	Purpose
			resolution queries
TCP	80	Generic / Various	HTTP fingerprinting and web interface access
TCP	102	Siemens Devices	Manufacturing Message Specification (MMS), overlaps IEC 61850
TCP	102	Siemens Devices	IEC 61850 / MMS for substation and SCADA devices
TCP	102	Siemens Devices	S7/S7+ / MMS communication for automation devices
UDP	111	Emerson Ovation Devices	RPC service registration / discovery for Ovation
TCP	135	Windows Devices	WMI queries for system and network management
UDP	137	Generic / Various	NetBIOS Name Service (NBNS) for Windows network discovery
UDP	138	Generic / Various	NetBIOS Datagram Service (NBT) for Windows file / printer sharing
UDP	161	Generic / Various	SNMP polling and trap communication
TCP	443	Generic / Various	HTTPS fingerprinting and secure web services

Protocol	Port	Communicates With	Purpose
TCP	445	Windows Devices	WMI / SMB queries for system management (replaces 135 for some cases)
TCP	502	OT Devices	Modbus TCP communication with PLCs and meters
UDP	1069	Cognex Cameras	Cognex Vision system discovery protocol
TCP	1911	BMS Controllers	Niagara FOX unencrypted protocol
TCP	1962	Phoenix Contact Devices	PC Worx engineering and control communication
TCP / UDP	2001	Profinet Devices	Profinet device communication for controllers and I/O modules
TCP	2001	Siemens Devices	SICAM / PROFINET (legacy and substation devices)
TCP	2222	Rockwell Devices	PCCC protocol for ControlLogix/PLC communications
TCP	2404	SCADA Devices	IEC 60870-5-104 for RTU and substation communications
TCP	3389	Windows Devices	RDP (Remote Desktop Protocol)
TCP	3500	Bachmann M1 Devices	Bachmann M1 controller communication

Protocol	Port	Communicates With	Purpose
TCP	4000	Emerson Devices	Emerson ROC 4000 controller data/control
TCP	4444	Schneider Electric	SmartX controllers (EcoStruxure Building Operation)
UDP	4800	Moxa Devices	Moxa Device Discovery protocol
TCP	4911	BMS Controllers	Niagara FOX secure (TLS/SSL) protocol
TCP	5001	Bosch Devices	Bosch PSI (Programmable System Interface)
TCP	5002	Mitsubishi Devices	MELSEC PLC MC Protocol over TCP
TCP	5007	Mitsubishi Devices	MELSEC PLC additional communication port
UDP	5009	Mitsubishi Devices	MELSEC Finder broadcast (device discovery)
TCP	5033	Siemens Devices	P2 protocol (used in legacy Siemens automation systems)
TCP	5050	Saia-Burgess Devices	Saia PCD controller communication
TCP	5094	HART-IP	HART-IP over TCP for smart instrumentation

Protocol	Port	Communicates With	Purpose
TCP	5313	Yokogawa DCS	CENTUM DCS engineering interface
TCP	5432	SEL (Schweitzer) Devices	PostgreSQL database access for energy devices
TCP	6626	WAGO Devices	WAGO I/O communication and programming
TCP	7700	Schneider Electric	ION power meters and energy management systems
TCP	8000, 8008, 8080, 8443, 8800	Generic / Various	Common HTTP/HTTPS alternative ports
TCP	9940	Yokogawa DCS	CENTUM status and diagnostics
UDP	12321	Honeywell Devices	Honeywell FTE UDP discovery / redundancy
TCP	18245	Schneider Devices	SRTP (Schneider Real-Time Protocol) for M340/M580 PLCs
TCP	18507	Emerson Devices	Emerson ROC / Flow Computer (FACE protocol)
TCP	18508	Emerson Devices	Emerson firmware upgrade service (UPGD)
TCP	20256	GE Devices	PCOM protocol for Proficy iFIX / CIMPLICITY SCADA

Protocol	Port	Communicates With	Purpose
TCP	20547	Procon	PROCON OS remote management interface
TCP	24576	ABB Devices	ABB Network Control (ABB_NC) protocol for substation automation
TCP	34964	Siemens Devices	PROFINET Connection Management (PROFINET CM)
TCP	39329	Emerson Devices	Ovation / VME-based control systems
TCP/ UDP	44818	OT Devices	CIP (Common Industrial Protocol) for Rockwell devices
UDP	47808	BMS Controllers	BACnet/IP communication for building automation devices
TCP/ UDP	48898	Beckhoff Devices	ADS/TwinCAT protocol for controller and engineering communications
UDP	48899	Beckhoff Devices	ADS/AMS Discovery (TwinCAT/Beckhoff IPCs)
TCP	50000	Siemens Devices	SIPROTEC 4 relay communication
TCP	51966	Honeywell Devices	Honeywell FTE (Fault Tolerant Ethernet) communications
TCP	55553	Honeywell Devices	CEE (Control Execution Environment) communications in Experion PKS

Protocol	Port	Communicates With	Purpose
TCP	55565	Honeywell Devices	FTE (Fault Tolerant Ethernet) communications for redundancy in Experion PKS

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

OT Agent

Flow Direction	Port	Communicates With	Purpose
Outbound	443	OT Security	First-time pairing with an OT Agent.
Outbound	28306	OT Security	Connection with the OT Agent.

IoT Connector Agent

Flow Direction	Port	Communicates With	Purpose
Outbound	TCP 10146 (secure port)	IoT Connector	Connects ICP to IoT connector agent
Outbound	TCP 10104 (unsecure port)	IoT Connector	Connects ICP to IoT connector agent

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.

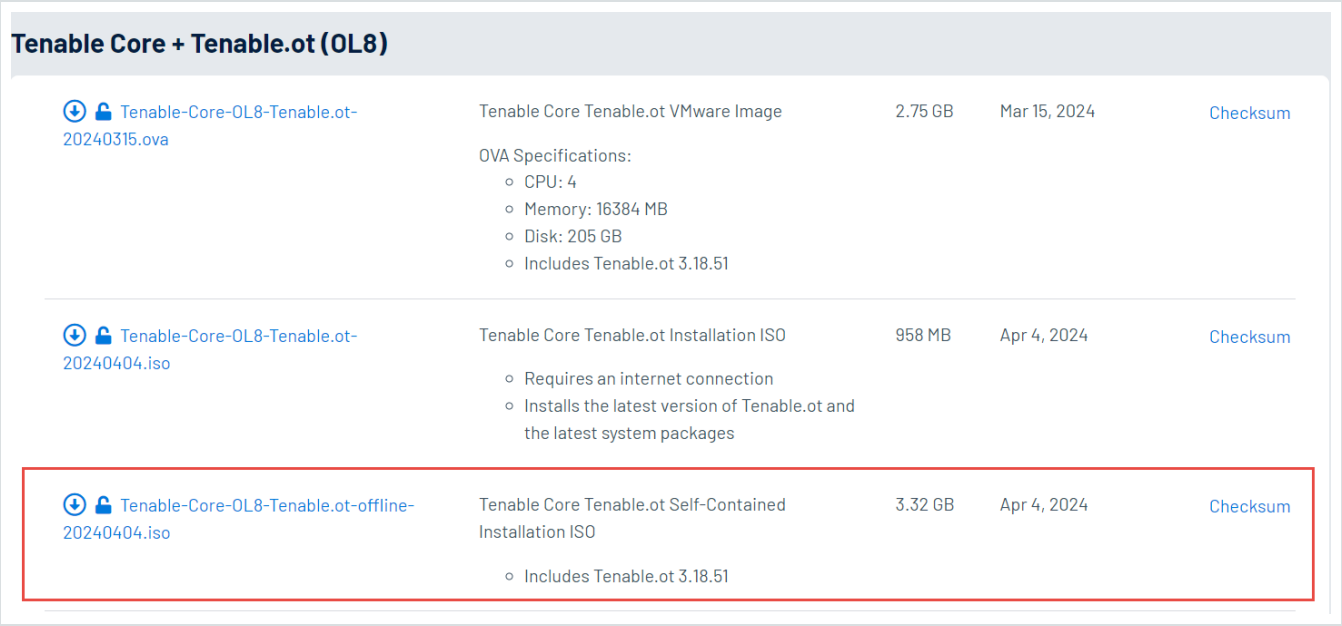
Before you Begin

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:

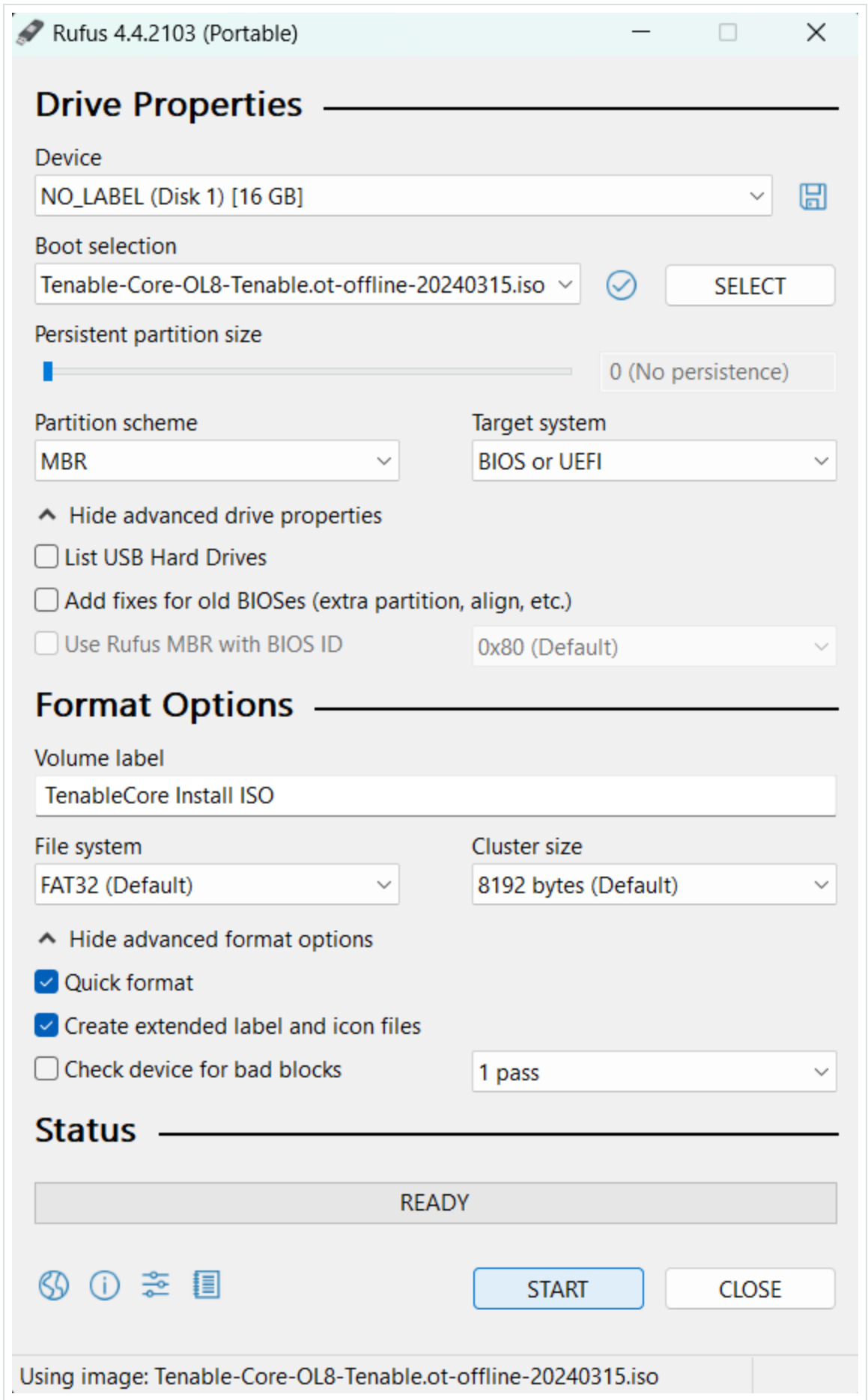
1. Download the latest Offline ISO file from Tenable Downloads.

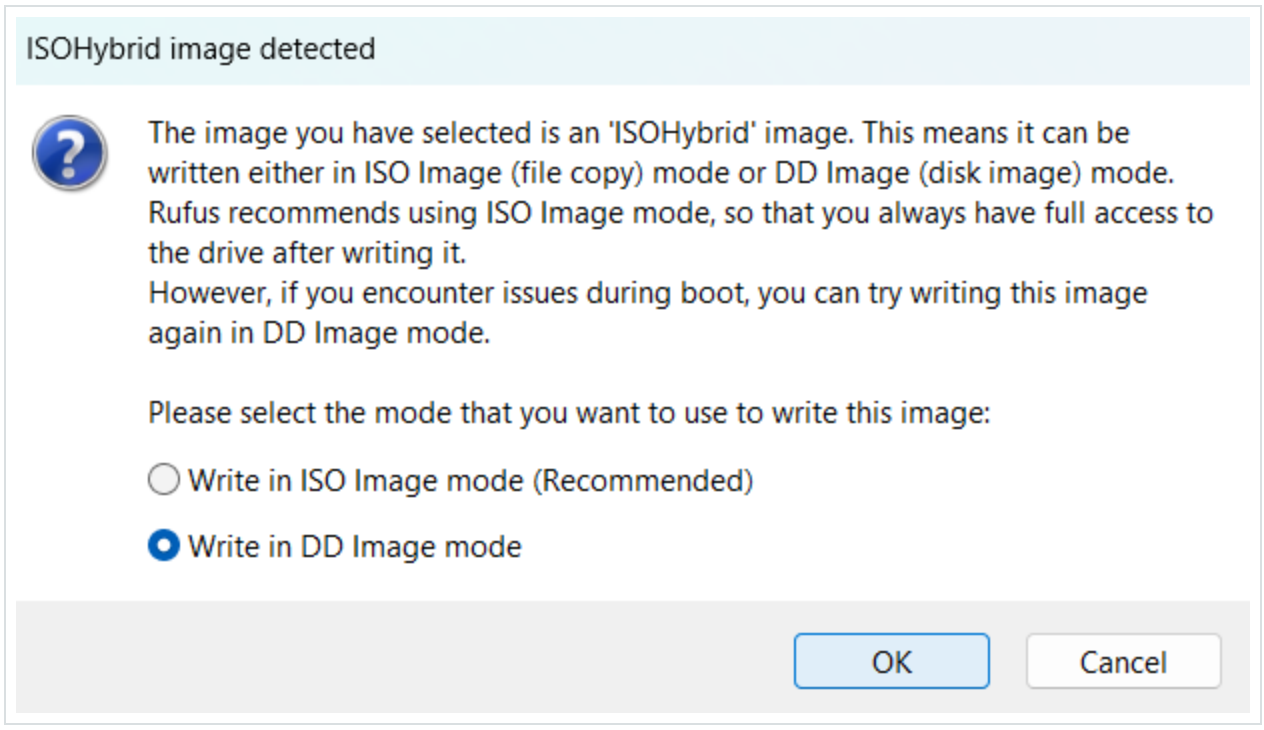


Tenable Core + Tenable.ot (OL8)

Tenable-Core-OL8-Tenable.ot-20240315.ova	Tenable Core Tenable.ot VMware Image OVA Specifications: ○ CPU: 4 ○ Memory: 16384 MB ○ Disk: 205 GB ○ Includes Tenable.ot 3.18.51	2.75 GB	Mar 15, 2024	Checksum
Tenable-Core-OL8-Tenable.ot-20240404.iso	Tenable Core Tenable.ot Installation ISO ○ Requires an internet connection ○ Installs the latest version of Tenable.ot and the latest system packages	958 MB	Apr 4, 2024	Checksum
Tenable-Core-OL8-Tenable.ot-offline-20240404.iso	Tenable Core Tenable.ot Self-Contained Installation ISO ○ Includes Tenable.ot 3.18.51	3.32 GB	Apr 4, 2024	Checksum

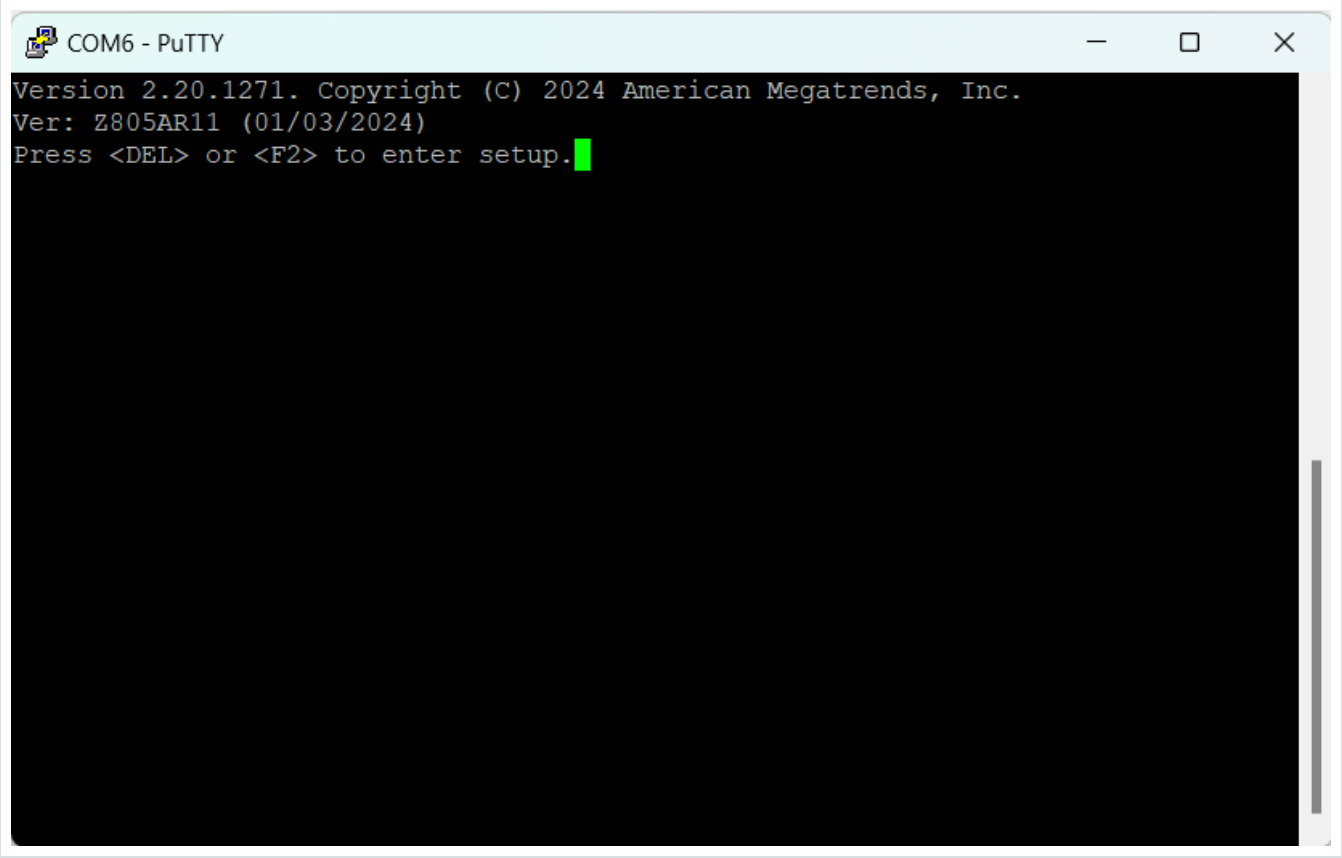
2. Plug the USB drive into a PC and flash the ISO onto the flash drive in DD mode.


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



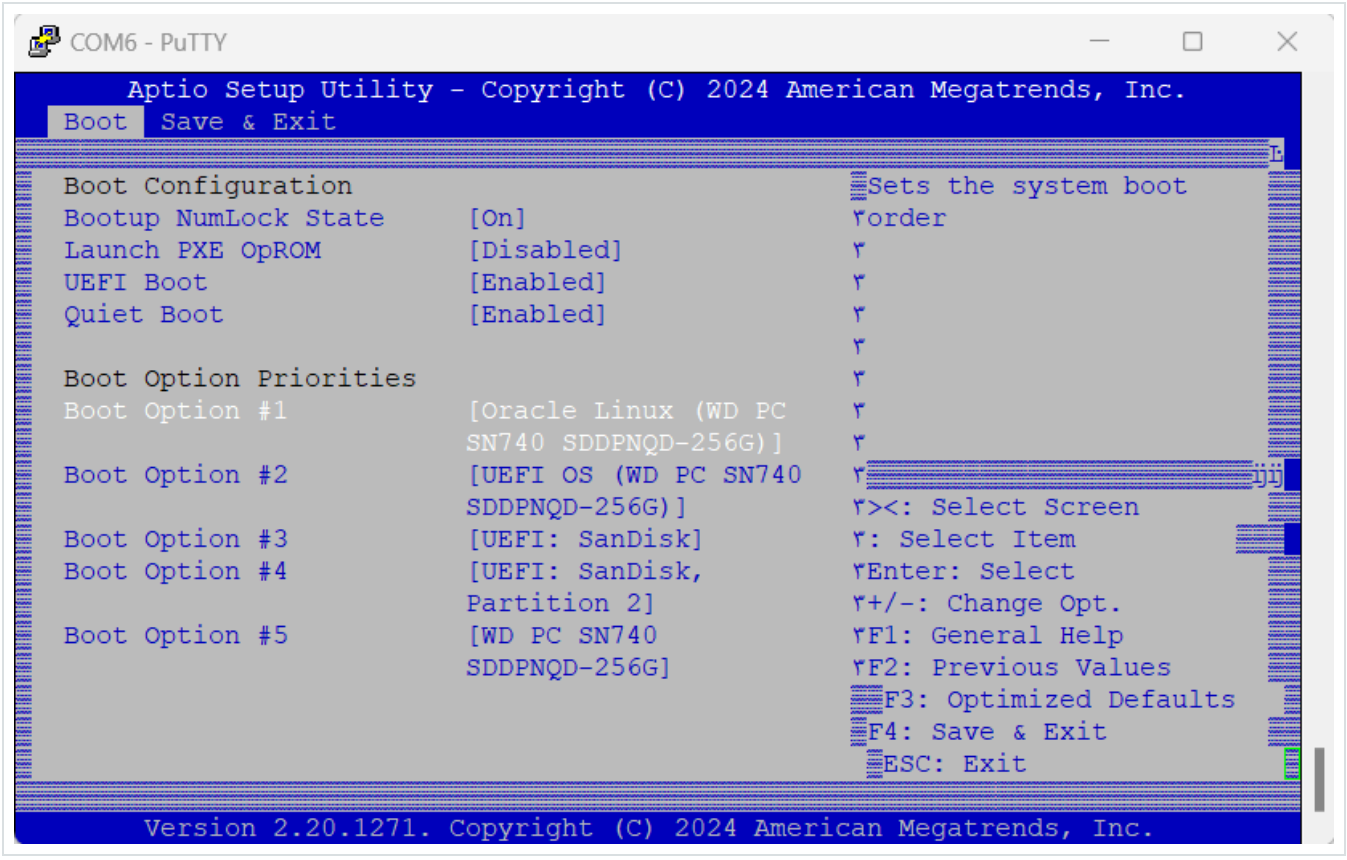
3. When finished, plug the USB drive into a USB port on the OT Security appliance.

4. Connect to the appliance via the Console Serial interface (Baud rate of 115200 bps with an 8N1 configuration), and power it on.



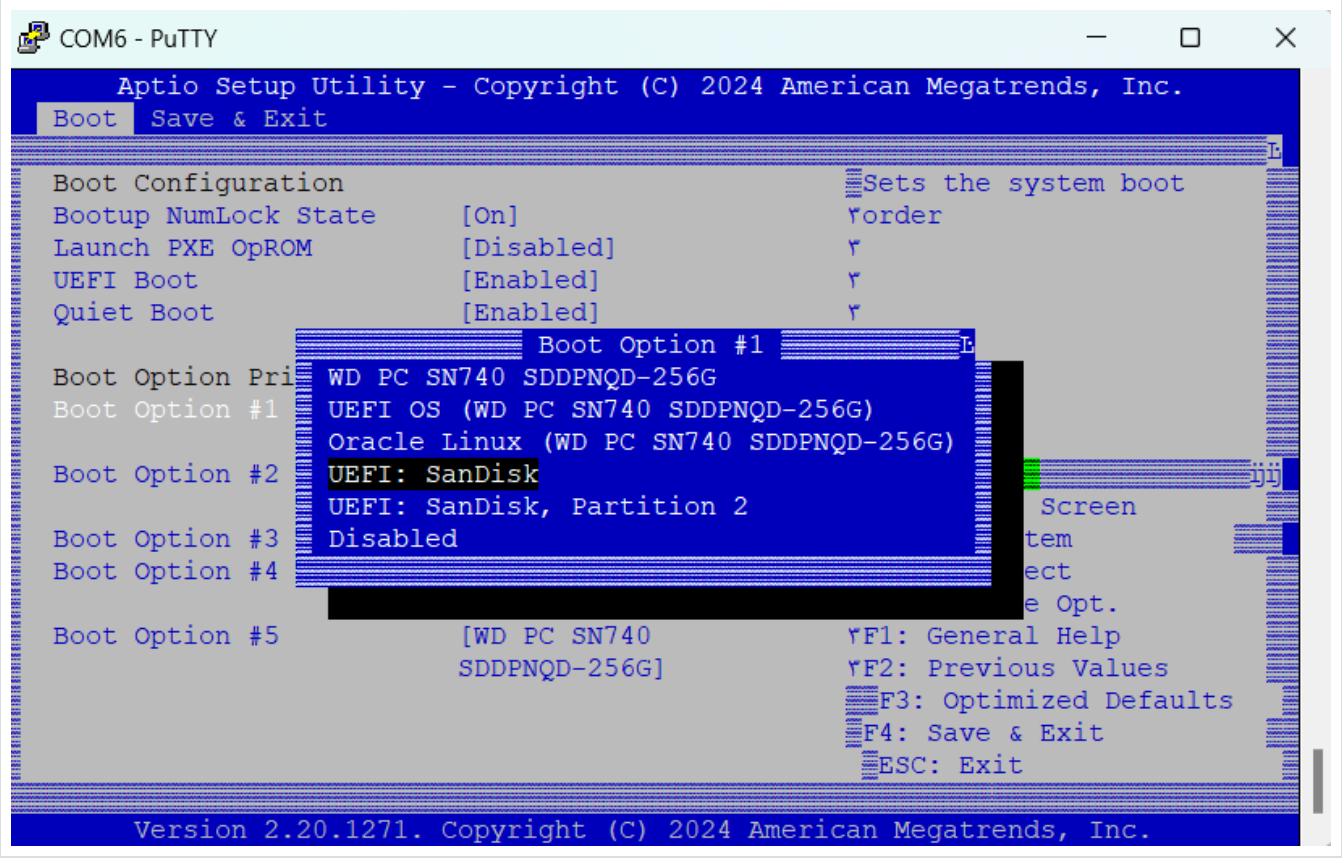
5. When prompted, press <DEL> to enter the setup.

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.

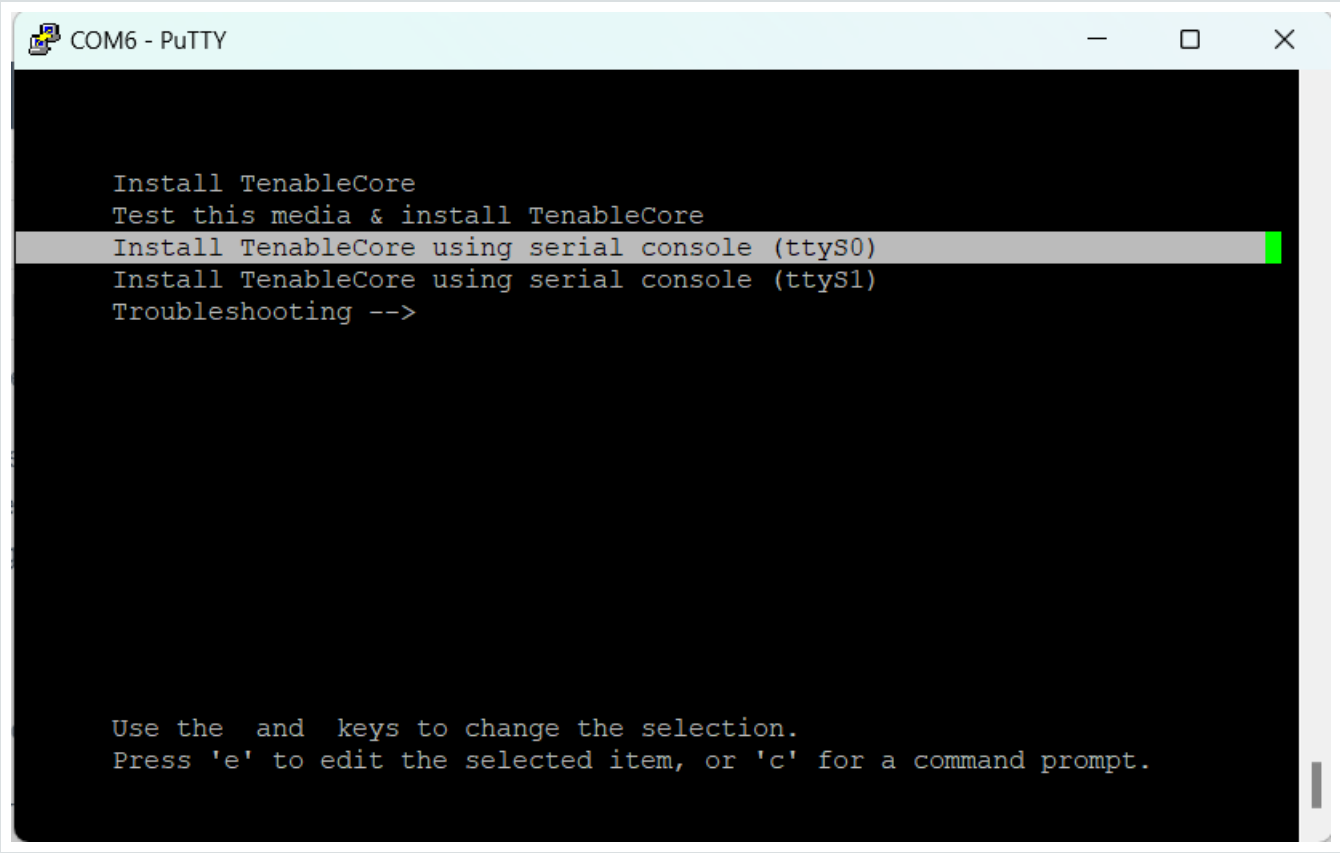


> Note: You can use “One-shot boot” on appliances that support the feature.

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 and HDMI), 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 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` from your computer to your virtual machine.
   For information about configuring your virtual machines, 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.

> Tip: 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. Make sure that you prepare your network infrastructure accordingly. For more information, see Network Considerations.

Management and Active Query

Connect the selected network interface to a network switch interface configured to allow management connectivity to the ICP as required.

Make sure to configure an IP address and other connectivity settings on the selected OT Security appliance interface via Tenable Core.

If you want to separate the Management and the Active Query roles, make sure each selected interface is connected to its dedicated switch interface. Assign IP addresses for each and configure the switch interfaces as needed to allow network reachability for both functionalities.

For more information, see Management and Active Query Roles Separation (Split-Port).

Network Monitoring

Connect one or more of the appliance interfaces selected for passive network monitoring to a configured port-mirroring destination (SPAN/RSPAN) interface on a network switch. You must configure port-mirroring to allow proper visibility of the OT network protocols and communications.

> Note: You can use OT Sensors or Encapsulated Remote SPAN (ERSPAN) to capture traffic that cannot be directly monitored by the appliance interfaces.

To connect the OT Security appliance to the network:

On a hardware appliance:

Tenable-provided hardware appliances may come with various quantities and types (RJ45 or SFP) of network interfaces. OT Security comes pre-installed with the default interfaces selected for each role. You may change this configuration at a later stage as required.

On non-Tenable-provided hardware, you must select interfaces for each role before manually initiating the OT Security installation process. Make sure to correctly utilize the available interfaces for each role.

On a virtual appliance:

If you deployed the appliance using the `.ova` file, the appliance comes pre-configured with four network interfaces. You can add additional network adapters/interfaces during the deployment or at a later stage.

If you deployed a custom virtual appliance using the `.iso` or `.zip` (Hyper-V) file, configure the required number of network interfaces.

Make sure to configure the virtual machine as per the requirements described in System Requirements. For more information on configuring networking on virtual machines, see the VMware documentation or the Hyper-V 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 Tenable Core User Interface

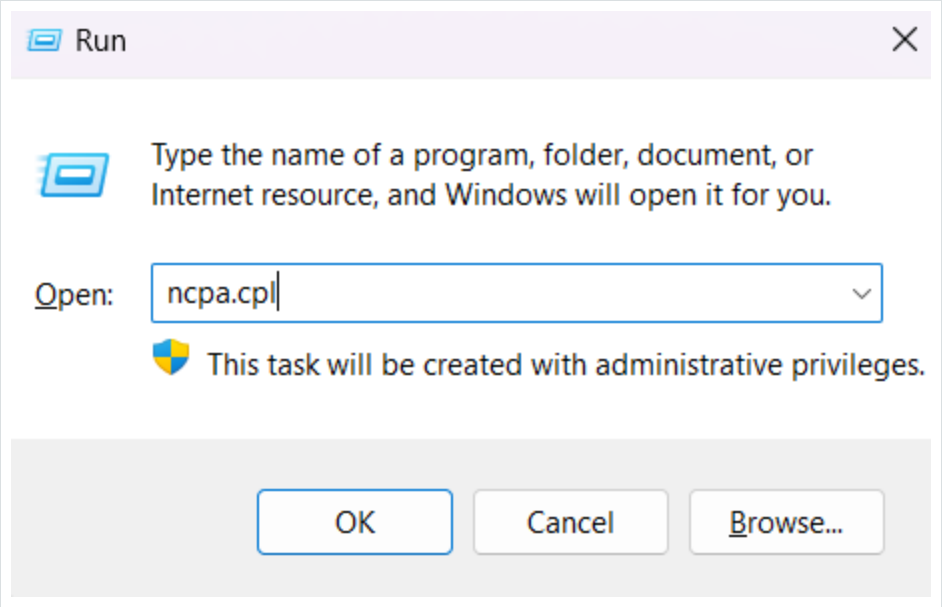
To complete the initial configuration via the Tenable Core user interface (available on https://<mgmt-IP>:8000) you need a working network connection to the appliance.

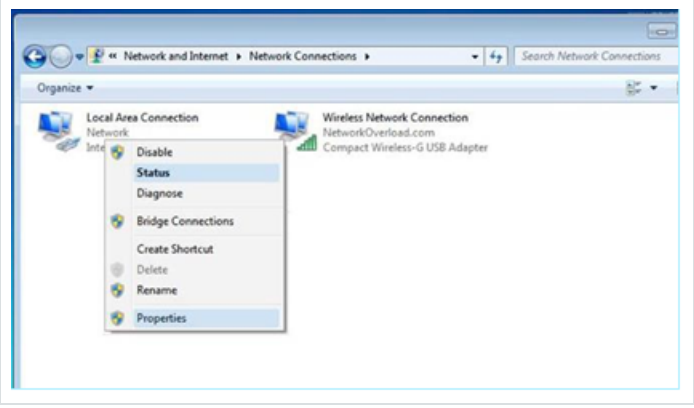
If you have not configured the management IP address, you can use either a directly connected PC or an appropriately configured network to reach the Tenable Core user interface on either of the following:

- System Port 1 – default management interface, pre-configured with IP address 192.168.1.5/24
- System Port 4 – 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.





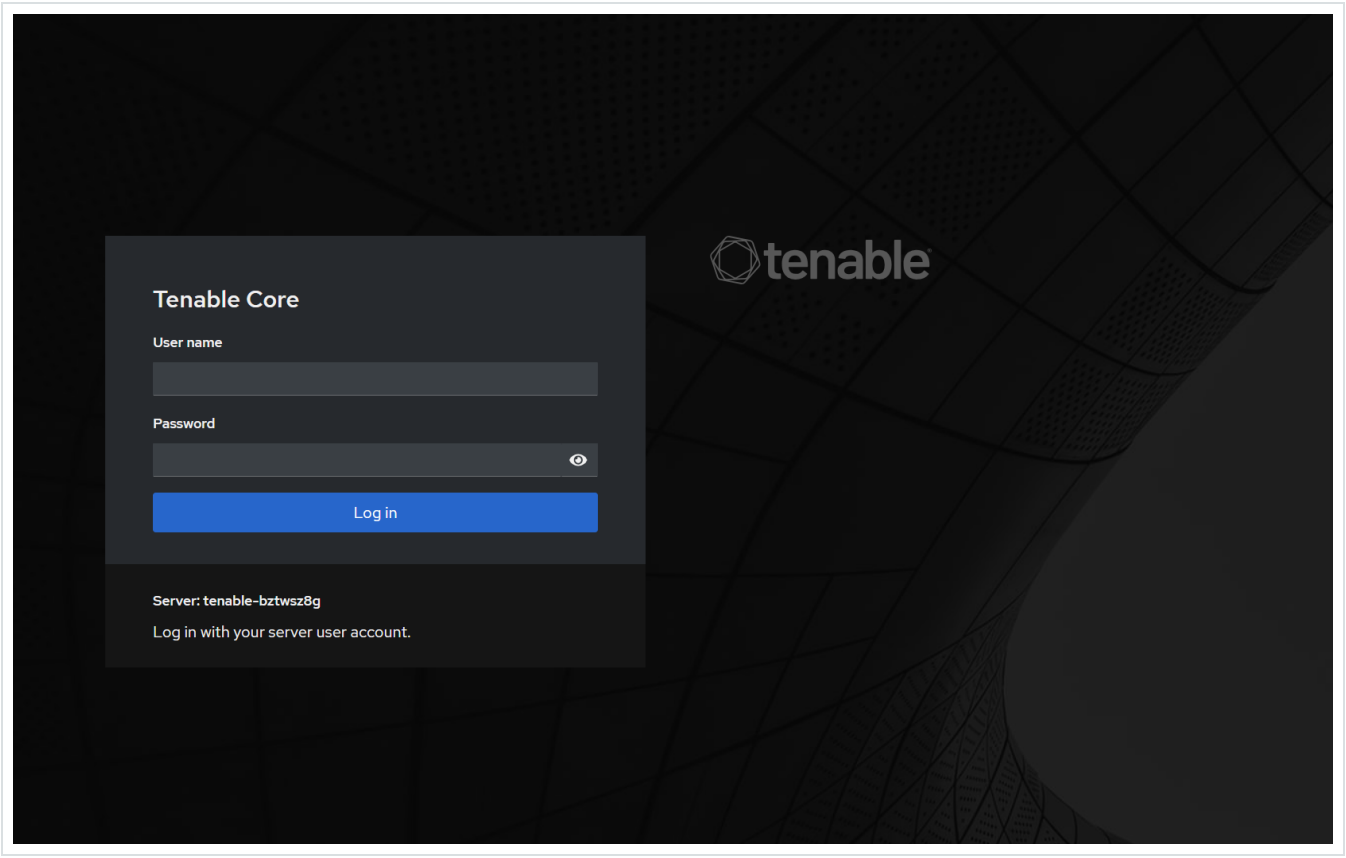
3. Right-click on your network connection (named Local Area Connection) and select Properties.

   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 System port 1 or 192.168.3.10 for the default address of System port 4.
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 an 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: To configure or change the management IP address, log in to Tenable Core and enable administrative access and edit the network configuration.

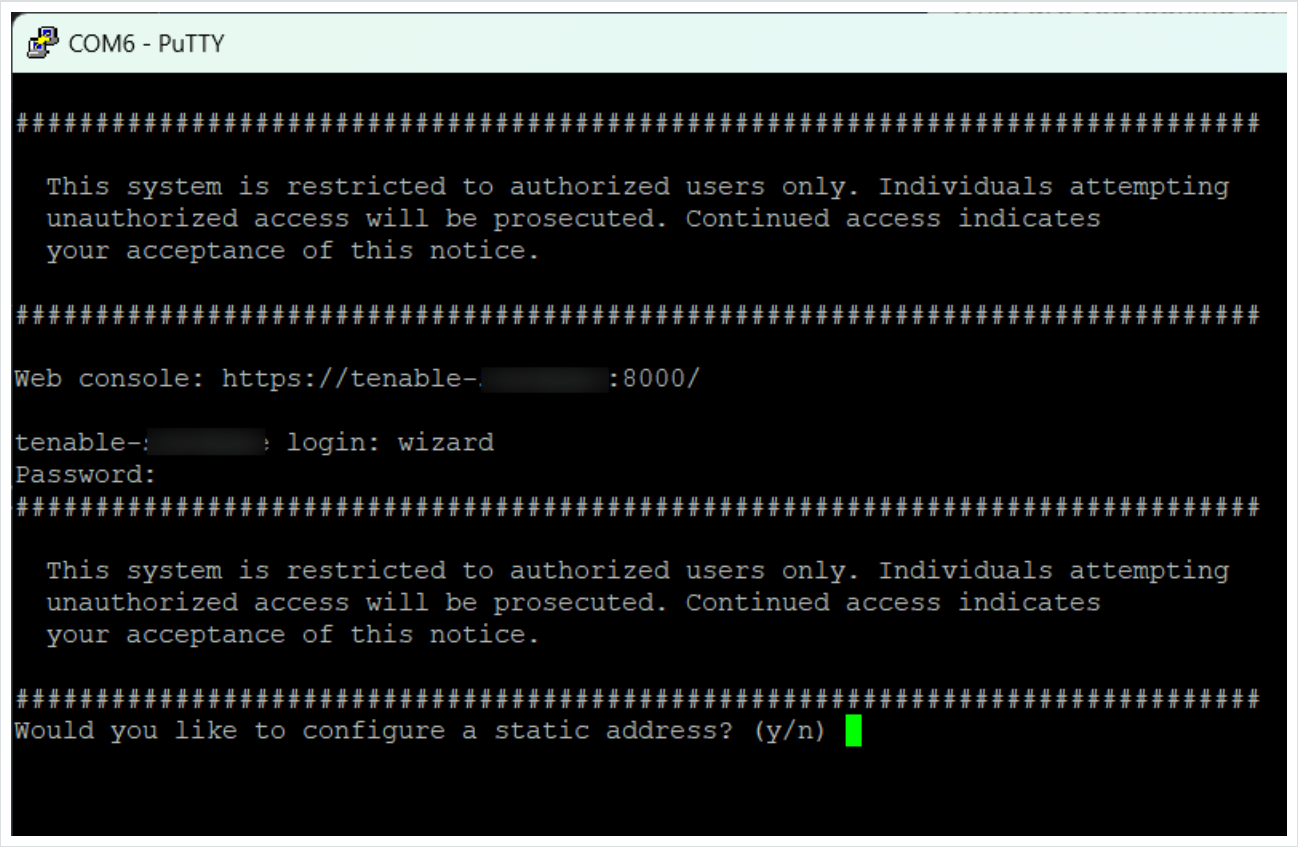
Initial Configuration via CLI (Optional)

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`.

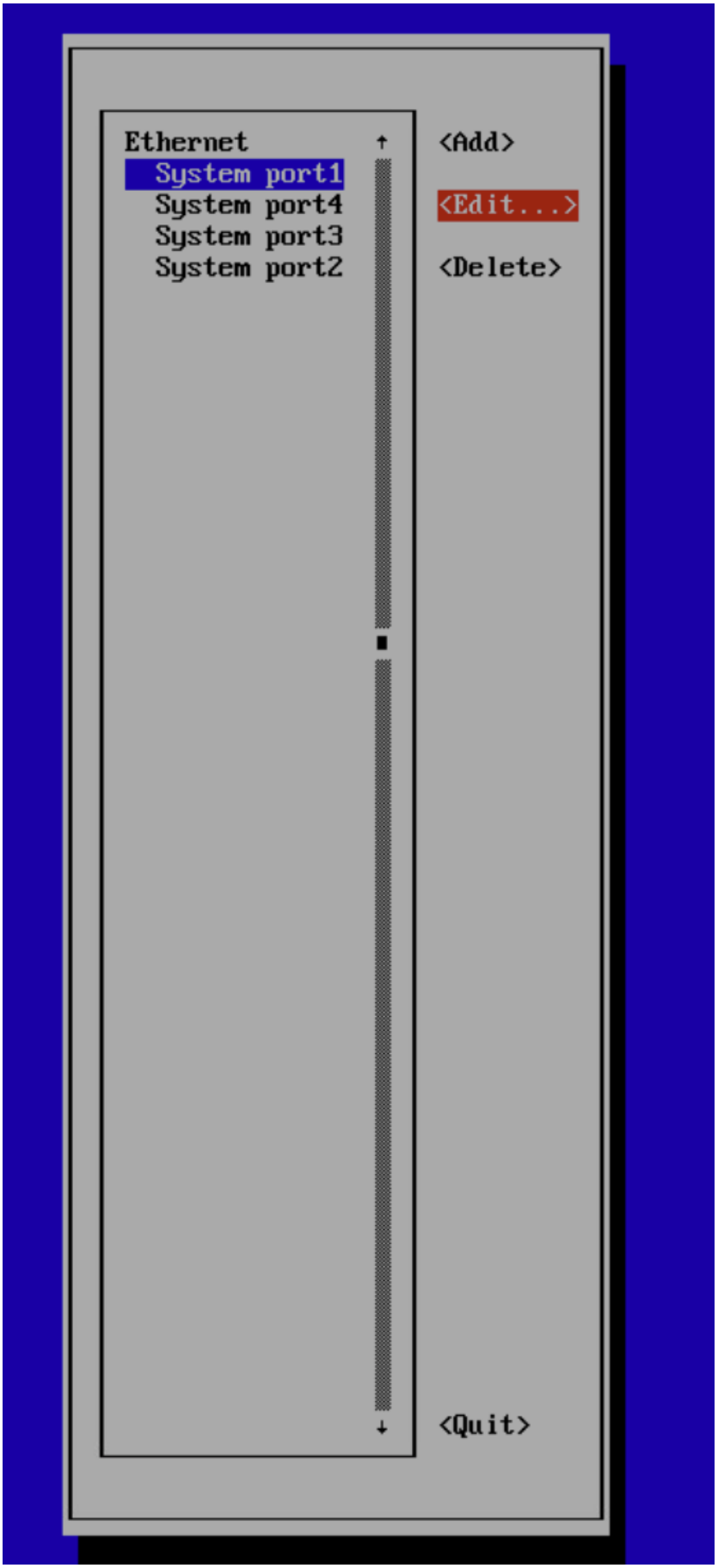
   The Network Manager terminal interface appears.



3. (Optional) To configure the management IP address, type **y**.

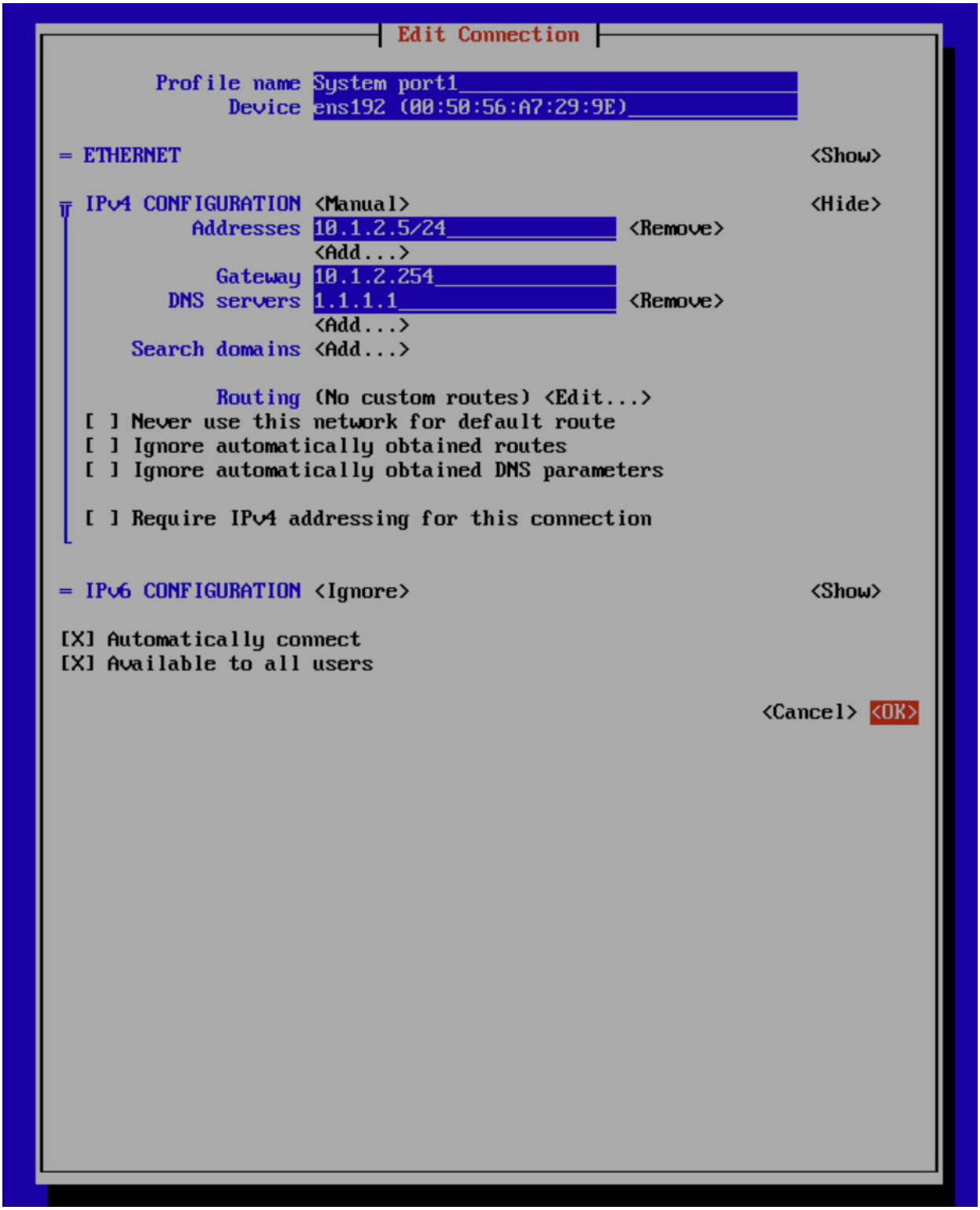
   > Note: If you choose to skip this step, you can always access this option using the `sudo nmtui` command.

a. Select System Port 1 (or System Port 3 if using the split-port configuration).


Ethernet
System port1
System port4
System port3
System port2
<Add>
<Edit...>
<Delete>
<Quit>

b. Press Enter.

The Edit Connection window appears.



c. In the IPV4 Configuration box, change the option from <Automatic> to <Manual>.

Note:

- On virtual machines and non-Tenable provided Hardware, Port 1 is preset to Automatic IPv4 configuration (DHCP).
- On Tenable-provided appliances, Port 1 is preset to 192.168.1.5/24. You can use this port to set up and directly connect the appliance for initial configuration, then change it later via the Tenable Core UI Networking tab or the `sudo nmtui` command from the CLI.

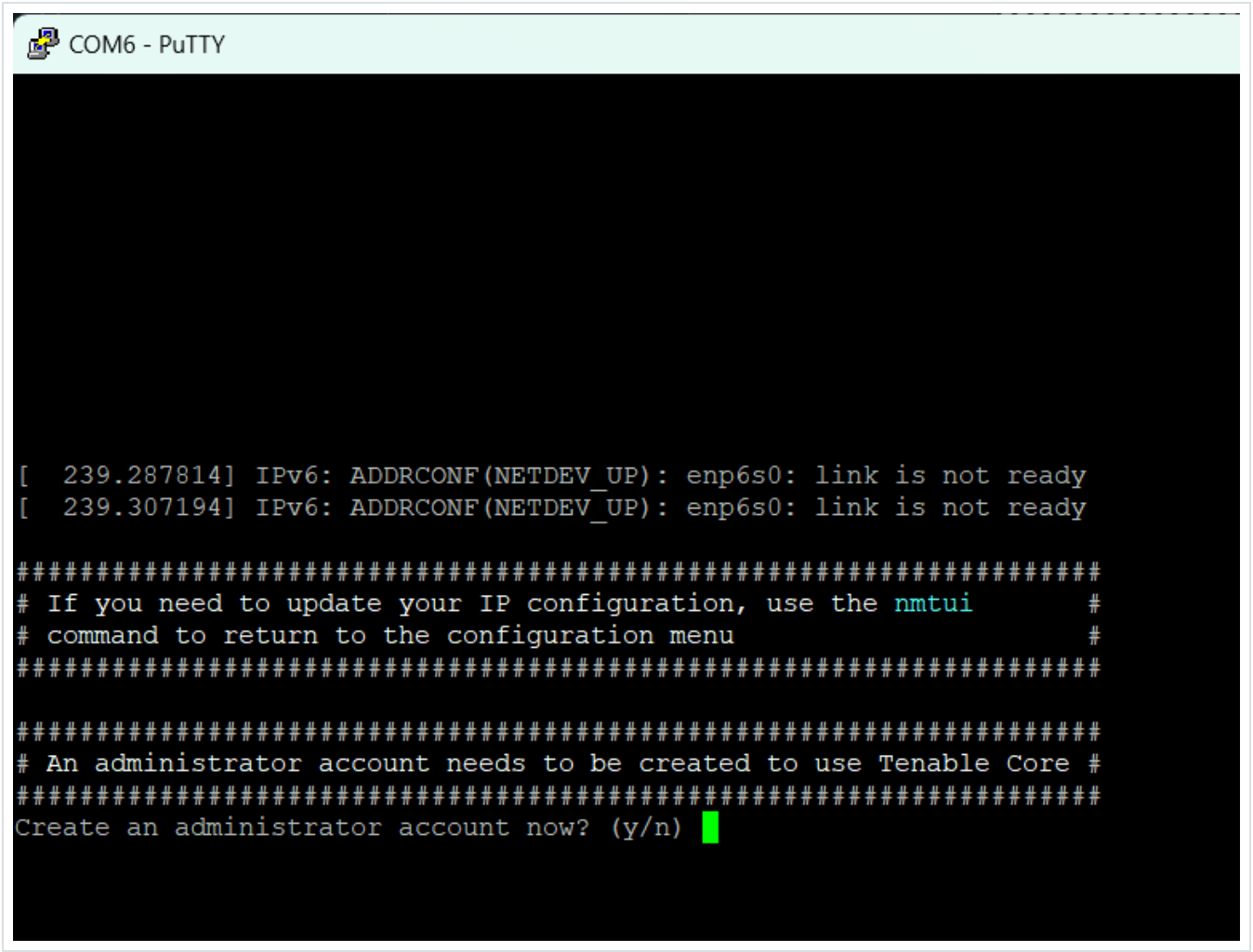
d. Navigate using the arrow keys and configure your required IP address, Default-Gateway, DNS Servers. You can change this configuration later.

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

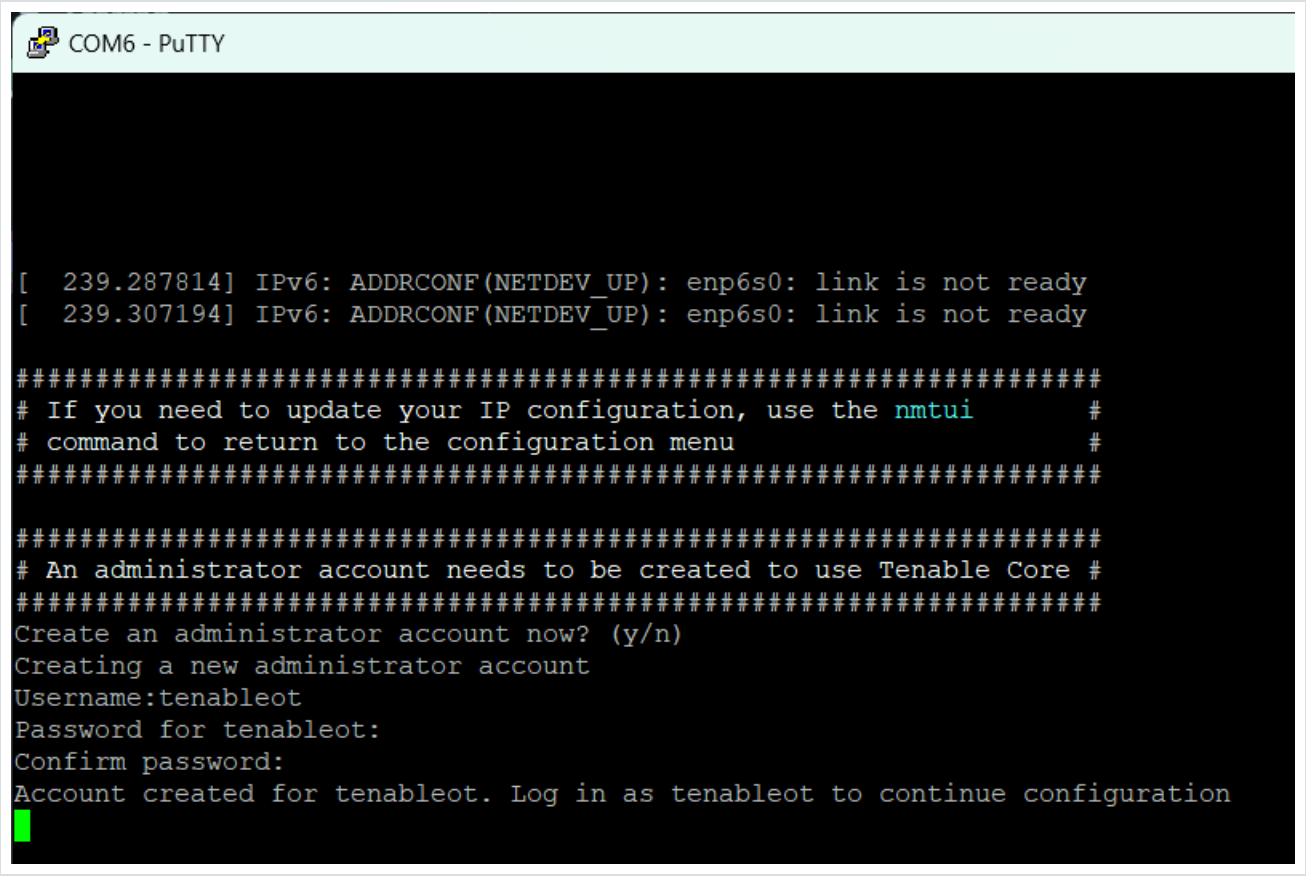
The Network Manager window appears.

4. Select <Quit>.

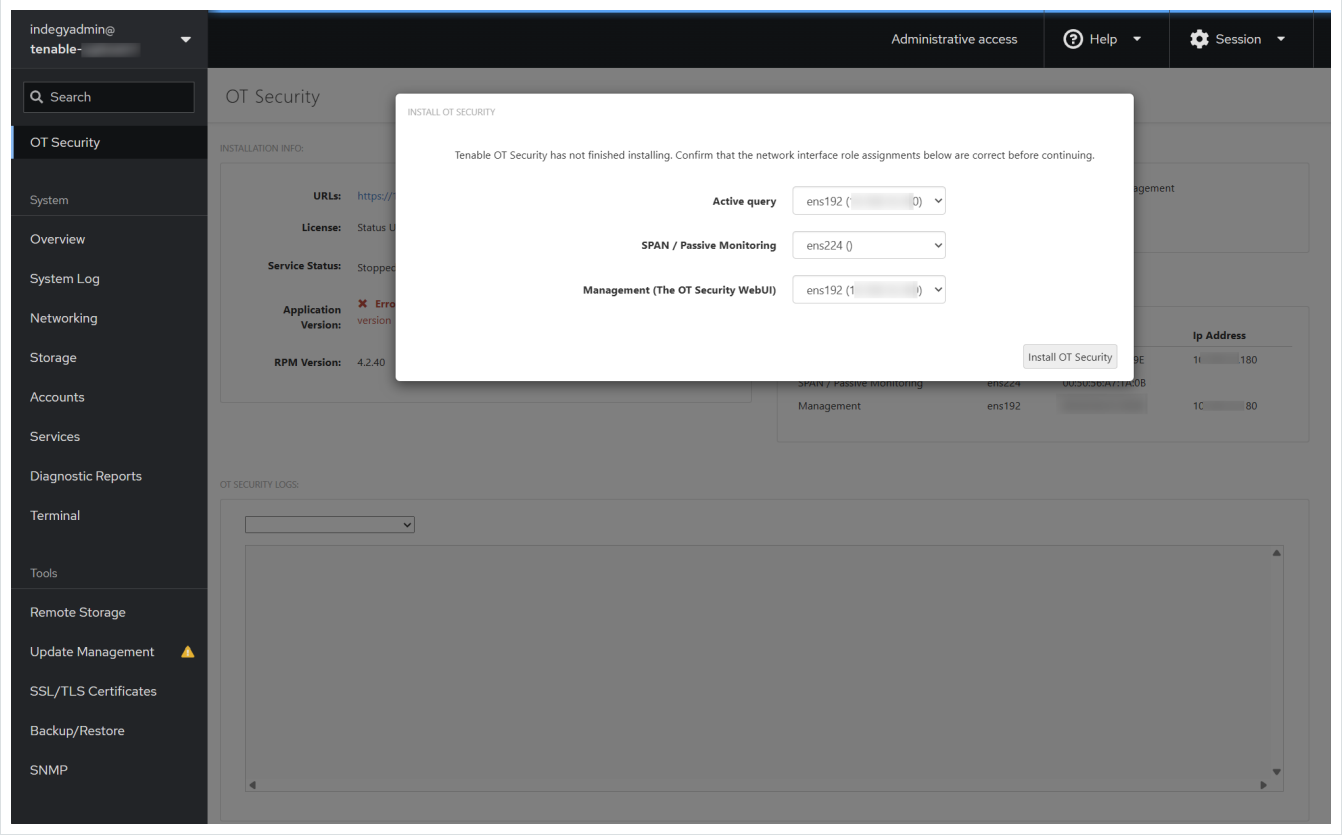
The Network Manager terminal window appears with the prompt to create an administrator account.



5. 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.



6. After you create the account, access the terminal through the console or a network connection (SSH or the Tenable Core interface (https://<mgmt-IP>:8000)) to log in.



On virtual machines and non-Tenable hardware, a prompt appears on the Tenable Core > **OT Security** page to install OT Security.

What to do next

Install OT Security on Tenable Core

Install OT Security on Tenable Core

Tenable-provided hardware appliances come with the OT Security application pre-installed. When deploying OT Security on custom hardware or virtually, it is required to initiate the installation process manually.

> Note:Before initiating the OT Security application installation, assign roles for each interface. Make sure that you configure the interfaces in Tenable Core and prepared the network infrastructure to allow proper connectivity. For more information, see Network Considerations and Connect OT Security to Network.

Before you begin

- Make sure you have Administrative access.
- Make sure that you have SSH or Cockpit access on Tenable Core virtual and physical appliances.

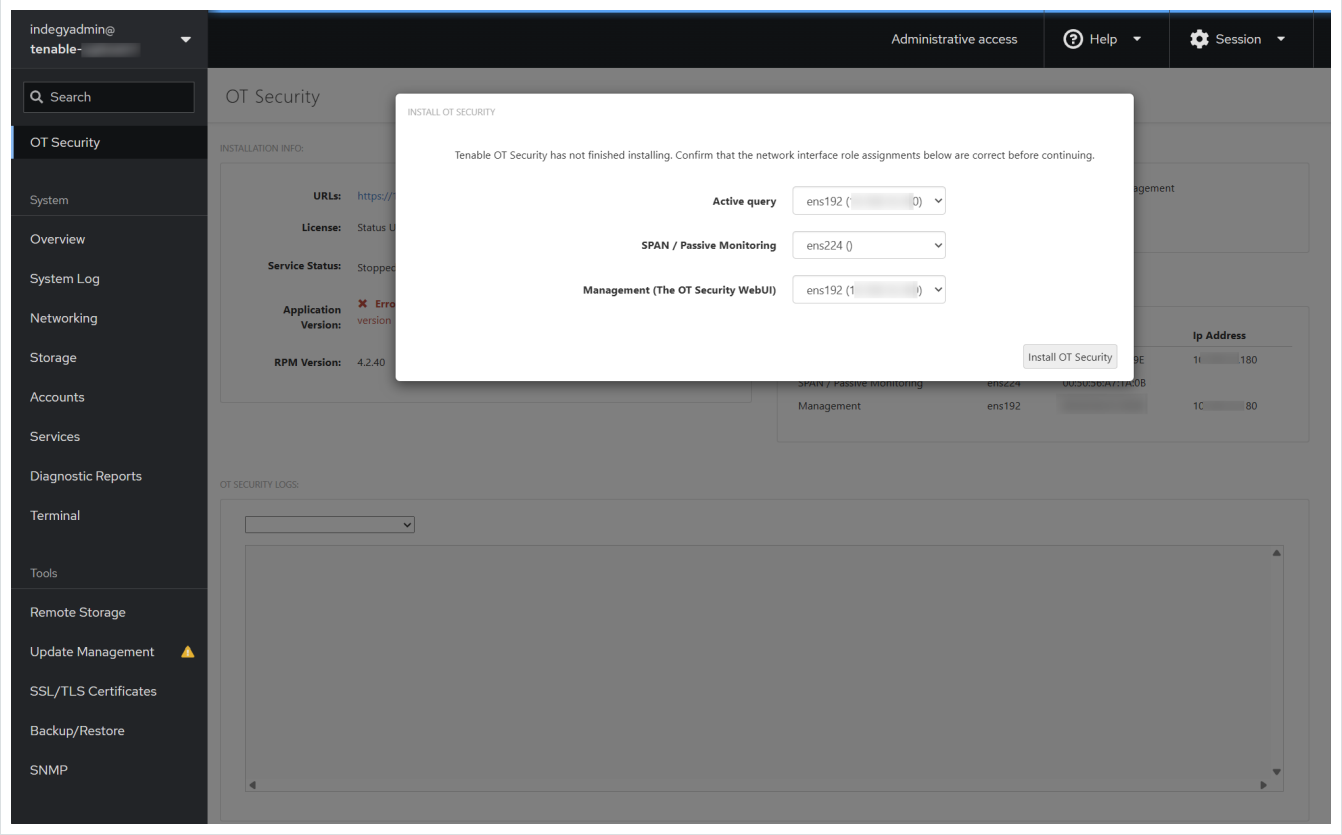
> Note: Administrator accounts can become inaccessible if you do not periodically sign in and update your password. If an administrative account gets locked due to password expiration, you can unlock the account using the remote unlock utility. This utility allows an ICP to remotely unlock its connected sensors and an OT Security Enterprise Manager (EM) to remotely unlock its connected ICPs in the event of an account lockout. For more information about using the utility, see the Knowledge Base article, Leveraging the Remote Unlock Feature in Tenable Core.

To install OT Security in Tenable Core:

1. Log in to Tenable Core from your Chrome browser: `https://<mgmt-ip>:8000`.
2. Navigate to **OT Security**.

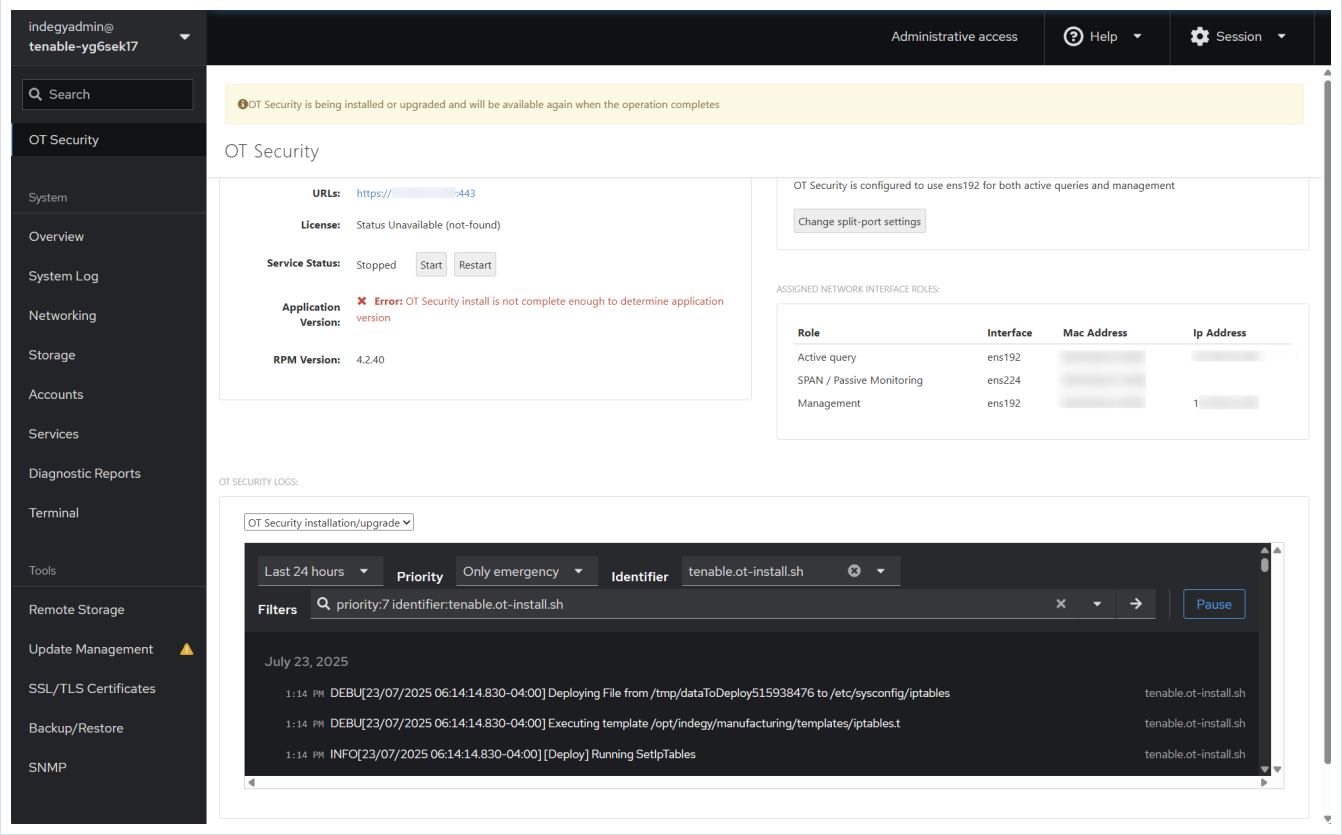
   The OT Security page appears.

> Note: On virtual machines and non-Tenable hardware, you are prompted to install OT Security.

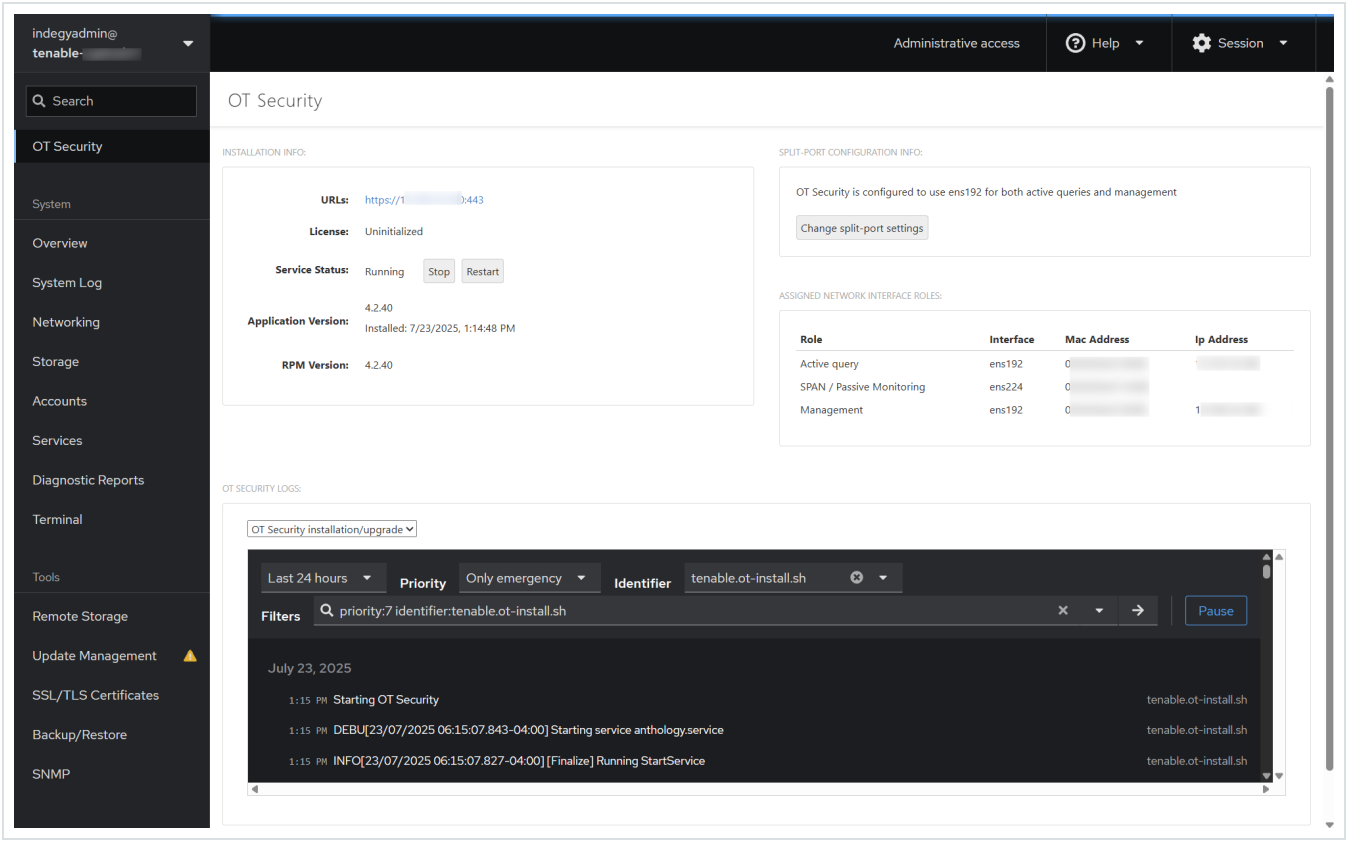


3. Click Install **Tenable OT Security**.

Tenable Core initiates the installation and displays a yellow banner with the message: `OT Security is being installed or upgraded and will be available again when the operation completes.`

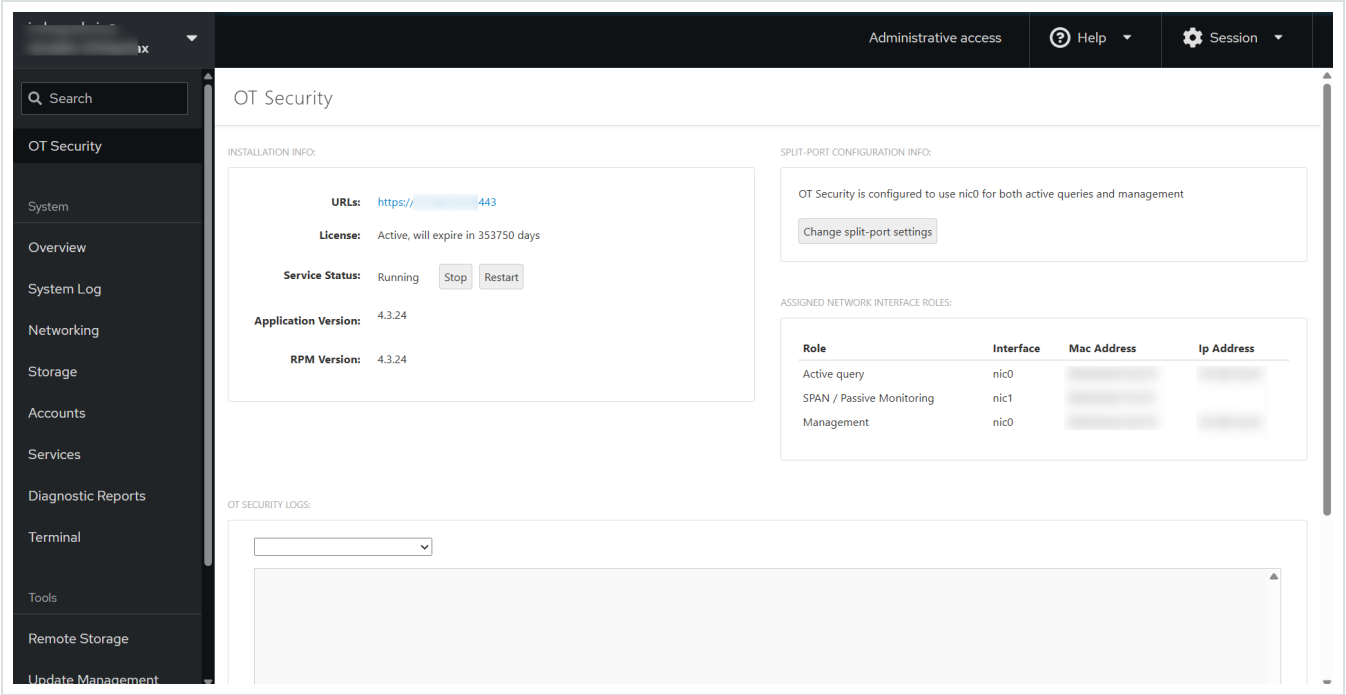


When the installation is complete, the yellow banner disappears and the License status changes from Unavailable to Uninitialized .



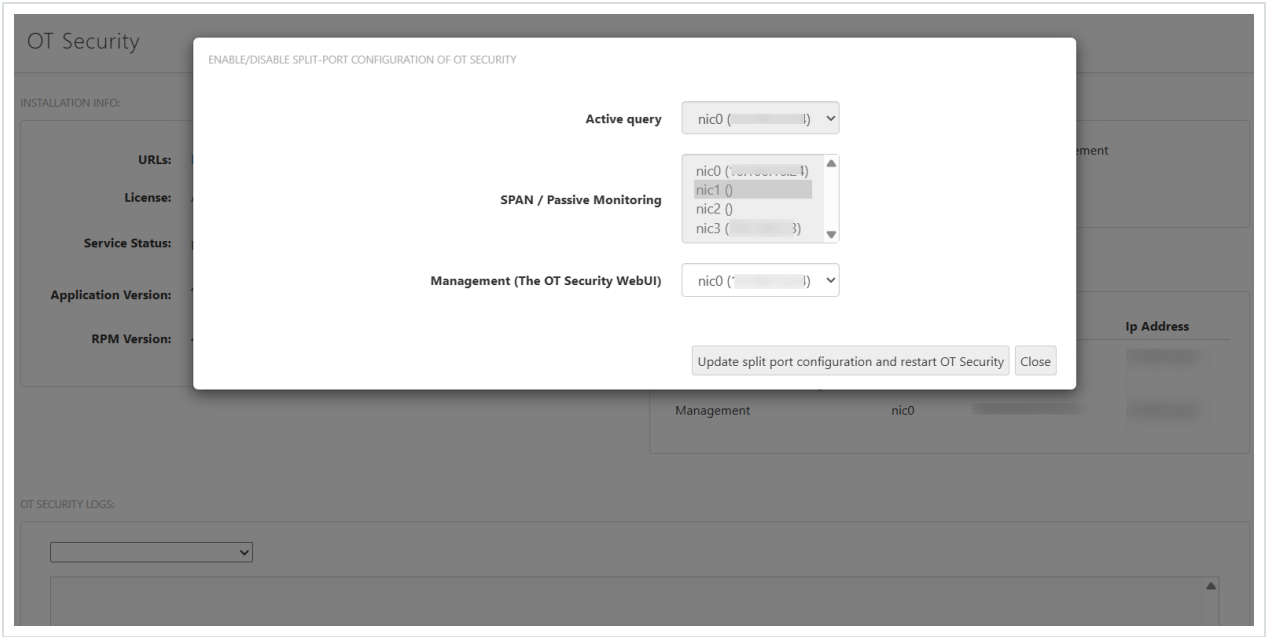
4. (Optional) Select the interface roles.

> Note: You can choose to retain the default configuration. The default interfaces configuration includes Port 1: Management + Active Query and Port 2: Passive Monitoring.

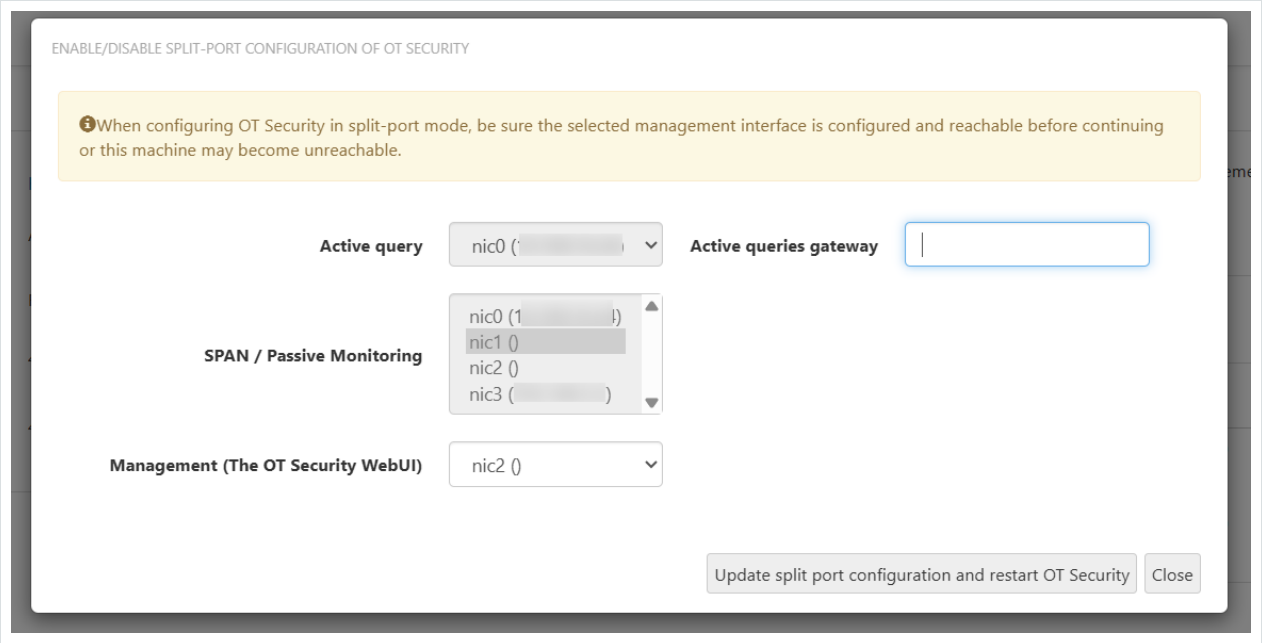


a. In the Split Port Configuration Info section, click Change split-port settings.

The Enable/Disable Split Configuration of **OT Security** window appears.



b. In the Management (The **OT Security** Web UI) box, move the management port to another interface, for example, Port 3.



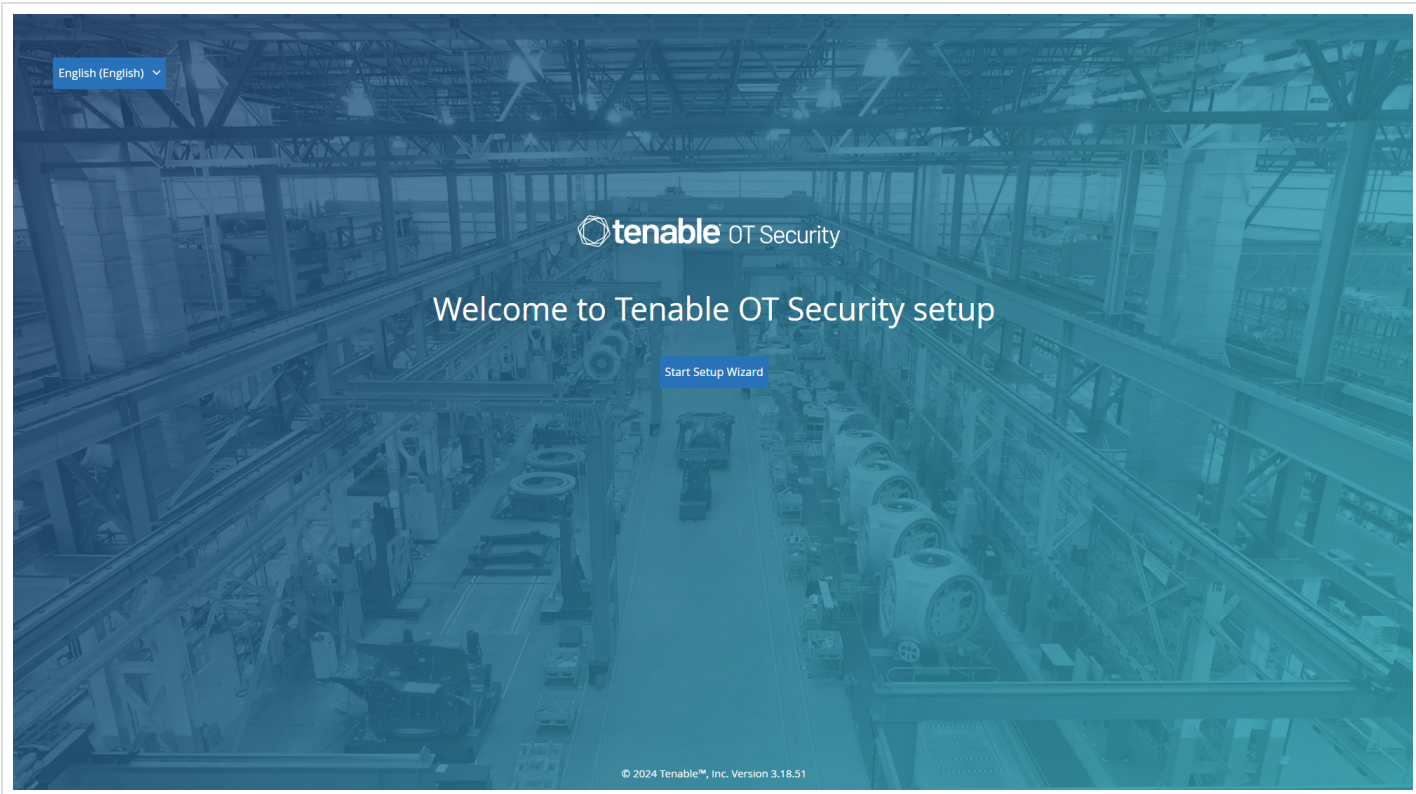
c. (Optional) In the Active queries gateway box, provide the gateway IP address.

d. Click Update split-port configuration and restart OT Security.

Tenable Core initiates a restart or installation as required.

> Caution: Do not install other updates or restart at this stage. The installation process may take some time to complete. Do not disrupt the installation process.

When the installation is complete, you can click the link in the URLs box to log in to the OT Security user interface.



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. Connect and Configure Management and Active Query Port Separation

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

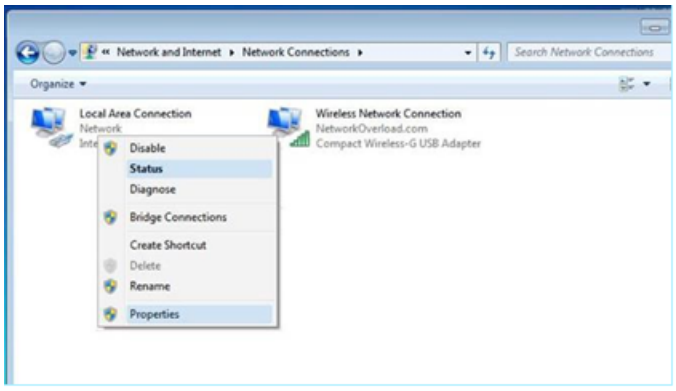
Log into the OT Security Management Console

To log into the OT Security management console:

1. Do one of the following:
   - Connect to the Management Console workstation (for example: PC and laptop) 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.

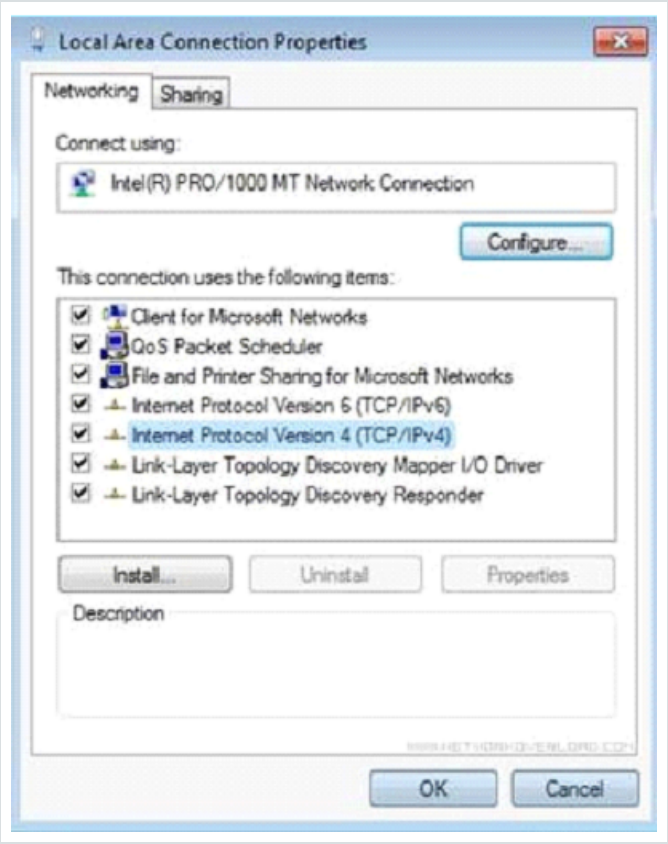
      The Network Connections screen appears.



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.

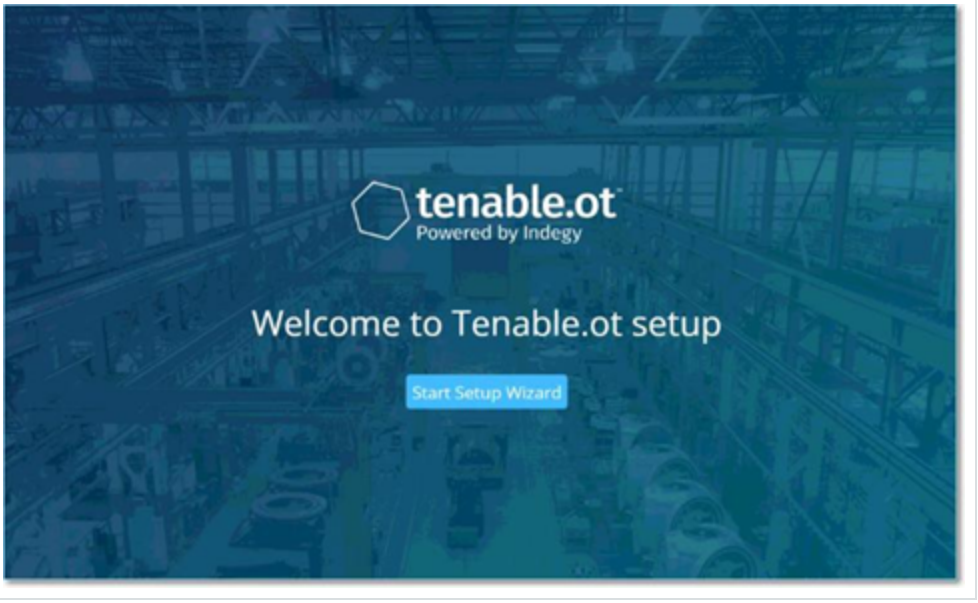
f. In the Subnet mask box, type 255.255.255.0.

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

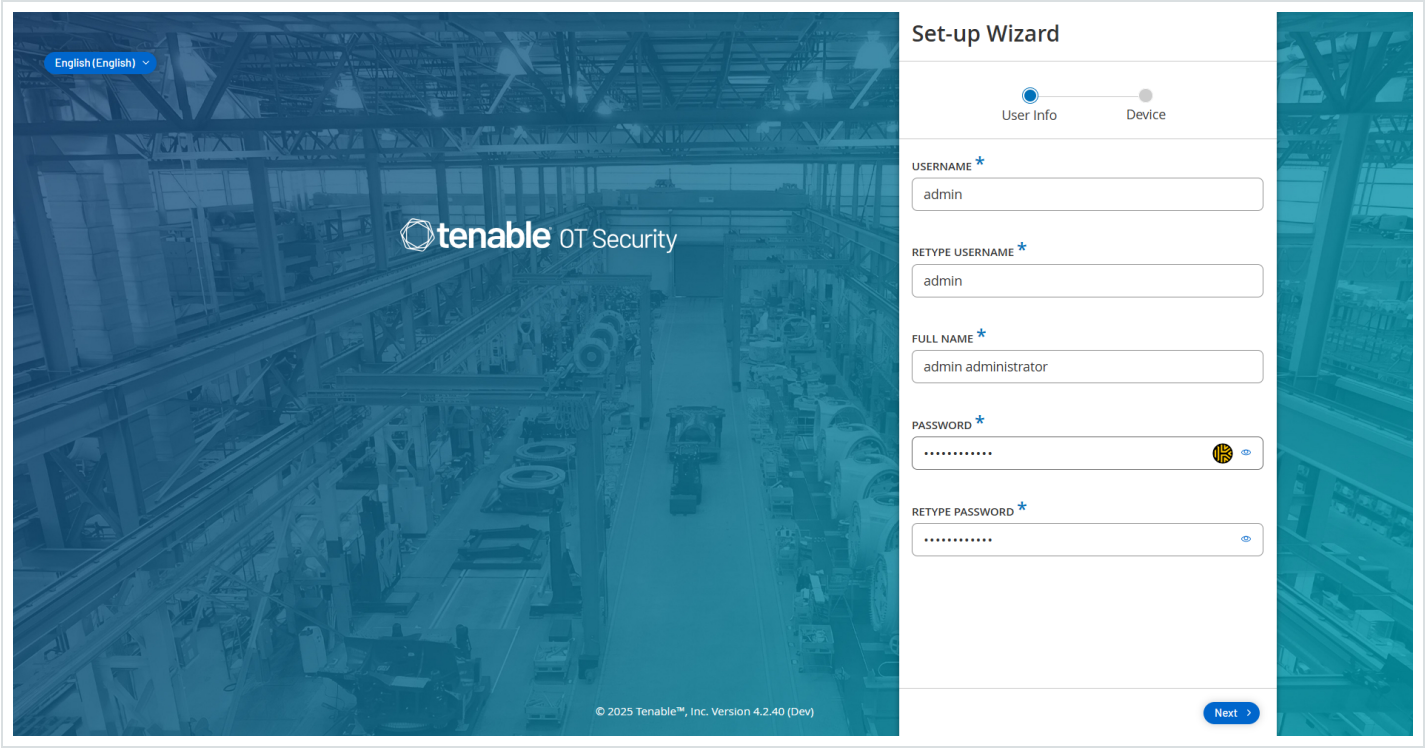
User Info

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



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 password.
6. Click Next.

   The Device page of the setup wizard opens.

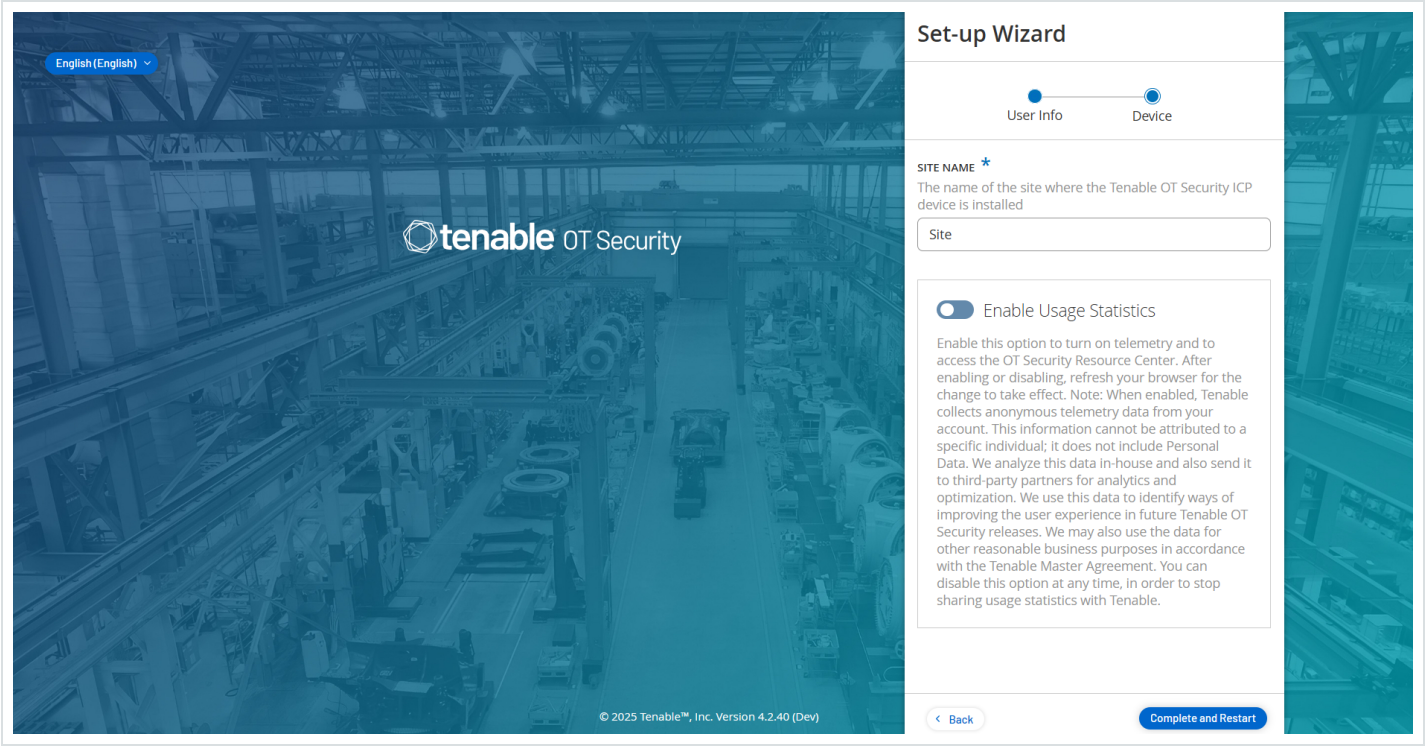
What to do next

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).



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

1. In the Site Name box, provide the name of the site where you installed OT Security.
2. (Optional) Click the Enable Usage Statistics toggle to allow OT Security to collect telemetry data and to access Resource Center.
3. Click Complete and Restart.

   OT Security restarts.

What to do next

- Connect and Configure Management and Active Query Port Separation
- OT Security License Activation

Connect and Configure Management and Active Query Port Separation

This is an optional step. If you selected the Split-Port option (to separate the Active Queries interface role from the Management role), you can now connect the secondary interface of the OT Security

appliance to its appropriate network switch interface, provided you have not done so in Tenable Core.

For more information see Management and Active Query Roles Separation (Split-Port).

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.

OT Security License Activation

Required OT Security User Role: Administrator

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 Account Management 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 Account Management portal for creating new sites to manage your assets.

For more information about the Account Management portal, see the Account Management Portal documentation.

To activate your OT Security license:

1. Log in to the Tenable Account Management portal using your community account.

   The Account page appears with the options that you have permissions to view.

2. Click the Tenable OT Security license.

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

3. From the Activation 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.

c. In the License code box, paste the code (Activation Code) that you copied from the Account Management portal.

d. Click Verify.

   OT Security enables the Generate activation certificate section.

e. Click Generate Certificate.

   The Generate Certificate panel appears.

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

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

5. In step 3 Enter activation code, click the Self-service link to open the Tenable Account Management portal.

   The Account Management portal page appears.

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

6. In the left navigation pane, click Products.

   The My Products page appears.

7. Search for your product using the 20-digit license code from OT Security.

   The OT Security product with the specific license code appears.

8. Click the Sites tab.

The Sites tab appears.

9. To create a site, click Manage Sites > Create Site.

   The Create New Site window appears.

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

      > Tip: Use the Label field to include the name of the device or ICP, which can help you differentiate between the various sites.

   b. In the Size box, type the number of IP addresses you want to assign to this site.

      > Tip: To adjust the number of IP addresses assigned to the license, use the slider located under the Size 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.

   f. Click Confirm.

10. Navigate back to the OT Security instance.

11. In the step 3 Enter activation code section, click Enter Activation Code.

    The Enter Activation Code panel appears on the right.

12. In the Activation Code box, paste the one-time generated code that you copied from the Tenable OT Security Account Management page. See step 8e.

13. Click Activate.

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

14. Click Enable.

    OT Security is now enabled and ready to use.

15. Navigate back to the Tenable Account Management portal and in the one-time generated activation code dialog box, click the I confirm I have saved the activation license checkbox.

16. Click Confirm.

    The newly added site appears in the Sites tab 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. When you update your license, you use your existing 20-digit license code.

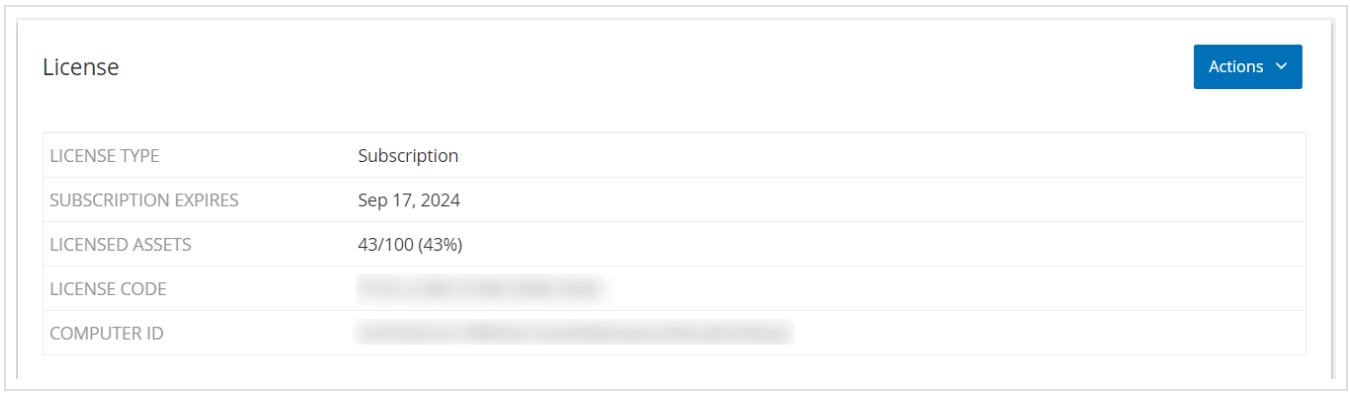
Before you Begin

- 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:

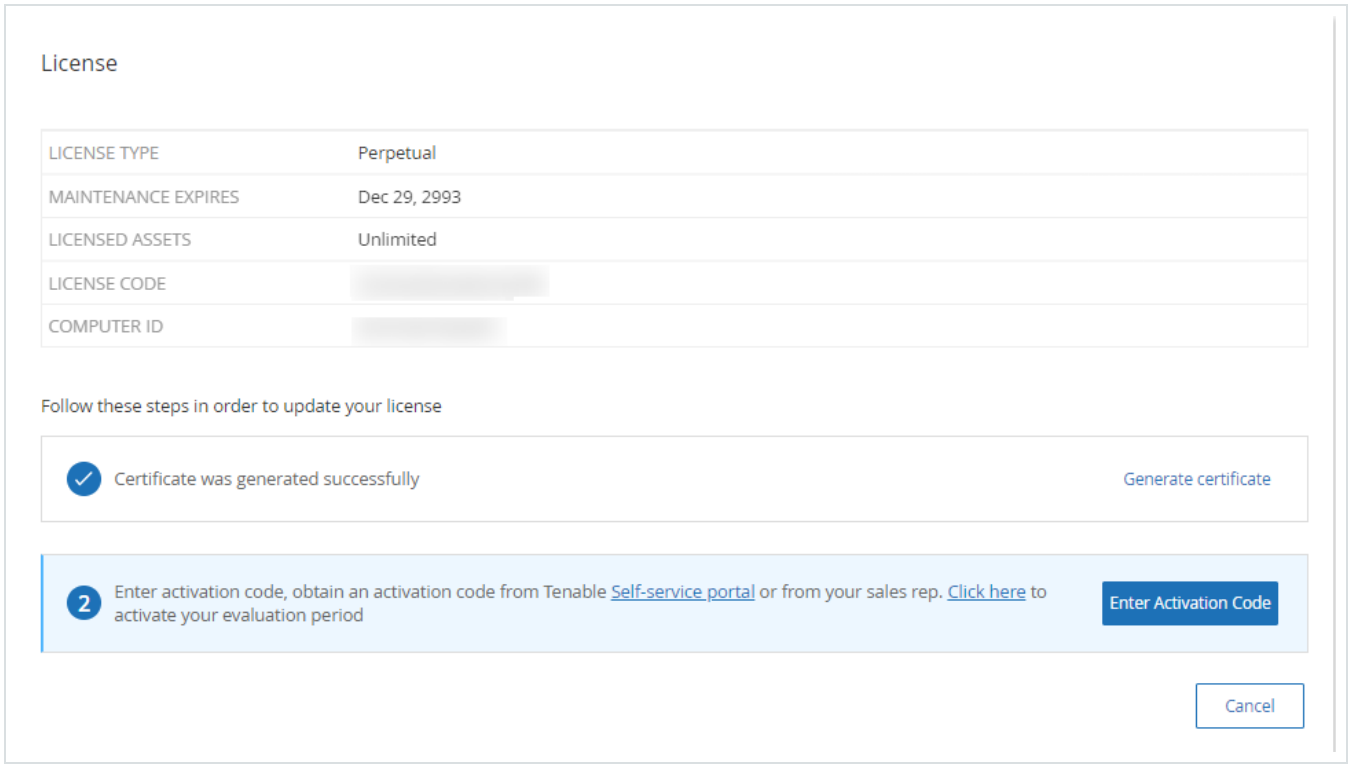
1. Go to Settings > System Configuration > License.

   The License window appears.



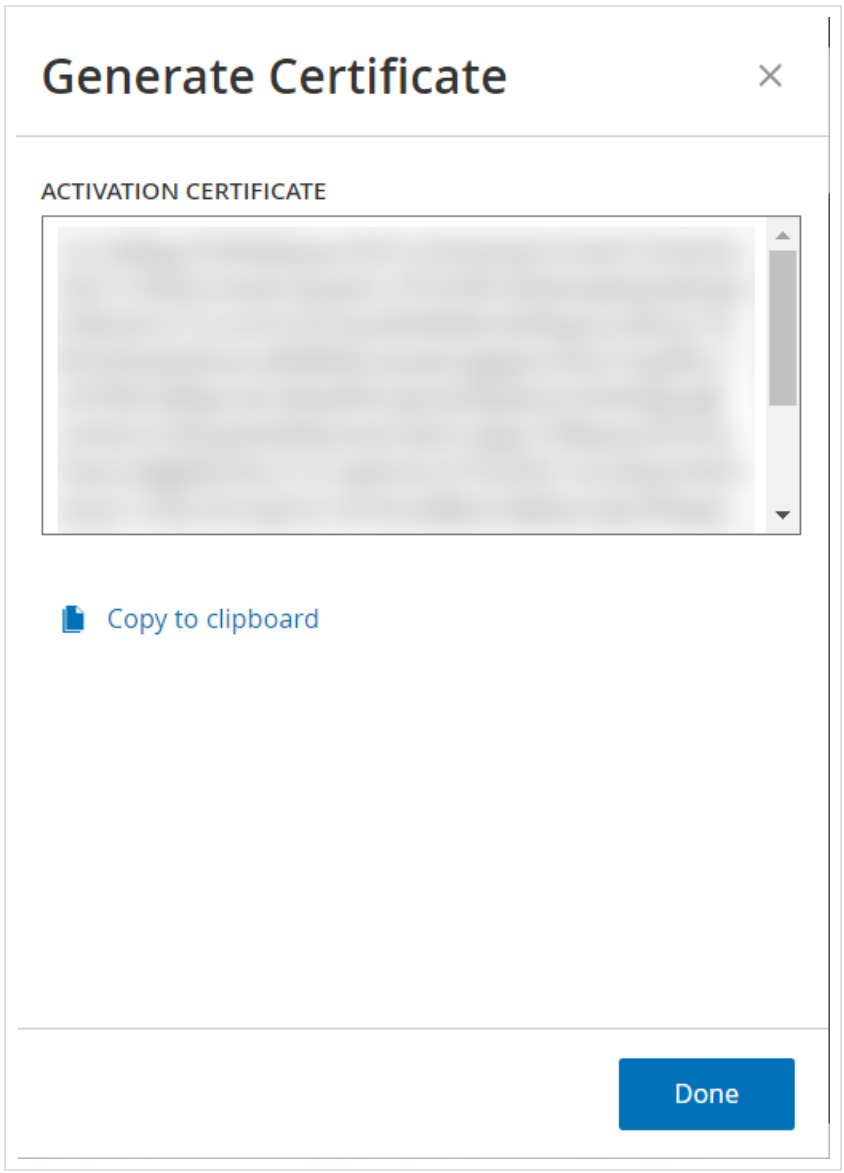
2. From the Actions menu, select Update license.

   The Generate Certificate and Enter Activation Code steps appear.



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. In the (2) Enter Activation Code box, click the Self-service portal link.

   OT Security redirects you to the My Account page on the Tenable Account Management portal.

Note: If you are on evaluation period, click the second link. See Update your license in offline mode.

6. Edit the site details in the Tenable Account Management portal:

   a. In the left navigation pane, click Products.

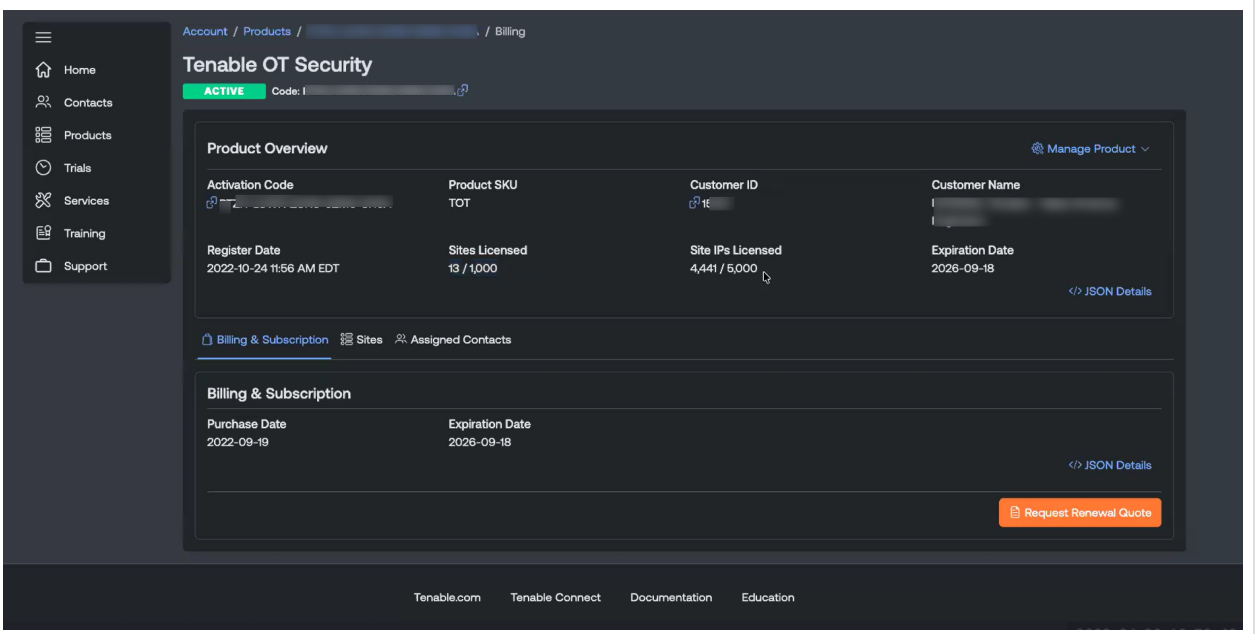
      The My Products page appears.

   b. Search for your product using the 20-digit license code from OT Security.

      The OT Security product with the specific license code appears.

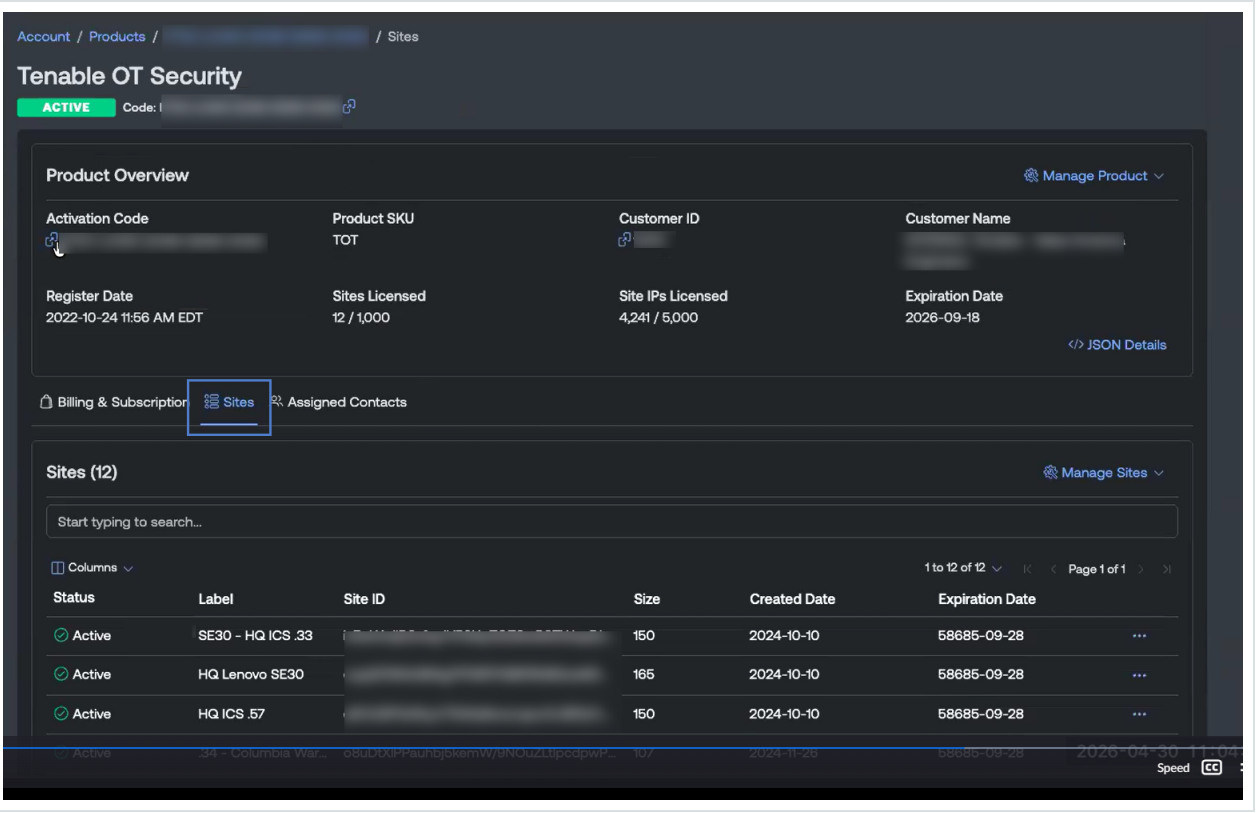
   c. Click the license code to view the product details.

      The Tenable OT Security page appears with details such as Product Overview, Billing & Subscription, and Sites.



   d. Click the Sites tab.

      The Sites section appears.

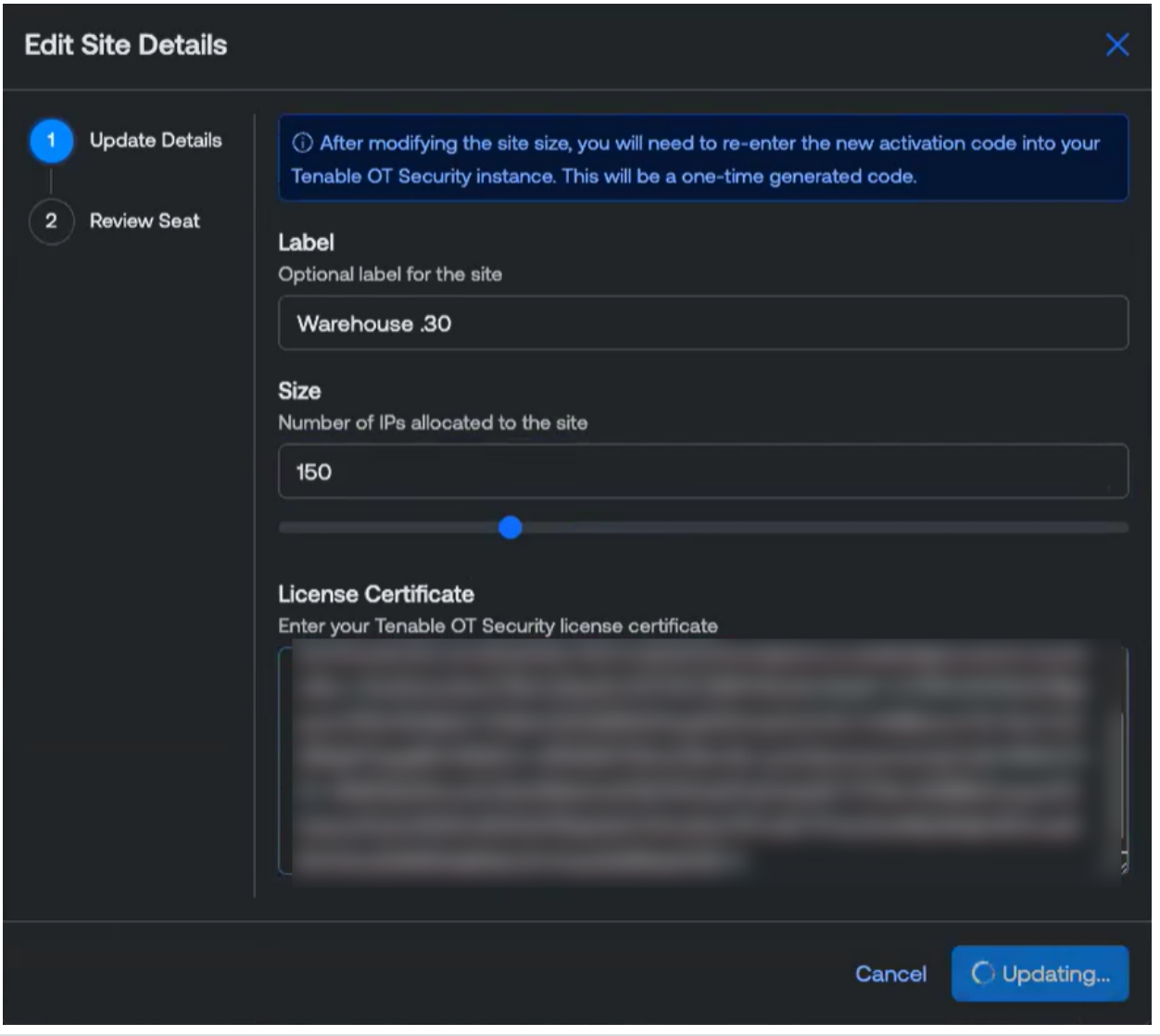


e. In the row of the site you want to edit, click the ••• button.

A menu appears.

f. Click Edit Site.

The Edit Site Details page appears.

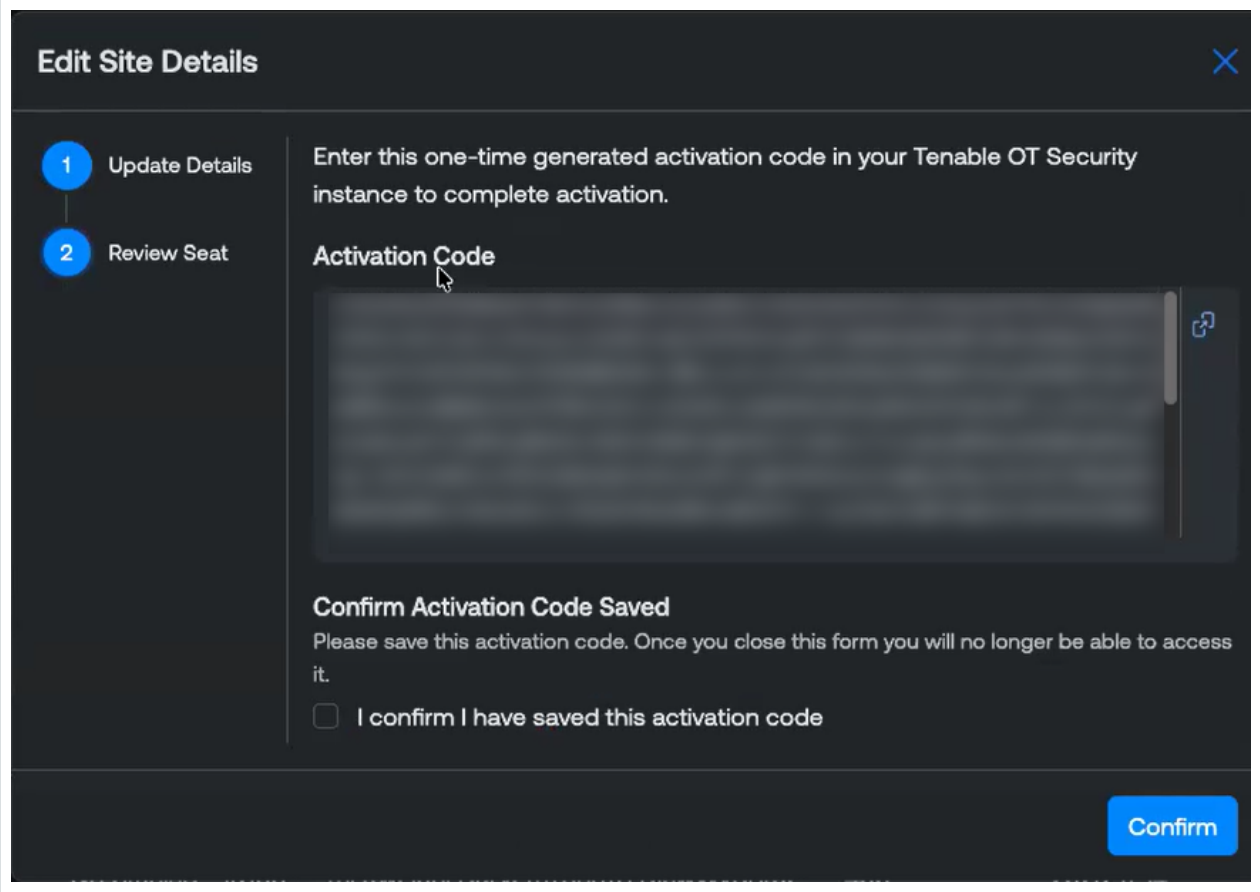


g. Adjust the details as needed.

h. In the Activation Certificate box, paste the certificate that you copied from the Generate Certificate window in OT Security.

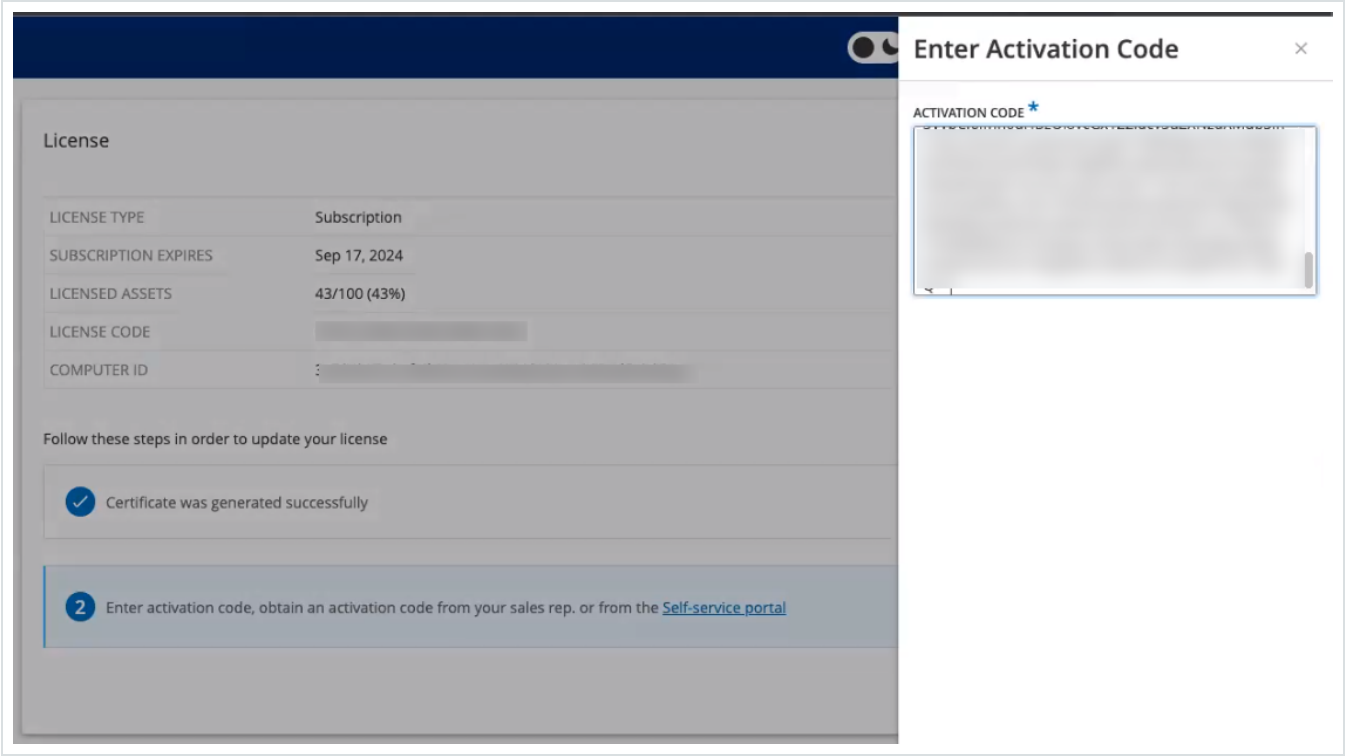
i. Click Update.

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.



j. Click the button, then click Confirm.

7. Navigate back to the OT Security instance.
8. In the (2) Enter activation code box, click Enter Activation Code.
9. In the Activation Code box, paste the one-time generated code that you copied from the Tenable OT Security Account Management page.

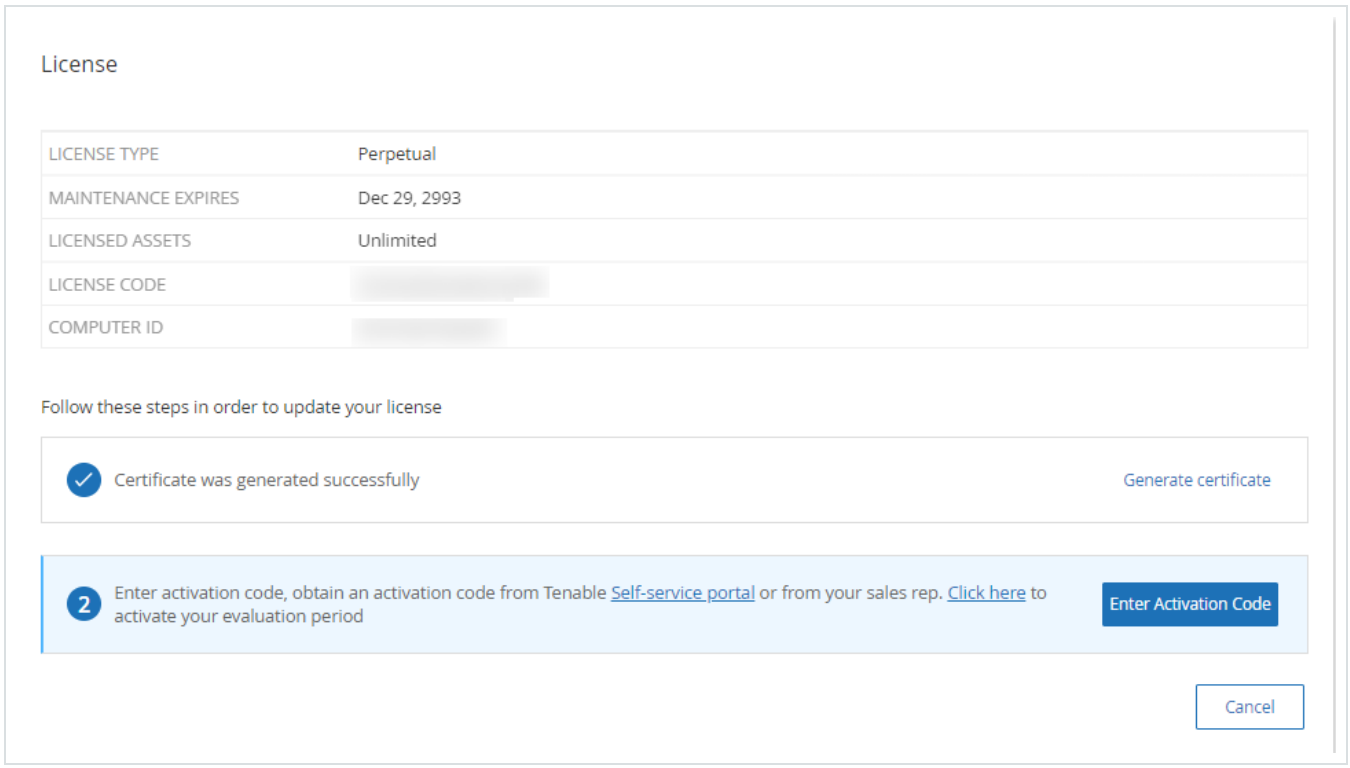


10. Click Activate.

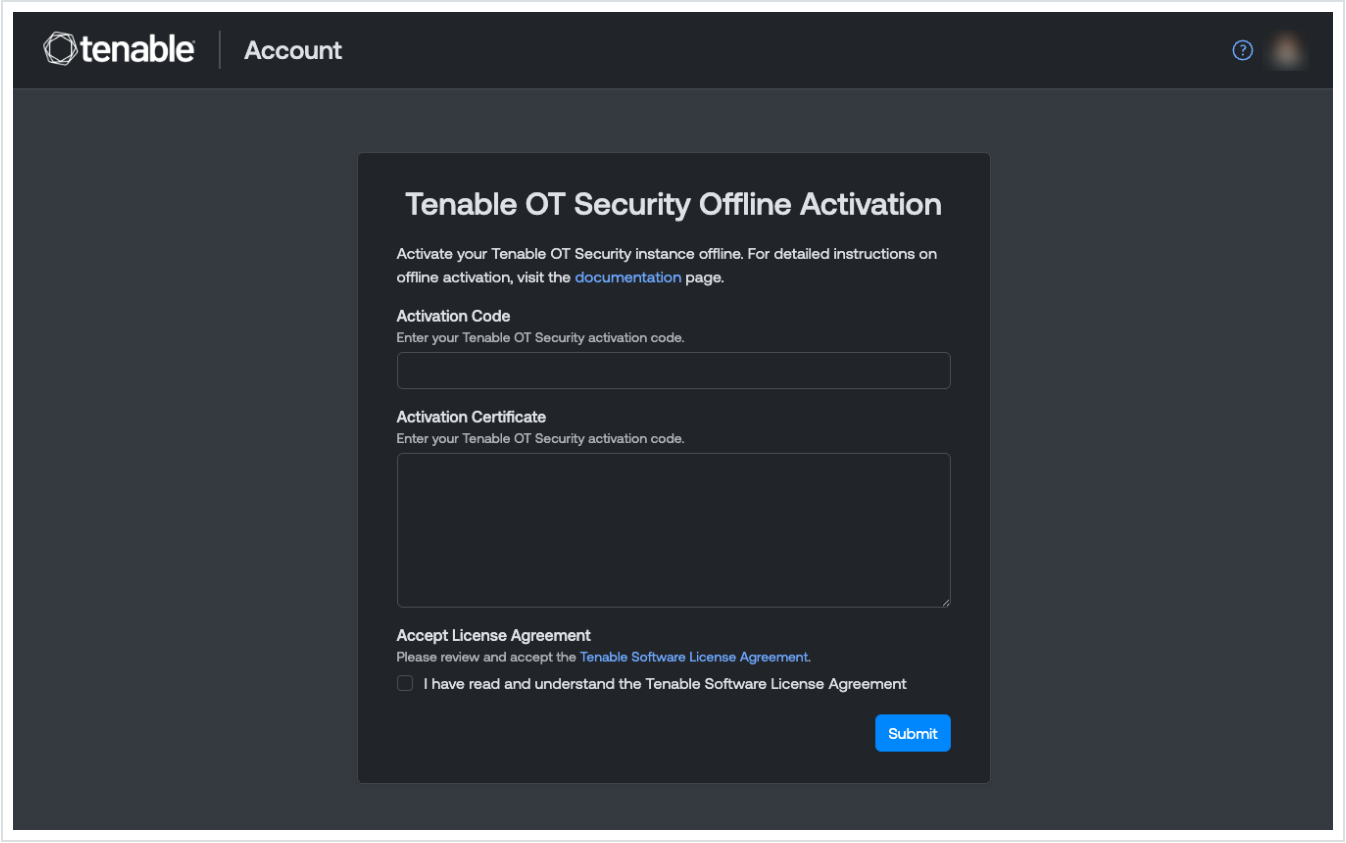
    OT Security shows a confirmation message that the system activated successfully and the License page shows the updated license details.

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.



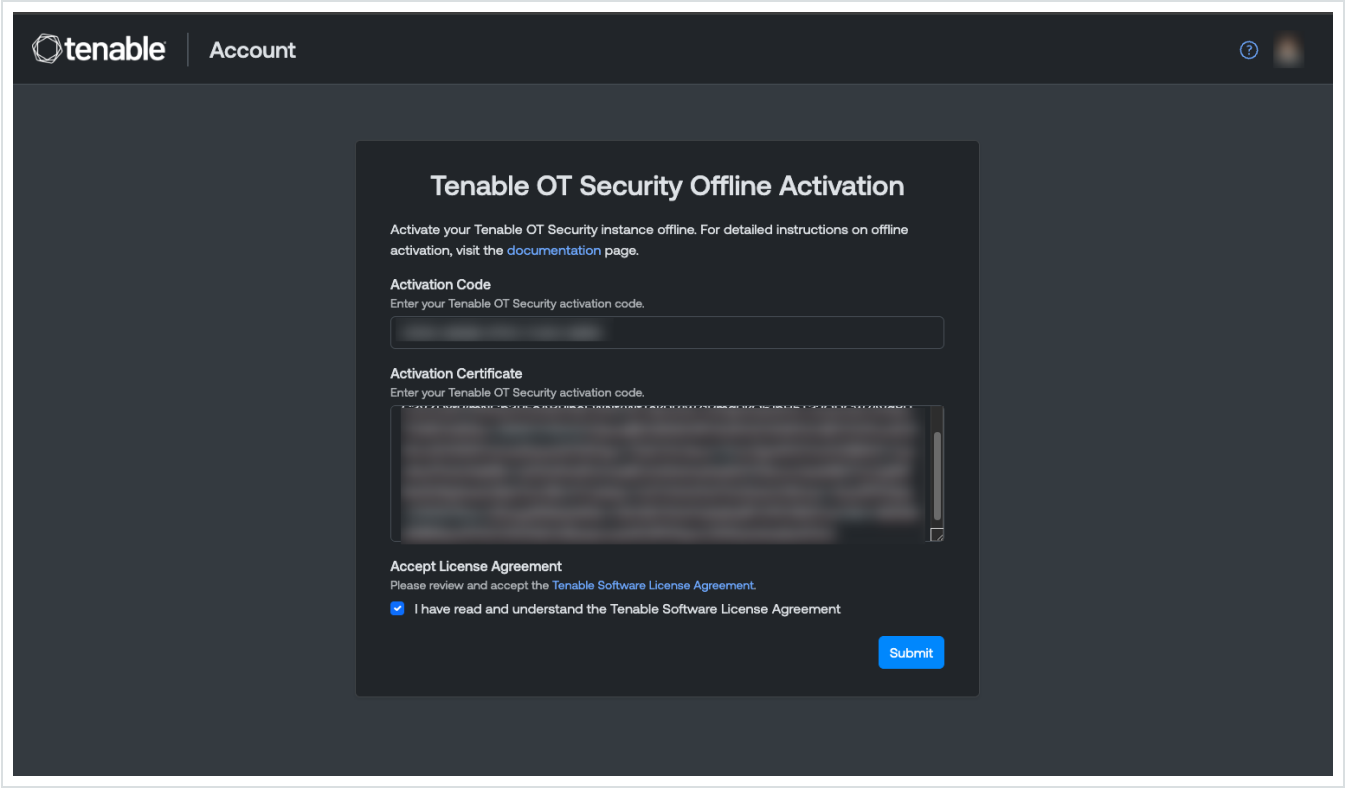
The Activate OT Security Offline window opens in a new tab.



> Note: You can access the Activate OT Security Offline screen from an Internet-connected device using the following URL: https://account.tenable.com/offline-activation/ot-security.

> 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.

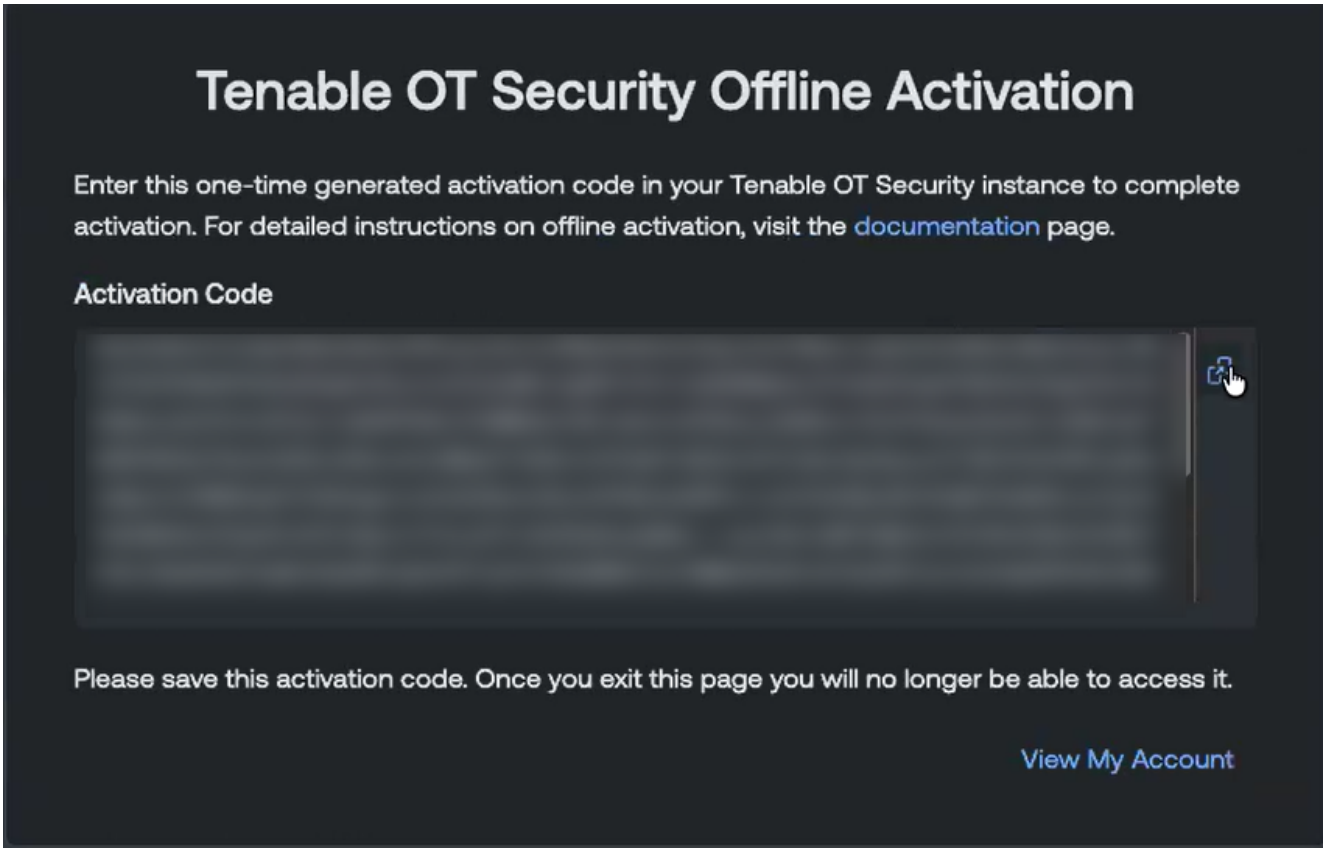
3. In the Activation Code box, type your 20-character License Code (which you can copy and paste from the License window).
4. In the Activation Certificate box, paste the Activation Certificate.
5. Click the I have read and understand the Tenable Software License Agreement checkbox.



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

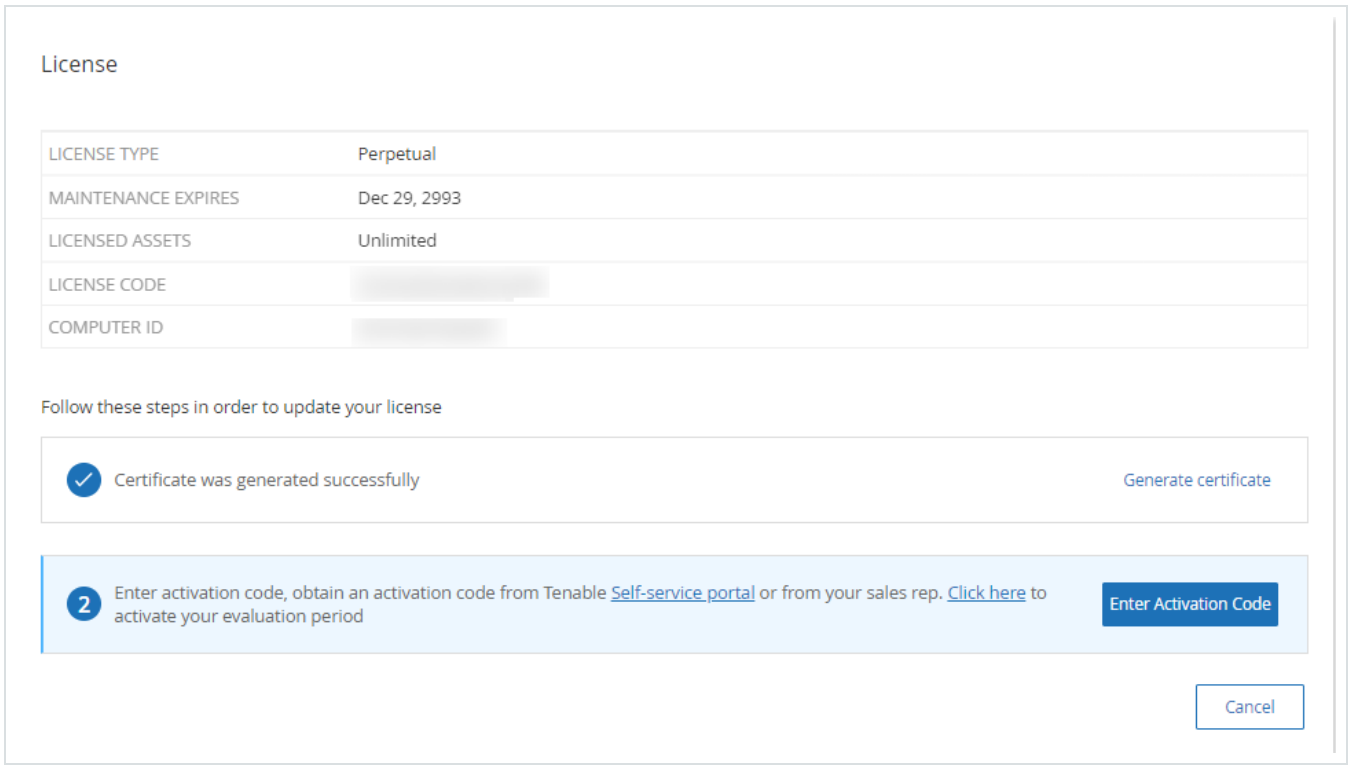
6. Click Submit.

   OT Security generates the activation code.



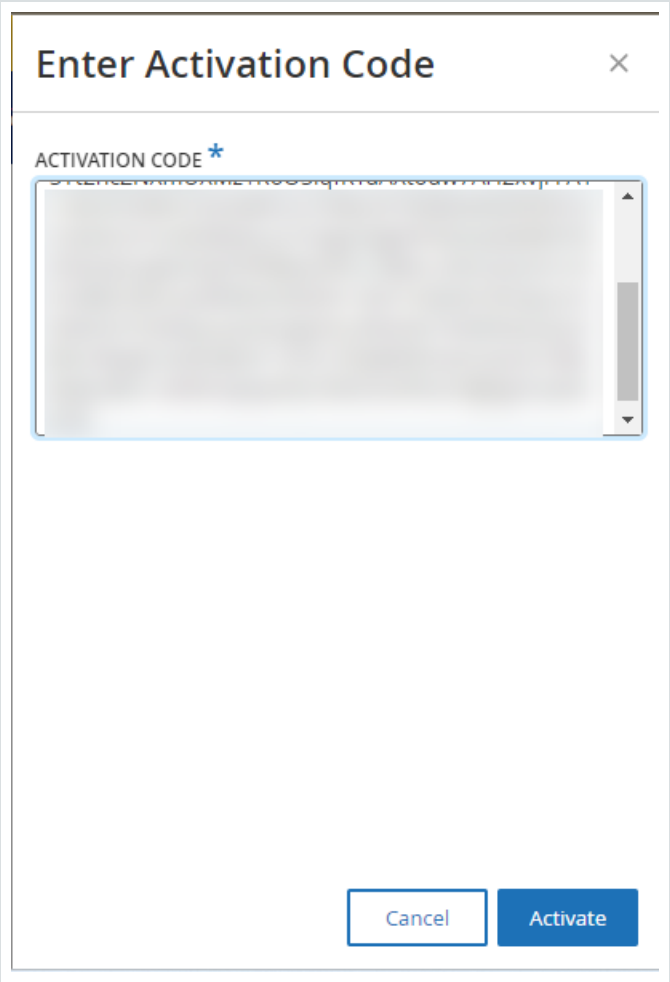
7. To copy the activation code, click the button.

8. Navigate back to the License tab in OT Security, and click Enter Activation Code.



The Enter Activation Code side panel appears.

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

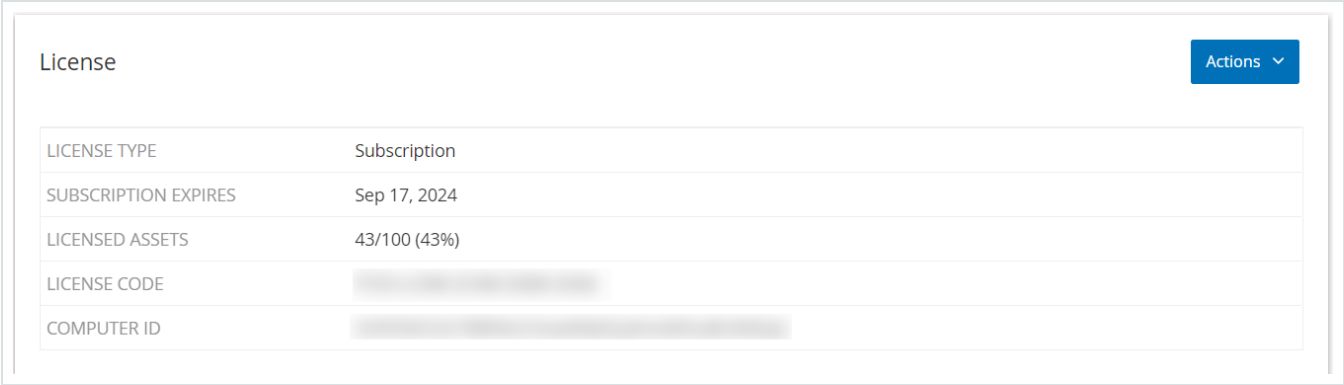
> Note:An evaluation or temporary license always has a unique license code.

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 (letters / 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:

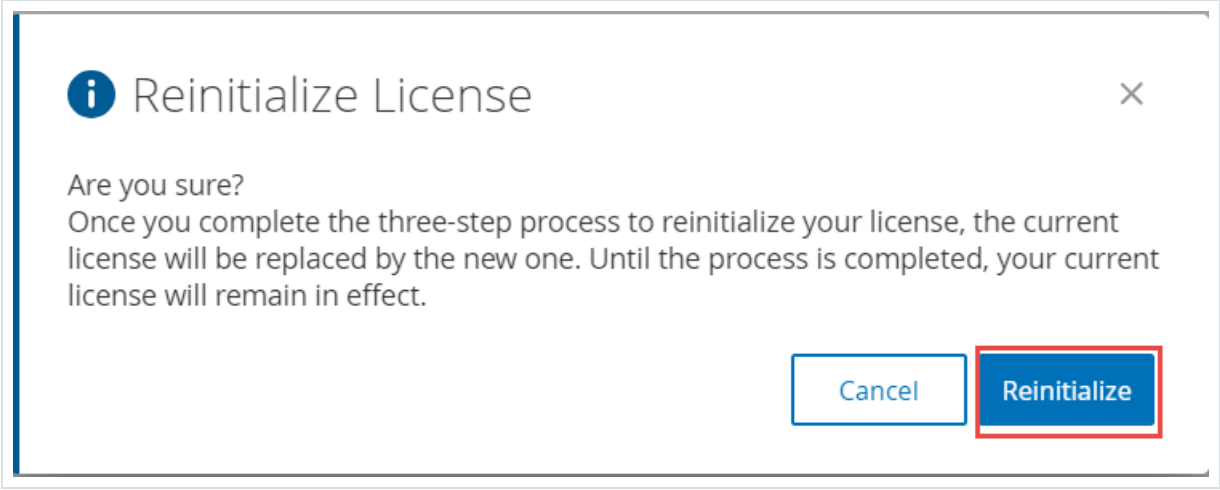
1. Go to Settings > System Configuration > License.



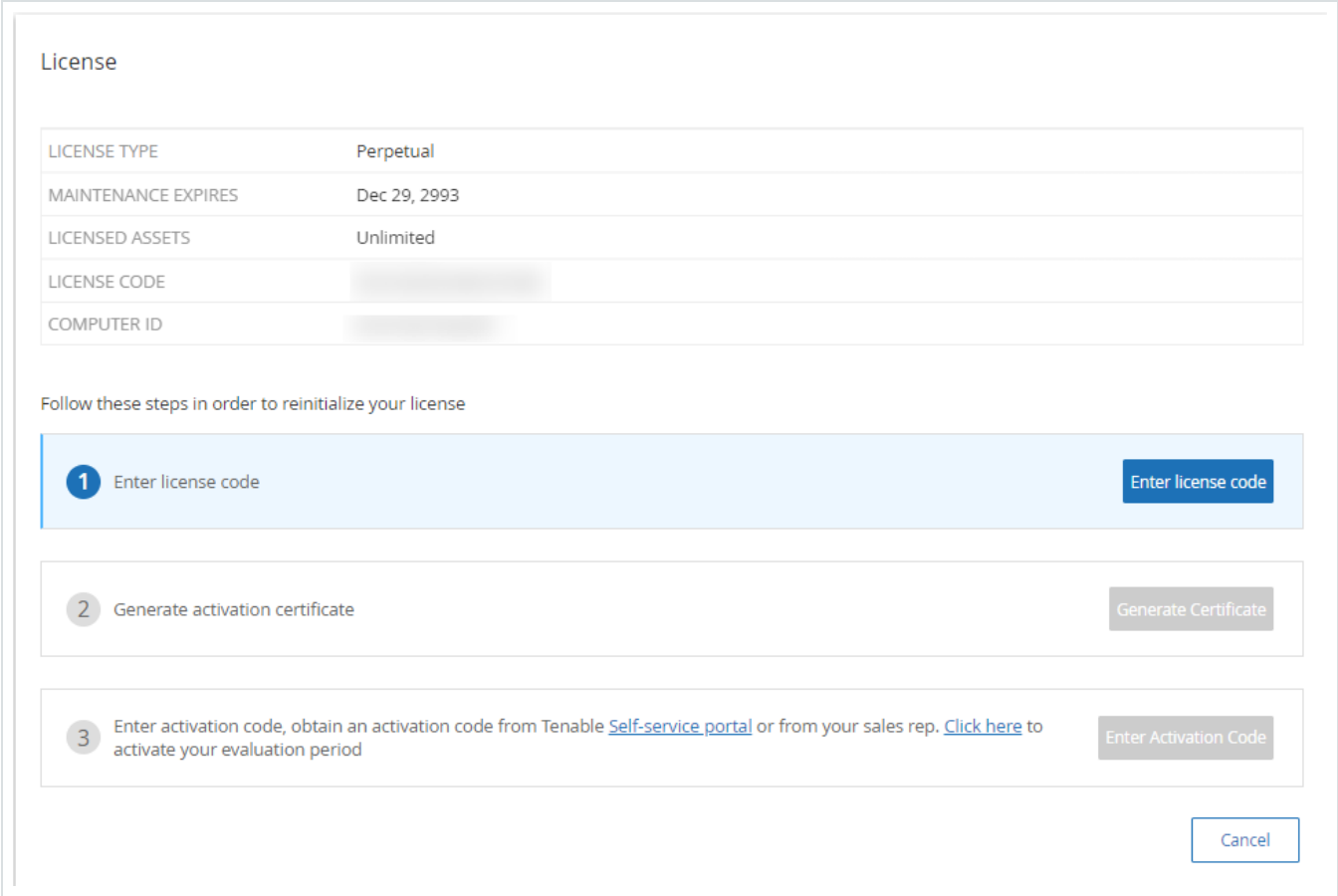
2. From the Actions menu, select Reinitialize license.

   A confirmation window appears.

3. Click Reinitialize.



The License window appears with the three reinitialization steps.



4. Follow the system start-up steps (Step 1 to Step 17) for activating your license in the Activate your License section.

   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, and authentication servers to start using OT Security.

Enable the OT Security System

Required OT Security User Role: Administrator

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.

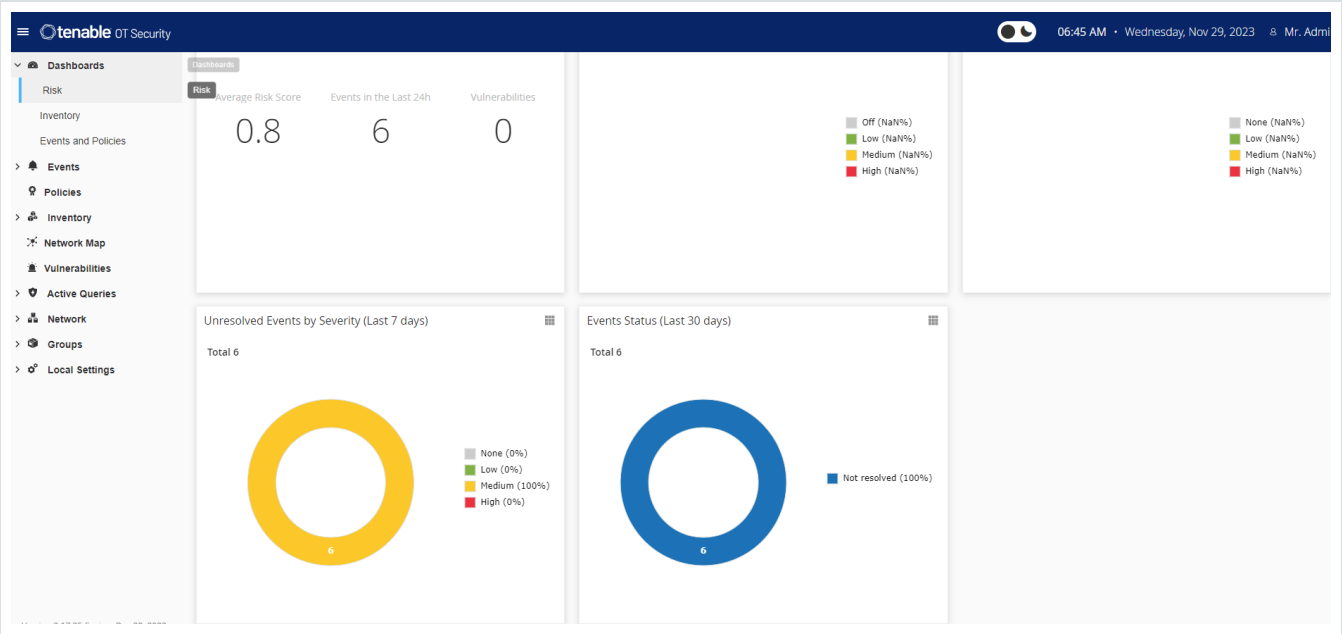
You can configure and activate additional functions such as Active Queries on the Settings window in the Management Console (user interface). For more information, see Active Queries.

> Important: Beginning with version 4.4, passive monitoring is disabled by default when you enable OT Security to reduce alert overload. To enable passive monitoring, navigate to the Settings > Network Definitions page and click to enable the Passive Monitoring toggle. The passive monitoring icon in the header indicates if the passive monitoring is enabled or disabled.

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 Environment Settings.

> 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).

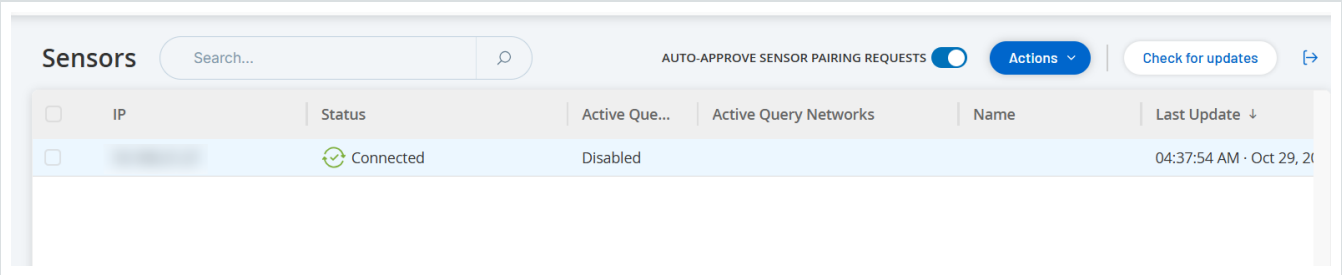
> Note: Tenable recommends a dedicated ICP user with administrator role for the process of pairing sensors, to prevent disruptions in connectivity (see Adding Local Users). You can add a new administrator user to pair multiple sensors.

> 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 Settings > Sensors window.

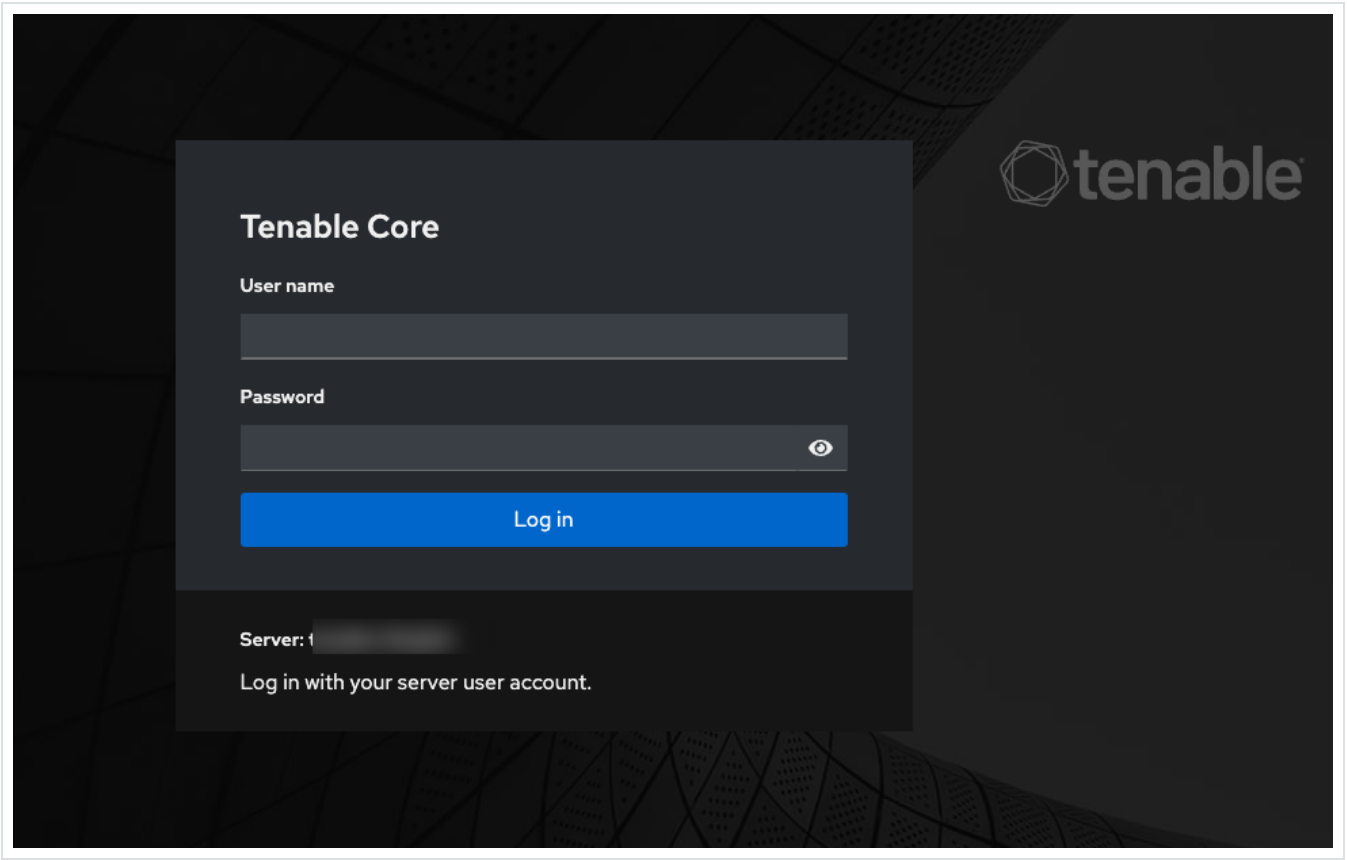


2. To enable automatic approval of Sensor Pairing, ensure that the Auto Approve Incoming Sensor Pairing Requests switch at the top of the page is toggled to ON. If not, all pairing requests require manual approval.

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.

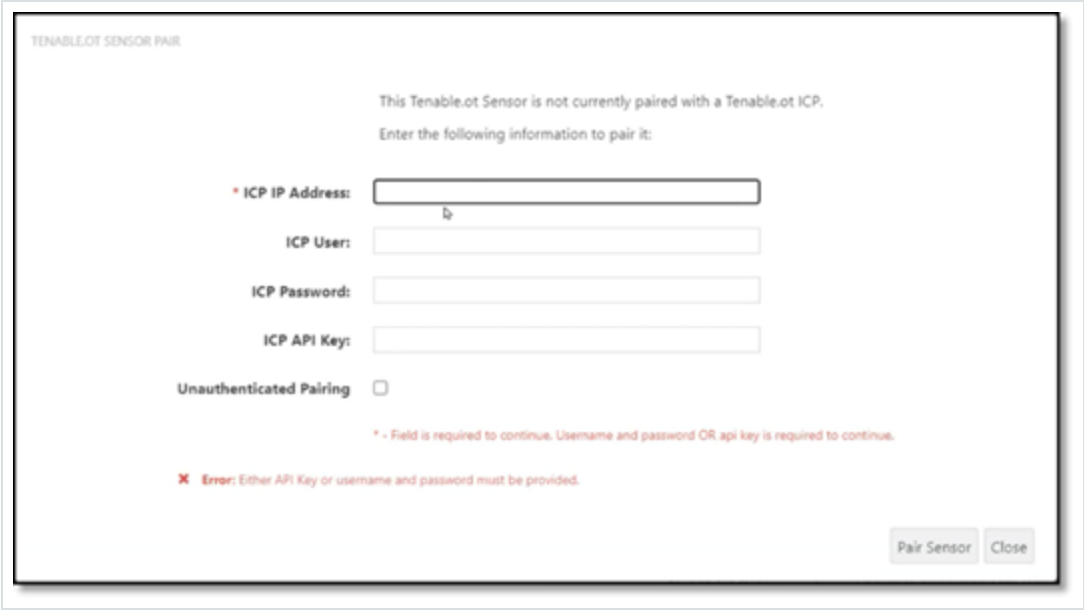
4. In the Tenable Core console login window, type your Username and Password, select the Reuse my password for privileged tasks checkbox, and click Log In.



> 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.



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.

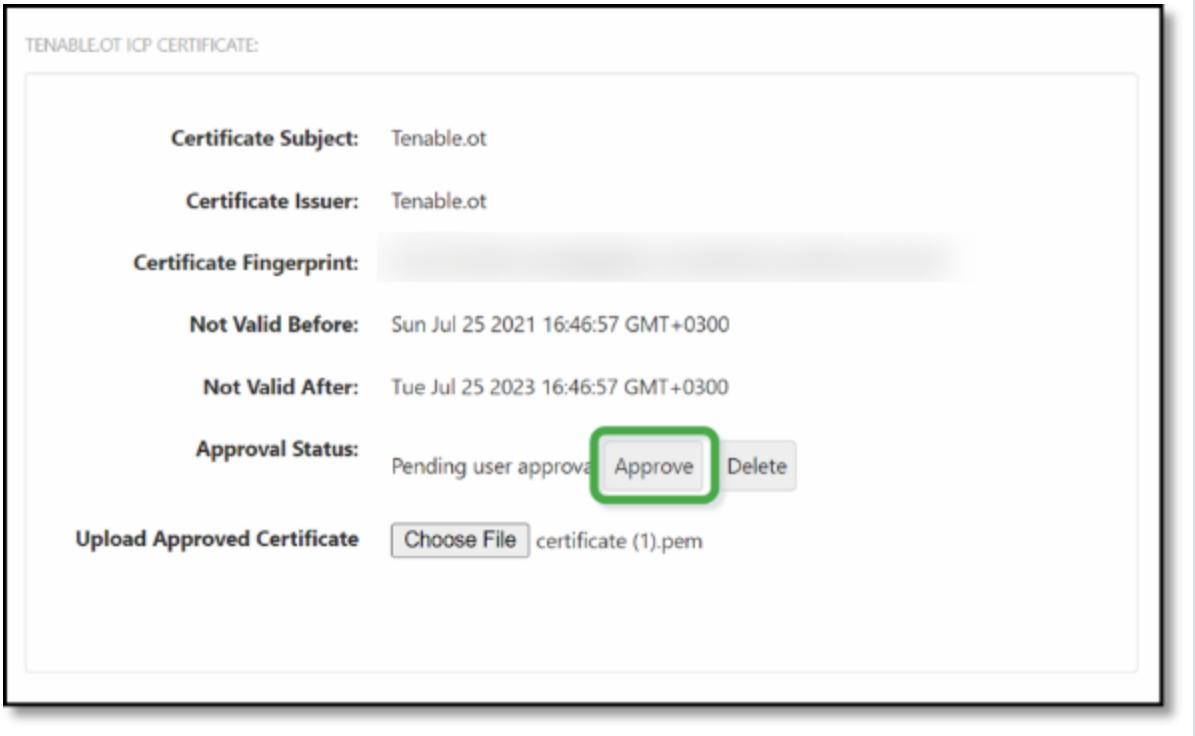
Note: Tenable recommends that you create a dedicated ICP user for pairing sensors in order to ensure connectivity during the pairing process (see Adding Local Users).

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.

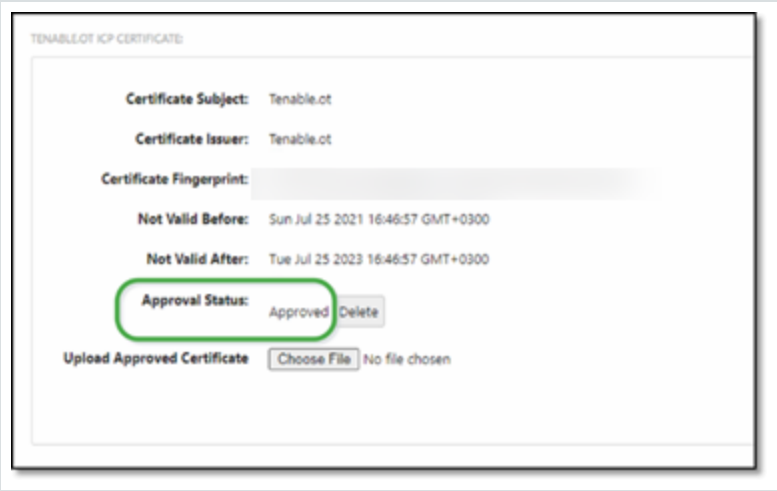
    If you prefer to upload a certificate manually:

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.

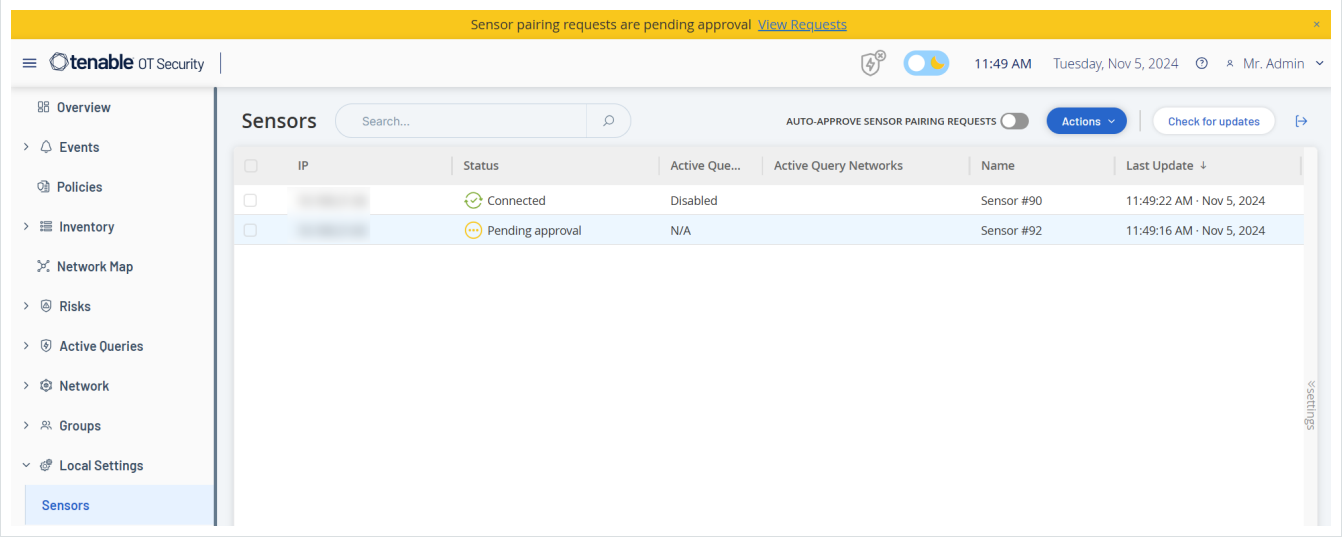
c. Navigate to the `.pem` certificate file to upload.

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

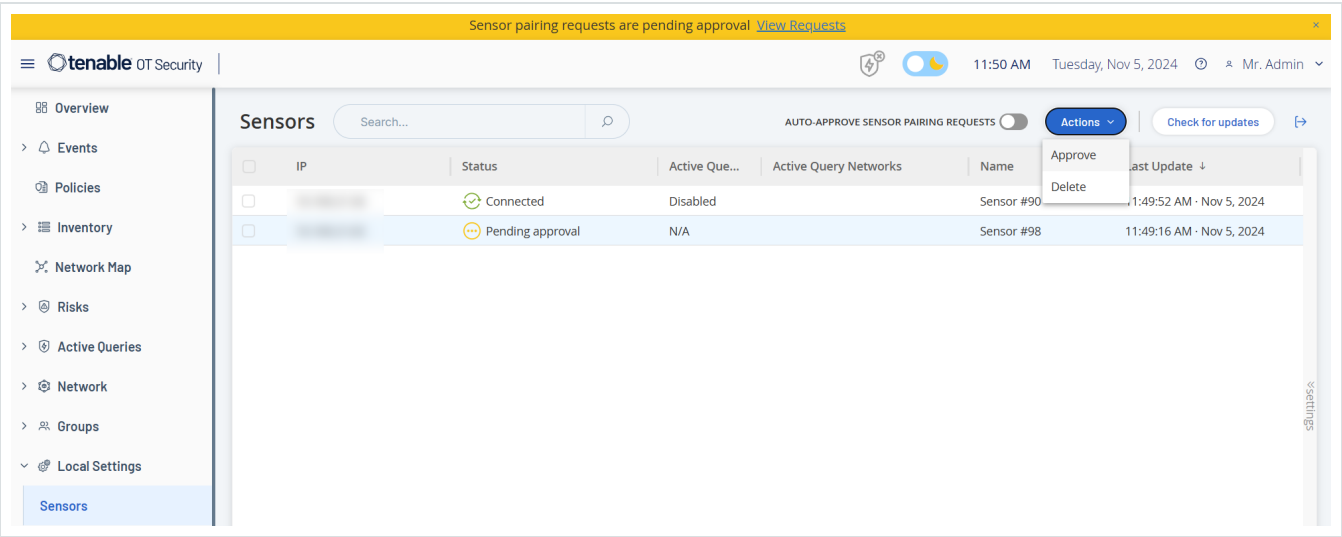


11. In the ICP user interface, navigate to Local Settings > Sensors.

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 Manage 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

You can install the configurable model sensor in a DIN rail or mount it on a standard 19-inch rack (using the “mounting ears” adapter kit).

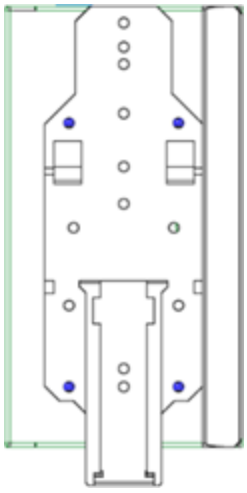
Set up a Configurable Sensor

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

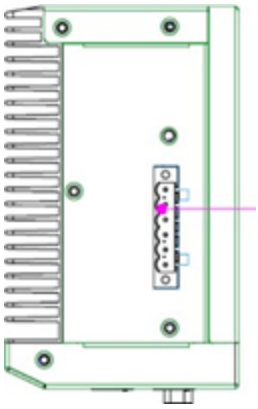
To mount the OT Security Configurable Sensor on a standard DIN rail:

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.

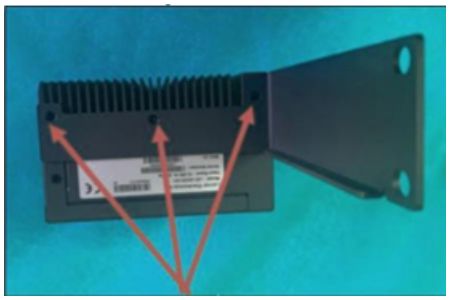
Then, insert the AC power supply cable (provided) into the power supply unit, and plug the other end into an AC outlet.

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.

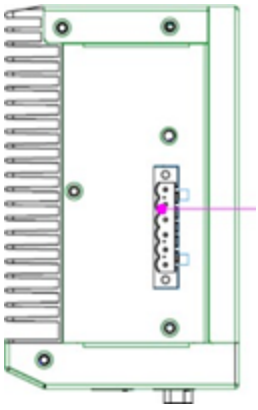
Note:

- 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 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 and laptop.) directly to Port 1 of the OT Security Sensor using the Ethernet cable.
    - Connect the Management Console workstation to the network switch.

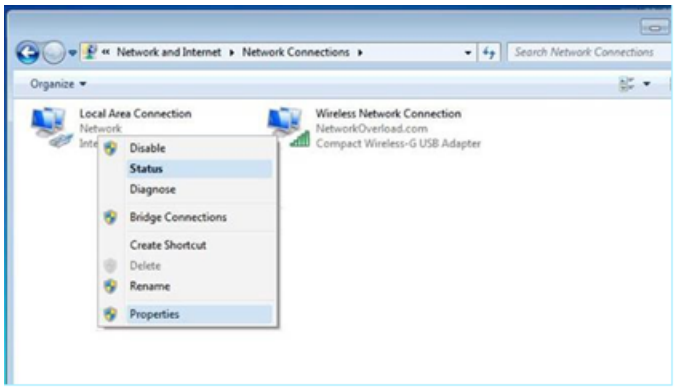
2. Ensure that the Management Console workstation is part of the same subnet as the OT Security Sensor (which is 192.168.1.5) or is routable to the unit.

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.

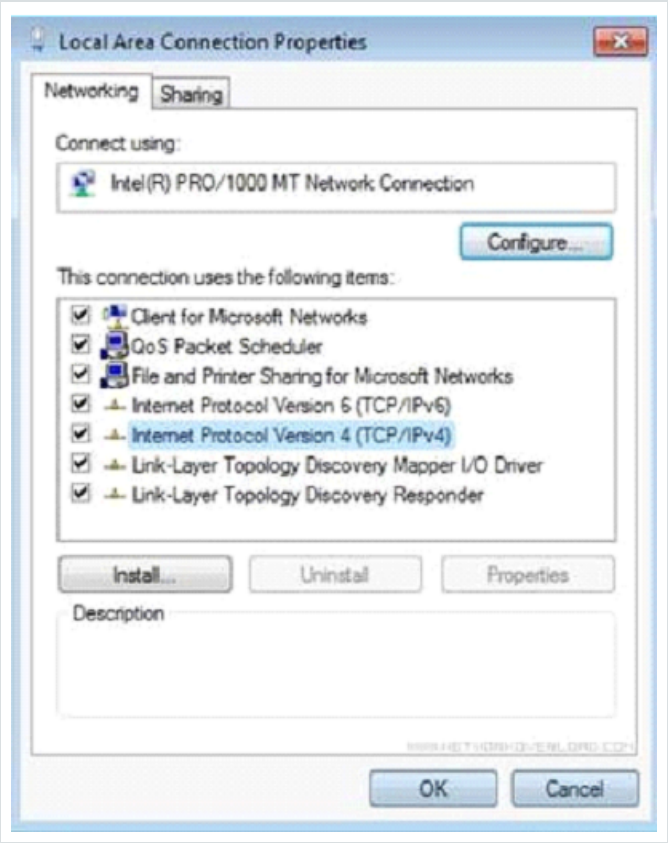
    > Note: Navigation may vary slightly for different versions of Windows.

    The Network Connections window appears.

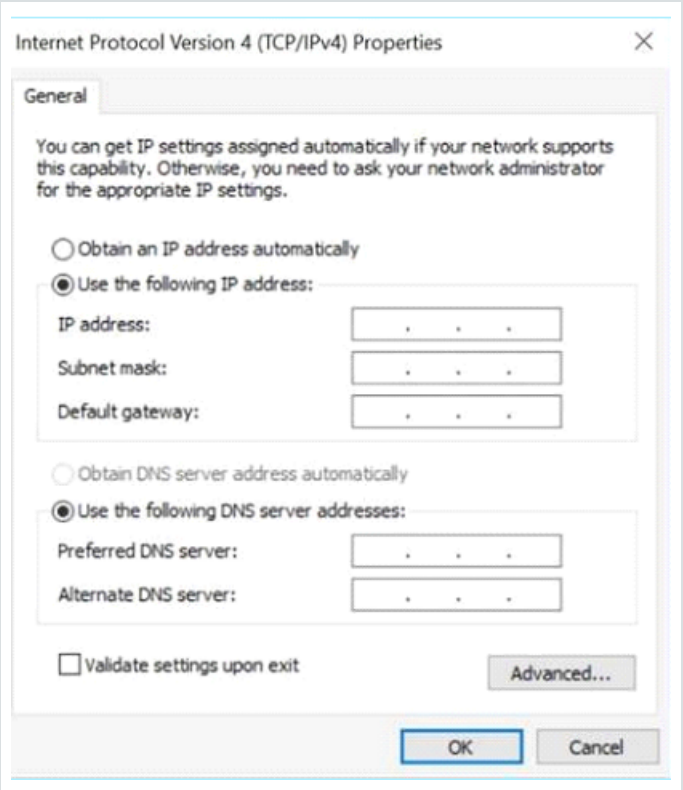
    b. Right-click Local Area Connections and select Properties.

    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.

Establish Console Connection and Initial Setup

This topic explains how to connect a local serial console to your OT Security appliances (ICP and Sensors). Use this connection method for initial IP configuration, network troubleshooting, or restoring access when the management IP is unreachable.

Before you Begin

Make sure you have the following software and hardware:

Software

- Terminal Emulator: A utility such as PuTTY, Tera Term, Serial, or Minicom.
- Drivers: Ensure you install the drivers for your specific USB cable or adapter(for example, FTDI or PL2303).

Hardware and Cabling Options

Identify your appliance type to select the correct cabling method:

- **Tenable OT Security** or **Tenable** ICP (Industrial Core Platform) Console
    - Port Type: RJ-45 Console.
    - Recommended Cable: USB-to-RJ45 console cable.

> Note: A light blue Cisco-style console cable is typically included in the appliance box. This is a standard cable (approximately. $10) commonly used for network switches.

- **Tenable Sensors:** Sensors have two hardware variations. Verify the physical ports on your device:
    - RJ-45 Console Port: Use a USB-to-RJ45 console cable.
    - DB9 (Serial) Port: Use a USB-to-DB9 serial cable.

> Tip: Tenable recommends that you use direct USB-to-DB9 female connector cables (single piece) rather than multi-part adapters to minimize connectivity issues.

Alternative Method (Legacy Adapters)

If you use a standard serial-to-USB adapter instead of a direct USB-to-console cable , you must use a null modem adapter or coupler in the chain.

> Tip: Many connection failures occur because standard serial adapters do not cross the transmit or receive pins correctly without a null modem.

Physical Connection

1. Connect the USB end of your cable to your workstation.
2. Connect the other end (RJ-45 or DB9) to the appliance.
    - Labeled Ports: Locate the port that has the Console label or with a monitor or IOIOI symbol.
    - Unlabeled Ports: If the ports do not have a label, connect to the single RJ-45 port located to the left of the USB ports.
3. Ensure the cable is firmly seated.

Identify the COM Port (Windows)

You must identify the Communication Port (COM) that Windows assigned to your cable.

1. On your Windows machine, right-click Start and select Device Manager.

    The Device Manager window appears.
2. Expand Ports (COM & LPT).
3. Locate your device (for example, USB Serial Port) and note the number (for example, COM3).

Configure Terminal (PuTTY)

Launch your terminal emulator (for example PuTTY) and configure the session with the following Tenable TTY settings.

In PuTTY, go to Connection > Serial and configure the following settings:

Setting	Value
Connection Type	Serial
Serial Line:	Your COM port (for example, COM3)
Speed (Baud)	115200
Data bits	8
Stop bits	1
Parity	None
Flow Control	None Note: Ensure Flow Control is not set to `XON/XOFF`.

Tip: On the Sessions page, save these settings as "Tenable OT Console" for future use.

Establish Connection

1. Click Open to start the session.
2. When the terminal window appears, press Enter twice to wake the console.

3. Verify that the following prompt appears:

```
################################################################################

  This system is restricted to authorized users only. Individuals attempting
  unauthorized access will be prosecuted. Continued access indicates
  your acceptance of this notice.

################################################################################
```

4. Log in at the prompt.

Initial Network Configuration

The management interface requires a Static IP. DHCP is not supported.

1. Run the network manager tool:

```
sudo nmtui
```

2. Select Edit a connection.
3. Select the management Interface (typically the first interface, for example, nic0 or eth0).

> Caution: Do not configure the second interface (often nic1). This is the SPAN or mirror port for passive monitoring and does not require an IP address.

4. Set IPv4 Configuration to `<Manual>`.
5. Select `<Show>` and enter the following:
    - Addresses: Your Static IP or CIDR (for example, 192.168.1.50/24)
    - Gateway: Your gateway IP address.
    - DNS Servers: Your DNS IP addresses.

6. Navigate to the bottom and select `<OK>` to save.
7. Select `Quit`.

Access the User Interface

After you configure the IP, do the following:

1. Connect a network cable from the Management port to your network switch.
2. Open a browser and navigate to the IP address via port 8000: `https://<YOUR_STATIC_IP>:8000`

   OT Security login page appears. You can now proceed with the Setup wizard. See Configure OT Security Settings using Setup Wizard .

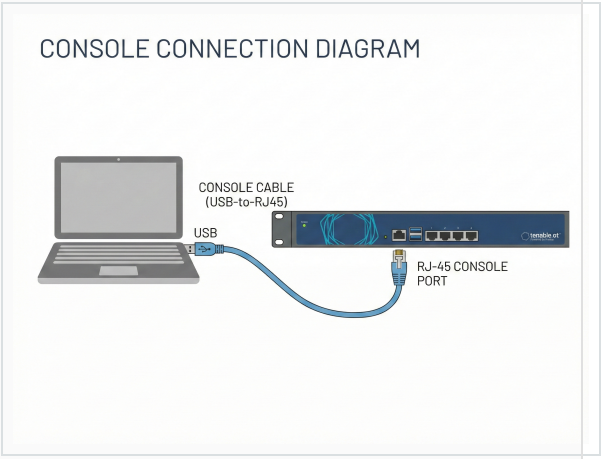
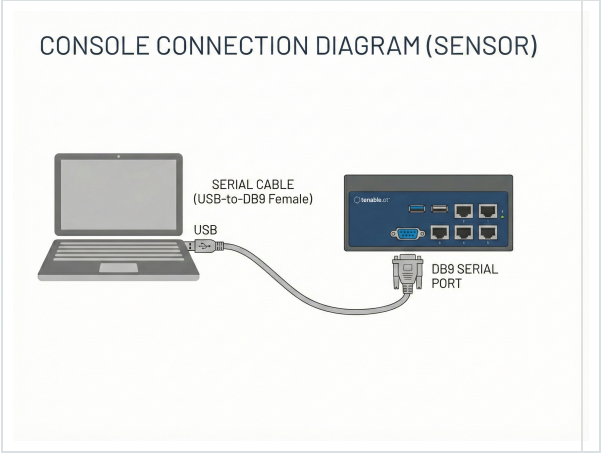
See also

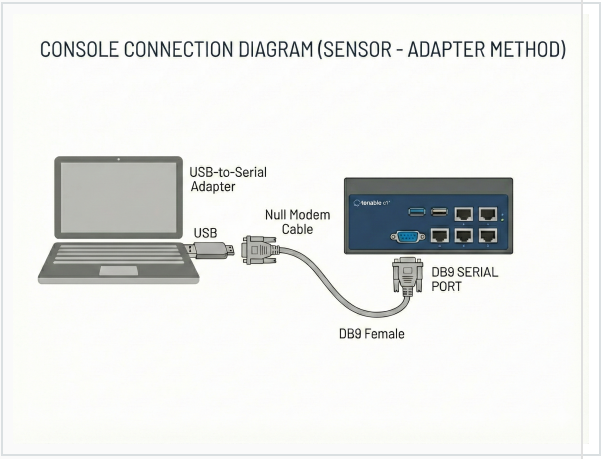
Console Cables to Connect to OT Security Sensor

Console Cables to Connect to OT Security Sensor

You can use the following cables to connect your laptop to OT Security Sensor:

Cable	Image	Console Connection Diagram

Console cable (USB-to-RJ45)		
Serial cable (USB-to-DB9 Female)		

Null Modem cable		

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-2024-03-11T135648.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)
```

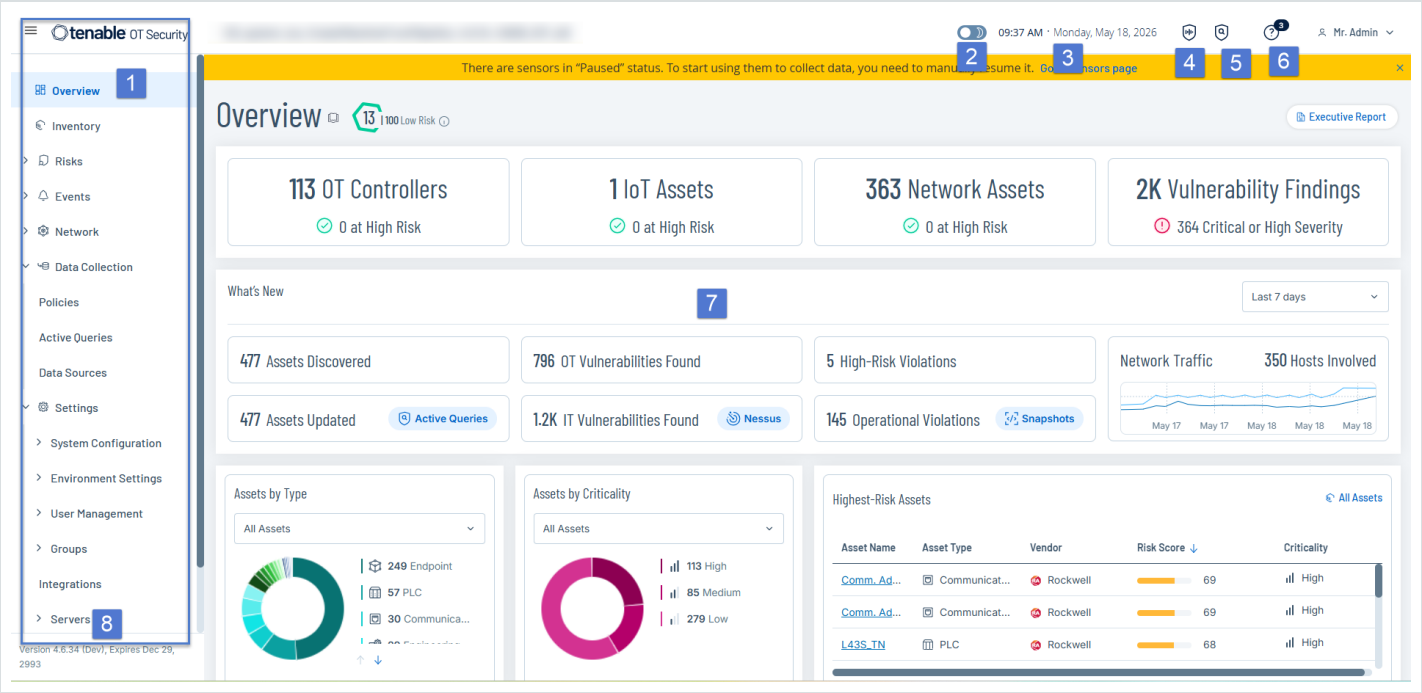
Where: `/home/admin/my-tc-ot-backup.tar` is the location of the backup files.

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.

Sl.No	User interfaceElement	Description
1	Main Navigation	Main navigation menu. Click the ☰ icon to show/hide the main navigation menu.
2	Dark Mode/Daylight Mode	Changes the display color scheme to Dark mode or Daylight mode.
3	Current Date and Time	Shows the current date and time as registered in the system.
4	Passive Monitoring	Indicates whether passive monitoring is enabled or disabled.

4	Active Queries	Indicates whether Active Queries is enabled or disabled.
5	Resource Center	OT Security resource center. Click to access help resources, new feature updates, and provide feedback.
6	Current User Name	Shows the name of the user who is currently logged into the system. Click the down arrow for menu options: 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.
7	License Info	Shows the OT Security software version and the license expiration date.
8	Main Screen	Shows the screen that you select in the main navigation.

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.

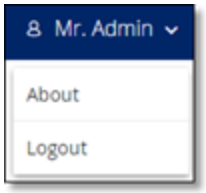
Check Current Software Version

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

To view the current software version:

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

OT Security displays the user menu.



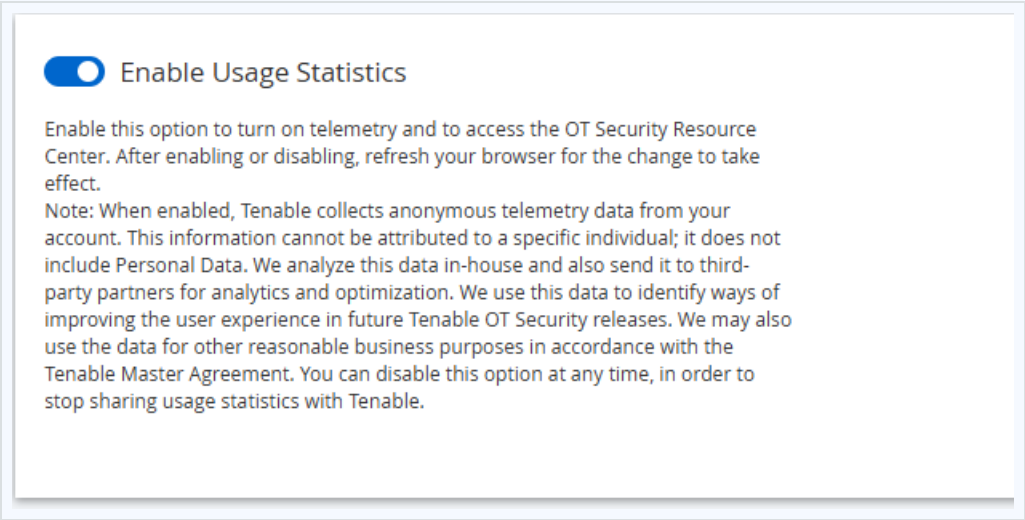
2. Click About.

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. The Resource Center ⓘ is disabled by default. To enable Resource Center, go to Settings > System Configuration > Device, and click to enable the Enable Usage Statistics toggle.



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:

- Overview – Shows widgets that give a general view of your network's inventory and security posture. This section provides a localized snapshot of your network's total asset footprint, top vulnerabilities, and critical security alerts. See OT Security Overview.
- Inventory – Shows an inventory of all the discovered assets, allowing comprehensive asset management, status monitoring of each asset, and viewing of their related events. The All Assets includes separate screens for specific type of assets: Controllers and Modules, Network Assets, and IoT. See Inventory.
- Risks – Shows all network threats detected by OT Security, including CVEs, vulnerable protocols, vulnerable open ports and more, along with recommended remediation steps. See Vulnerabilities.
- Events – Shows all events that occurred as a result of policy violations. The All Events page has with separate screens for each specific type of event. For example: Configuration Events, SCADA Events, Network Threats, or Network Events. See Events.
- Data Collection - This section includes the following configuration pages:
    - Policies – The administrative control plane for threat rules. View, edit, and activate policies in the system. See Policies.
    - Active Queries – Allows you to configure and enable active queries. See Manage Active Queries.
    - Data Sources – Configure sensors, agents, and IoT Connectors. Manually upload assets, SCD files, Rockwell Project Files, and PCAP files. See Data Sources.
- Active Queries – Allows you to configure and enable active queries. See Manage Active Queries.
- 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 the network 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.
- Network Map – Shows a visual representation of the network assets and their connections. See Network Map.

- Settings - View and configure the system settings. See Settings.
  - Groups – View, create and edit groups used in policy configuration. See Groups.

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.

Important: In version 4.0 and later, OT Security introduces several UI changes, but not all pages in the application are updated. In this version, only the pages under Inventory and Vulnerability Findings use the improved method to customize, filter, sort, and search. These steps are documented in sections with headings marked specifically for 4.0. For example: Customize the Column Display in OT Security 4.0 and later.

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. For OT Security 4.0 and later, click Displayed Columns > Reset to Default.

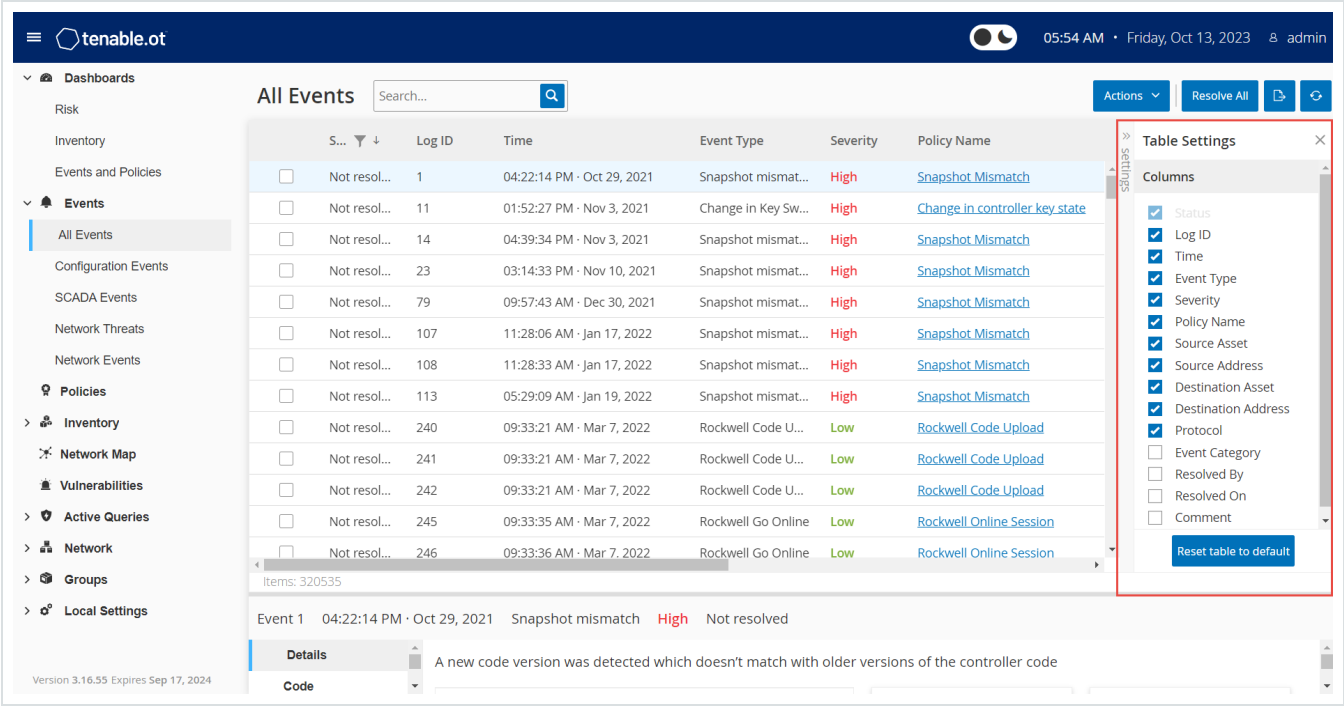
Customize the Column Display (3.19 and earlier)

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.



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.

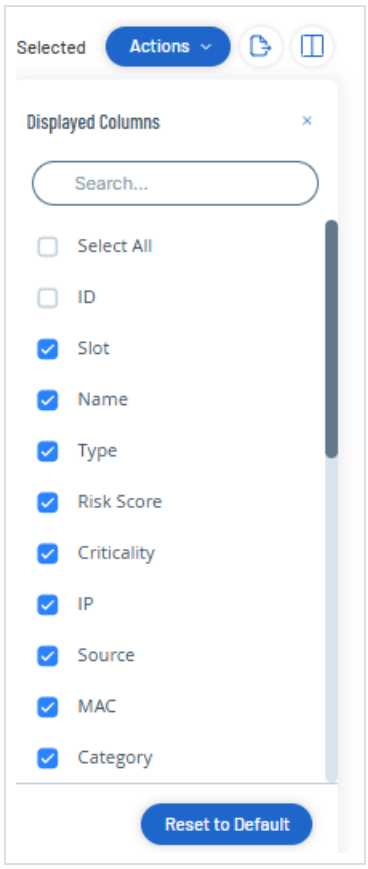
To adjust the order of display of the columns:

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

Customize the Column Display (4.0 and later)

1. In the header bar, click the button.

   The Displayed Columns panel appears.



2. Select the checkboxes next to columns you want to show.

   Note: Clear the checkboxes next to columns you want to hide.

   Tip: Use the Search box to search for specific columns.

3. Click the button to close the Displayed Columns panel.

   OT Security displays only the selected columns.

Group Lists by Categories (3.19 and earlier)

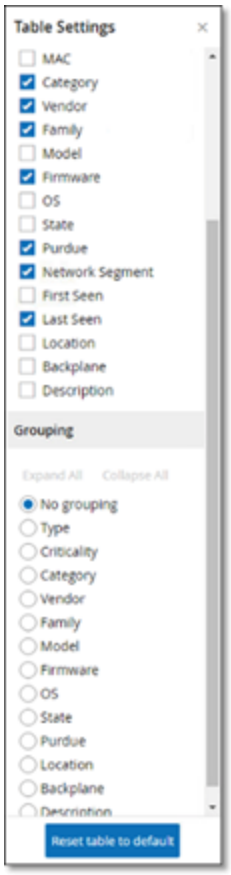
For the Inventory pages, you can group the lists by various parameters that are relevant to that particular screen.

To group the lists:

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

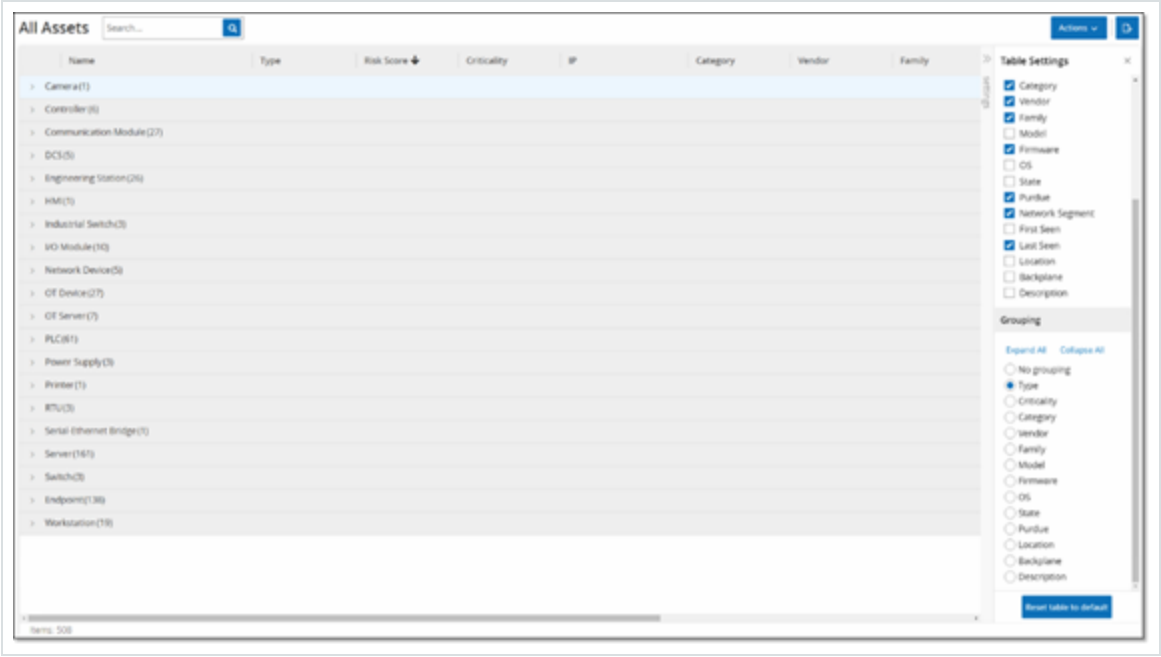
   The Table Settings pane appears on the right with the Columns and Grouping sections.

2. Scroll down to the Grouping section.



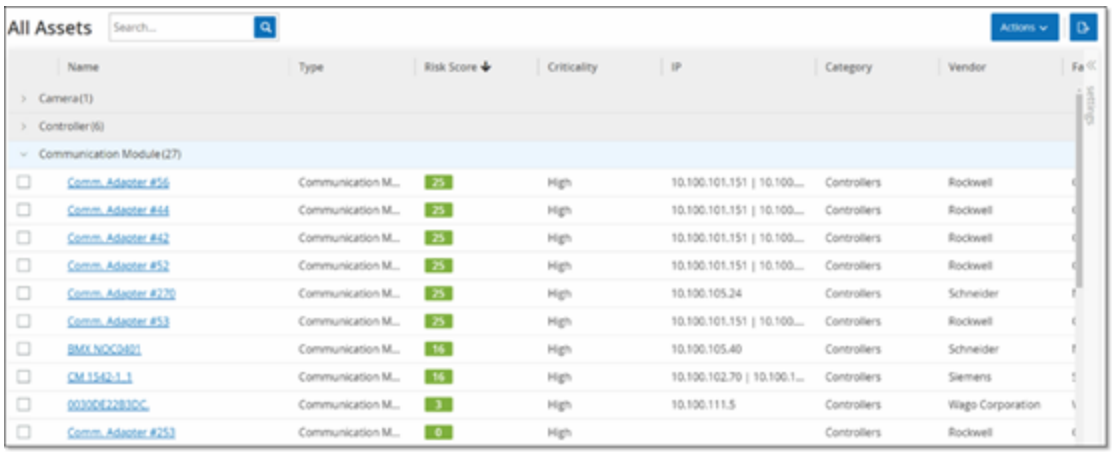
3. Select the parameter by which you want to group the lists. For example, Type.

   OT Security displays the grouped categories.



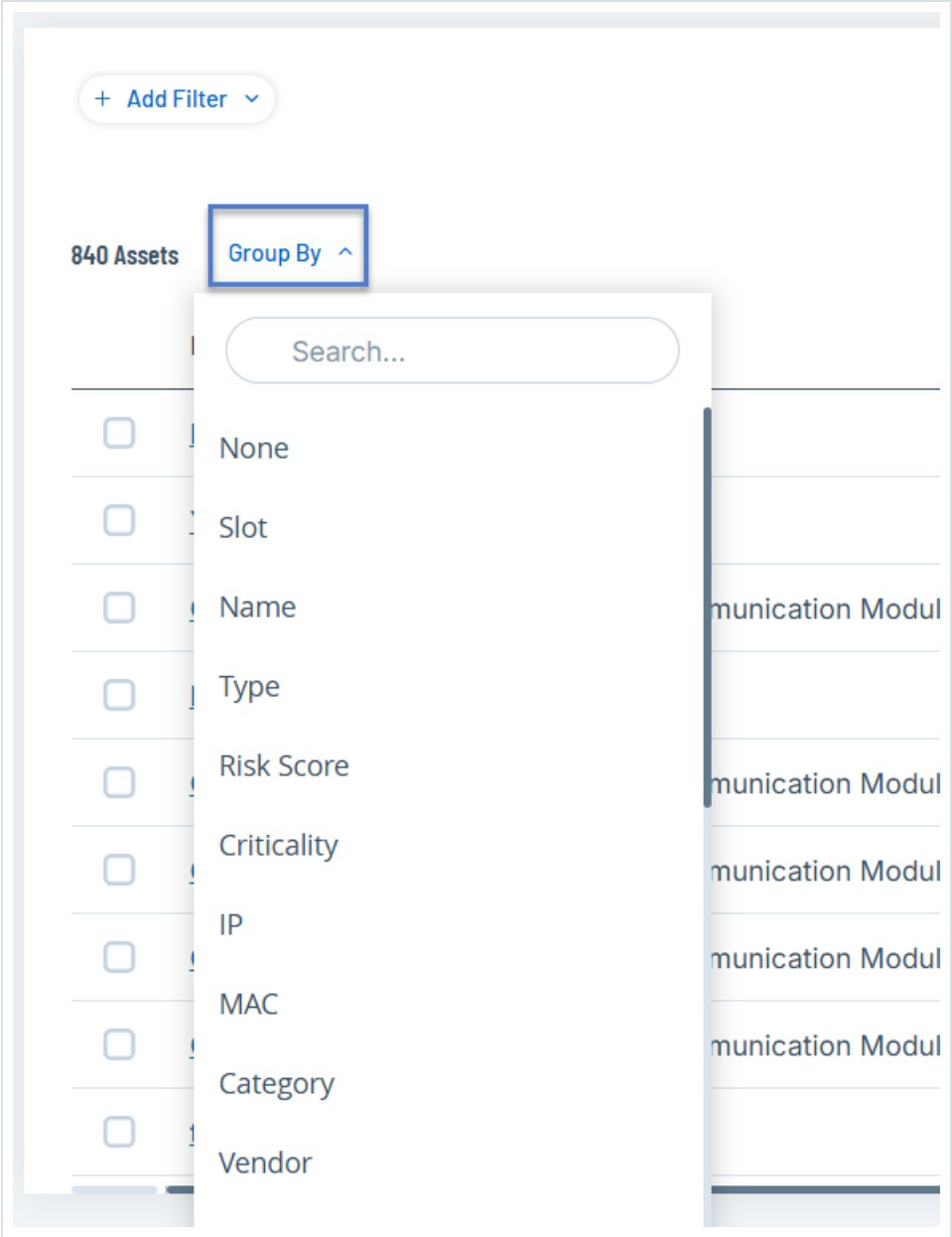
4. To close the Table Settings window, click x or the Settings tab.

5. Click on the arrow next to a category to show all instances for that category.



Group Lists By Categories (4.0 and later)

1. In the table header, click the Group By drop-down list.



2. Select the parameter to use to group the list. For example: Name.

> Tip: Use the Search box to search for a specific parameter.

OT Security groups the list by the selected parameter.

> Note: Use the Expand All or Collapse All buttons to expand or collapse the list respectively.

Sort Columns

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 again to reverse the display order (that is, A→Z, Z→A).

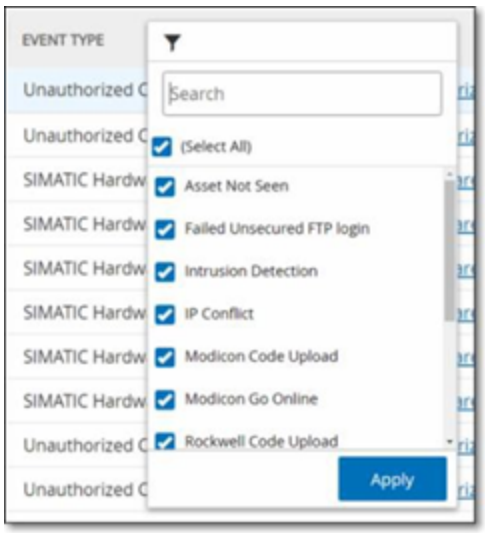
Filter Columns (3.19 and earlier)

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 page offers a selection of relevant filters. For example, in the Controllers Inventory window, you can filter by Name, Addresses, Type, Backplane, and Vendor.

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 to display and clear the checkboxes for those 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.

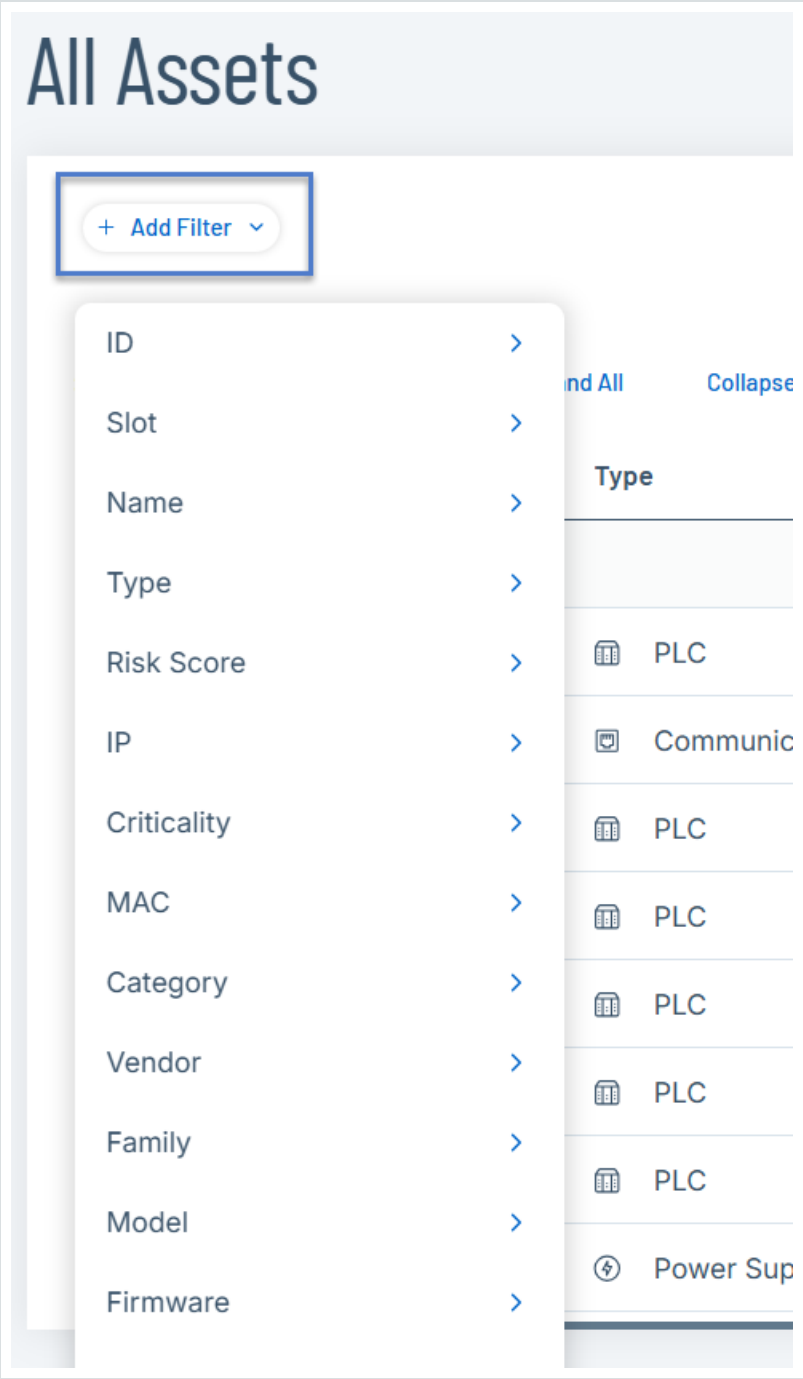
To remove the filters:

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

Filter Columns (4.0 and later)

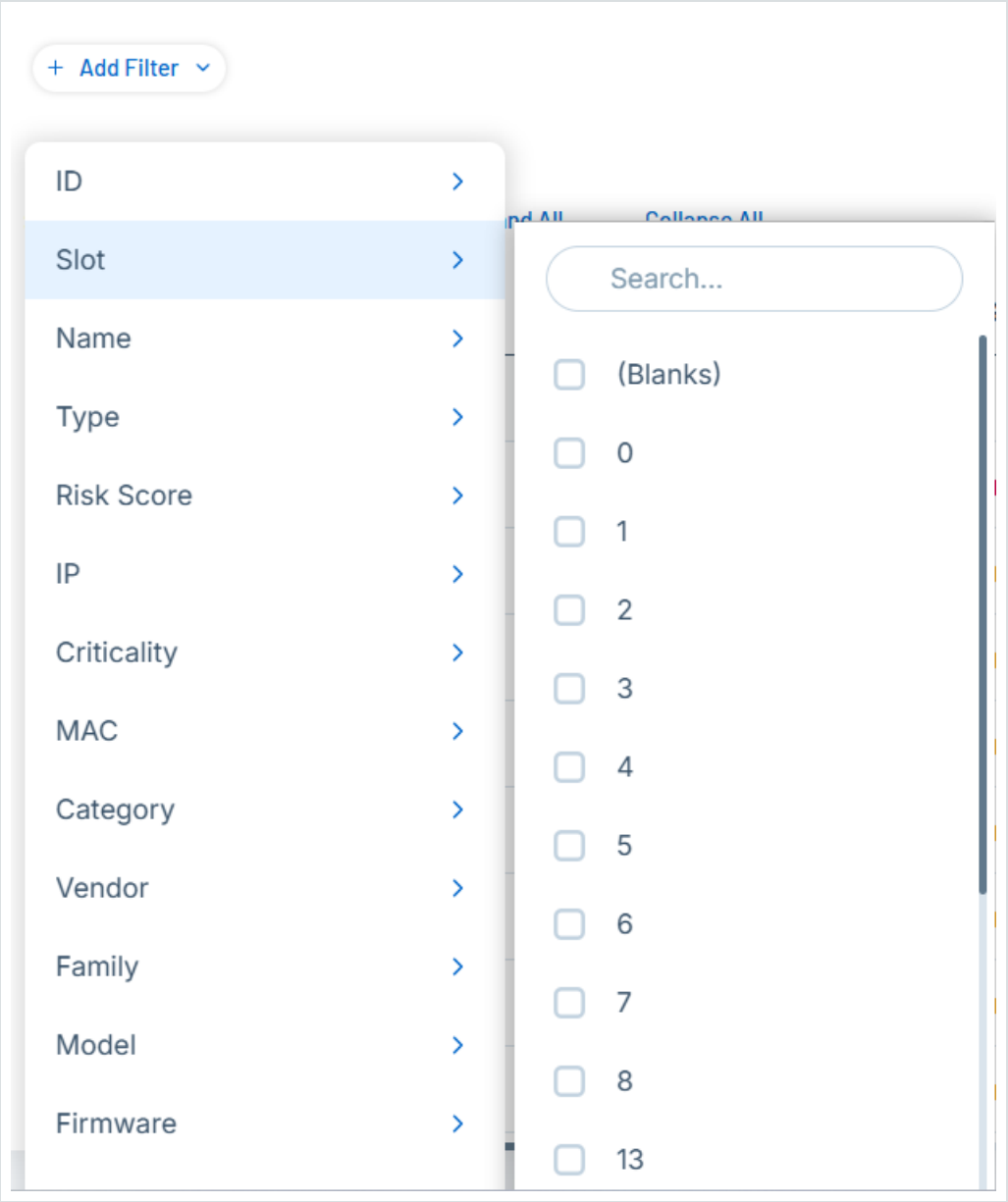
1. In the table header, click the Add Filter drop-down list.

   A drop-down menu appears with available filter elements.



2. Select the element you want to filter by.

   A list of filter options appears.

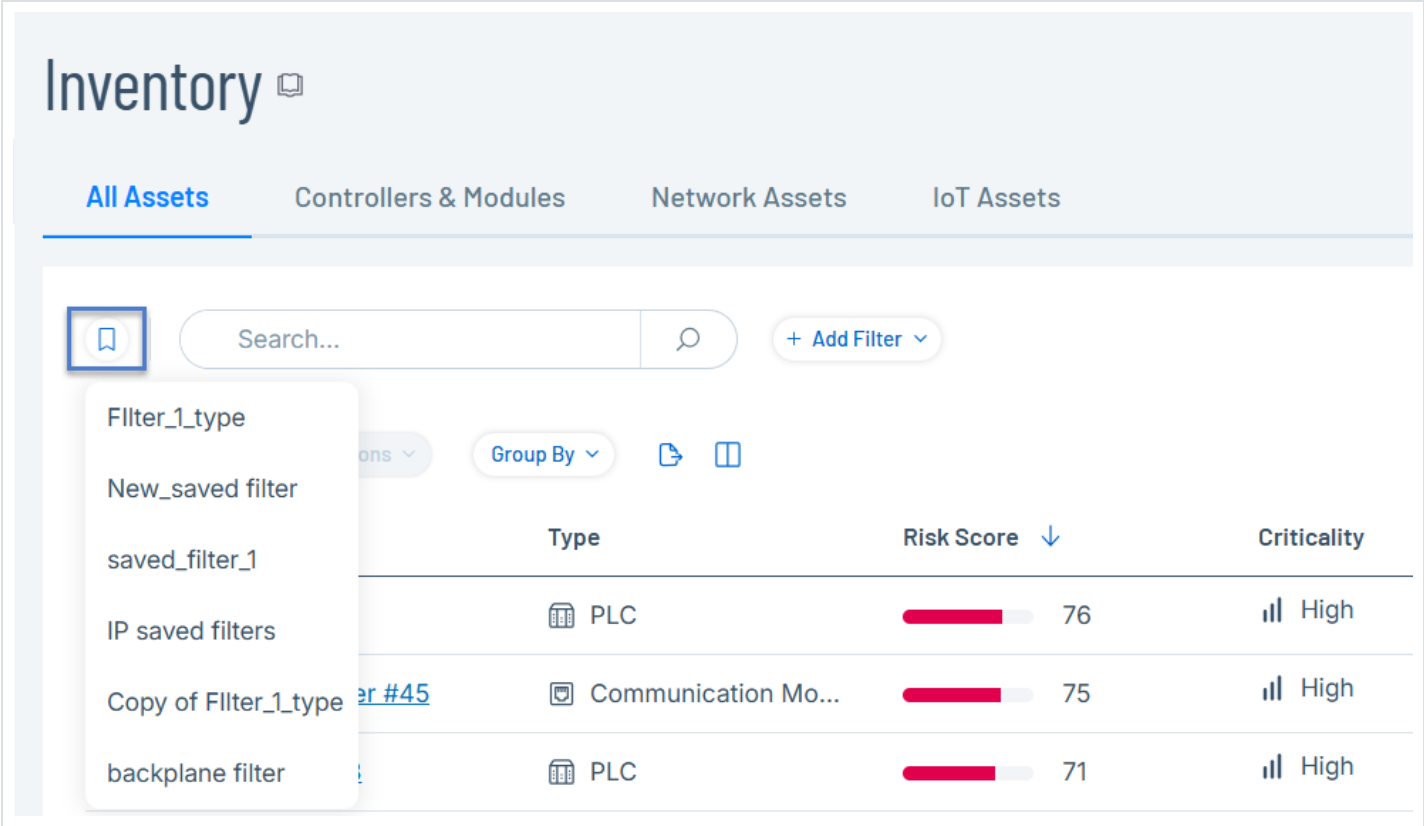


3. Select the checkboxes next to the options you want to filter.

> Tip: Use the Search box to search for specific filter options.

Save a Filter

You can save the filters that you use frequently and access them from Saved Filters as needed. This allows you to save and quickly return to your specific filtered views.



Note: The Save Filter functionality is available on the Inventory, Findings > Vulnerabilities, and Findings > Policy Violations pages.

To save a frequently used filter:

1. In the table header, click the + Add Filter drop-down list.

   A drop-down menu appears with available filter elements.

2. Select the required filter elements.

3. Click Apply Filter.

   OT Security displays the filtered results.

4. To save the filter, click Save Filter.

   The Save Filter panel appears.

5. In the Name box, type a name for the filter.
6. Click Save.

   OT Security saves the filter.
7. To access the saved filters, click the button.

   The list of saved filters appears.
8. Click the required filter and view the filtered results.

Modify Saved Filters

You can make changes to existing saved filters.

To make changes to an existing saved filter:

1. In the table header, click the click the button.

   The list of saved filters appears.
2. Click an existing saved filter you want to modify.
3. Add or remove filter elements as required.
4. Click Save Filter and select Save Changes.

   OT Security saves the changes to the filter.

Create a Copy of the Saved Filter

You can create a duplicate of the saved filter and save it as a new filter.

To duplicate a saved filter and save it under a new name:

1. In the table header, click the click the button.

   The list of saved filters appears.

2. Click an existing saved filter you want to copy.
3. Click Save Filter and select Save as Copy.

   The Save Filter panel appears.
4. In the Name box, change the filter name.
5. Click Save.

   OT Security saves the filter.

Remove All Filters

To clear all applied filters and return the table to its original, unfiltered state:

- In the table header, click Remove All Filters.

View Saved Filters

You can view your saved filters using two methods:

- From any page where saved filters are enabled, select the Saved Filters icon. See Save a Filter.

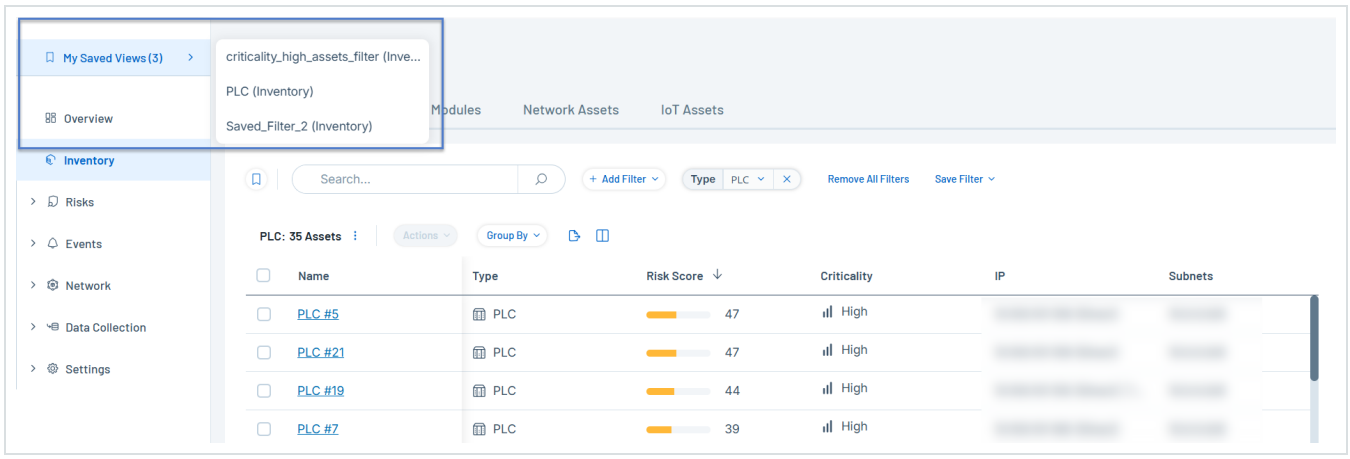
  > Note: Saved filters are currently enabled only for Inventory, Vulnerability findings, and Policy Violation findings pages.

- From any page, select My Saved Views in the left navigation menu.

To view all your saved filters from any page:

1. On the left navigation menu, click My Saved Views or select the Saved Filters icon from the Inventory page.

   A list of saved filters appear.



2. Click any filter name.

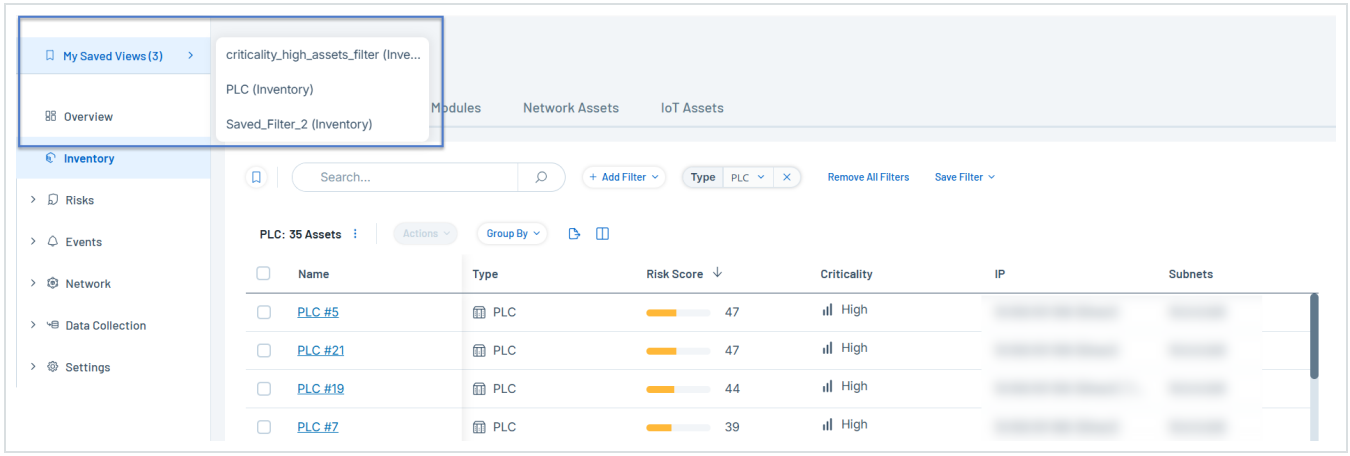
   OT Security displays the Inventory page with the filtered assets view.

Edit the Saved Filter Name

To modify the filter name:

1. On the left navigation menu, click My Saved Views or select the Saved Filters icon from the Inventory page.

   A list of saved filters appear.

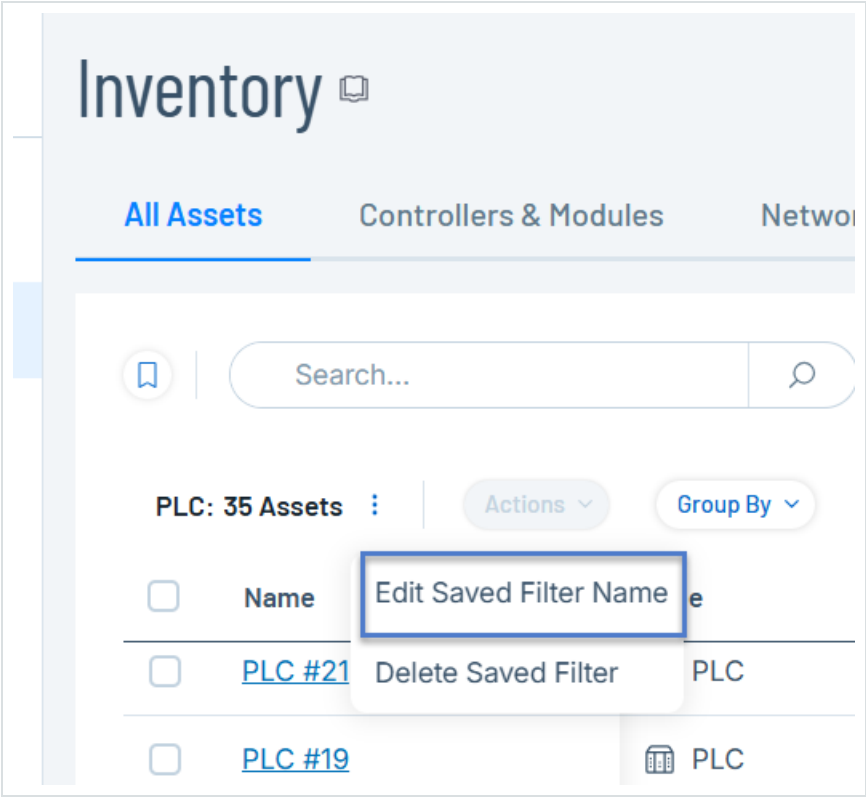


2. Click the filter name you want to modify.

OT Security displays the Inventory page with the filtered assets view.

3. Click the More options ⋮ button next to the filter name.

   A menu appears.



4. Select Edit Saved Filter Name.

   The Edit Saved Filter panel appears.

5. Modify the name as needed.

6. Click Save.

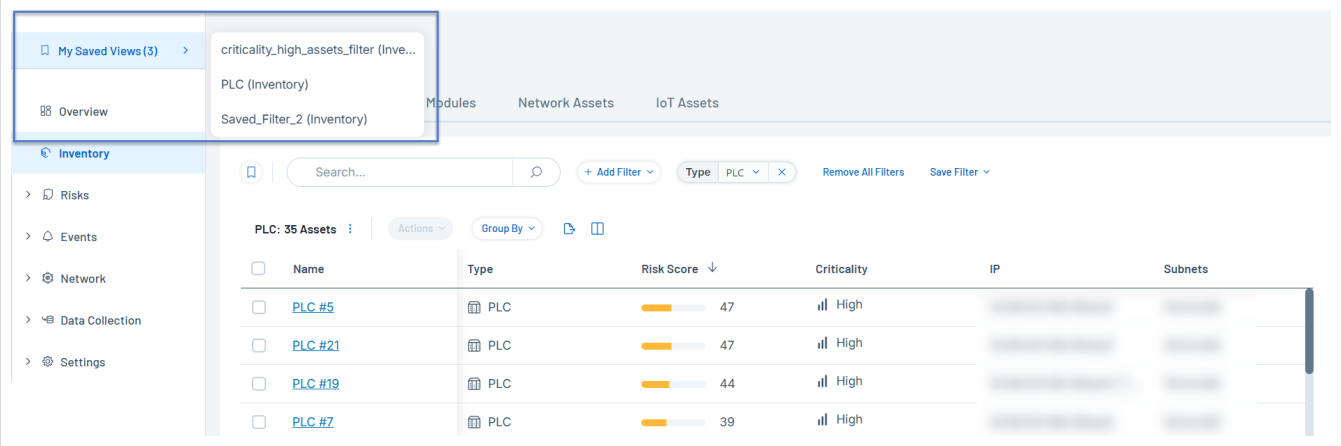
   OT Security saves the modified filter name. To modify filter details, for instance, add or remove filters, see Modify Saved Filters.

Delete a Saved Filter

To delete filters:

1. On the left navigation menu, click My Saved Views or select the Saved Filters icon from the Inventory page.

   A list of saved filters appear.

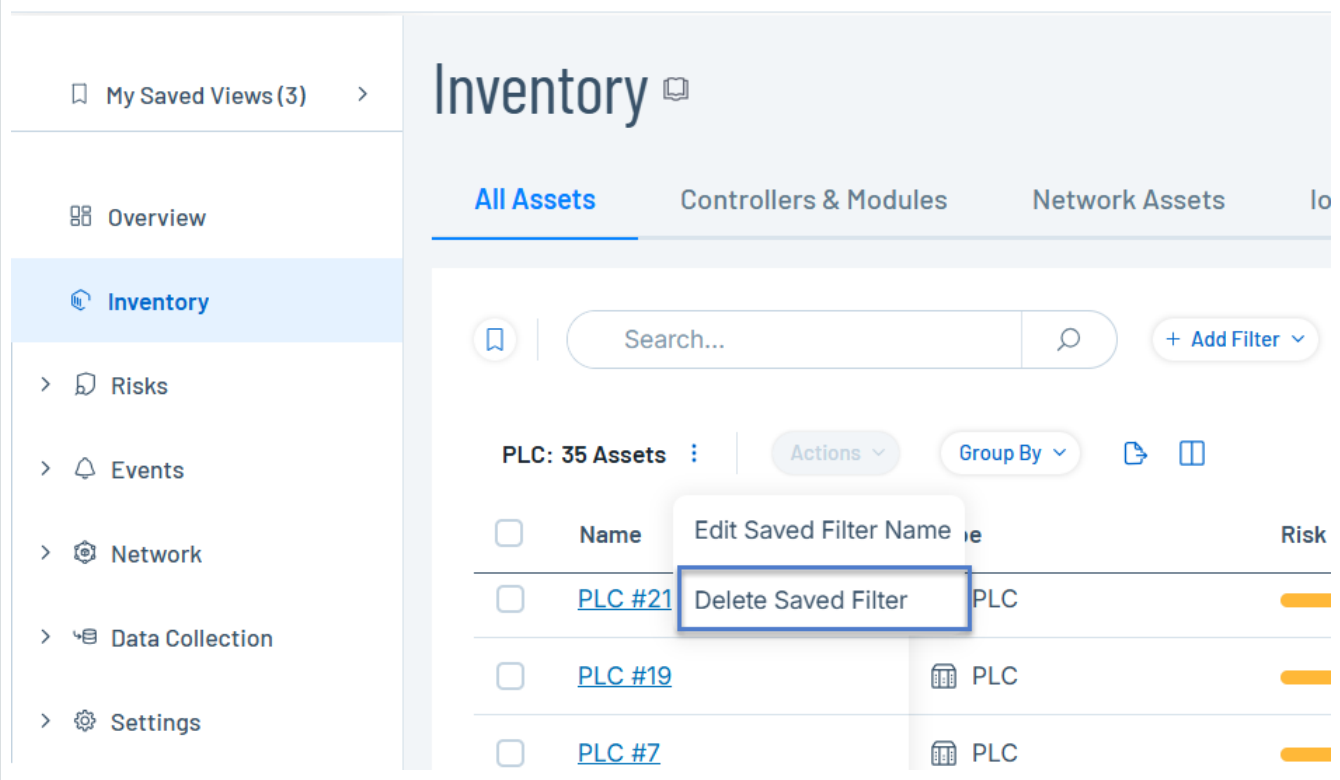


2. Click the filter you want to delete.

   OT Security displays the Inventory page with the filtered assets view.

3. Click the More options ⋮ button next to the filter name.

   A menu appears.



4. Select Delete Saved Filter Name.

   OT Security deletes the filter.

Search (3.19 and earlier)

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.

Search (4.0 and later)

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 button.

Export Data

You can export data from any of the lists shown in the OT Security UI (For example: Events, and Inventory.) 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:

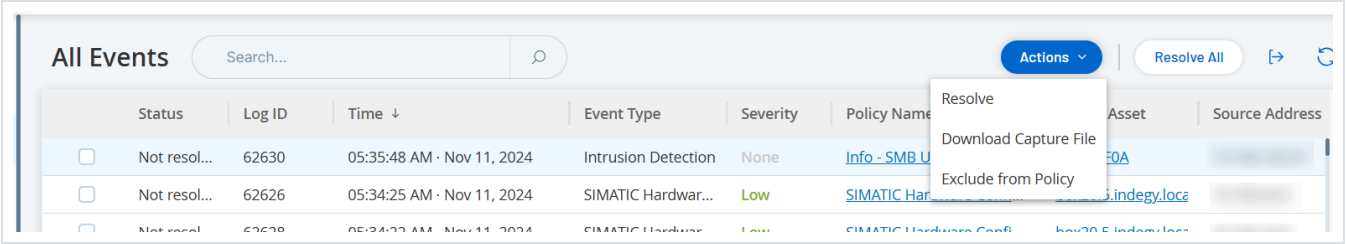
1. Go to the page for which you want to export data.
2. In the header bar, click the button.

   OT Security downloads a CSV format of the data.

Actions Menu

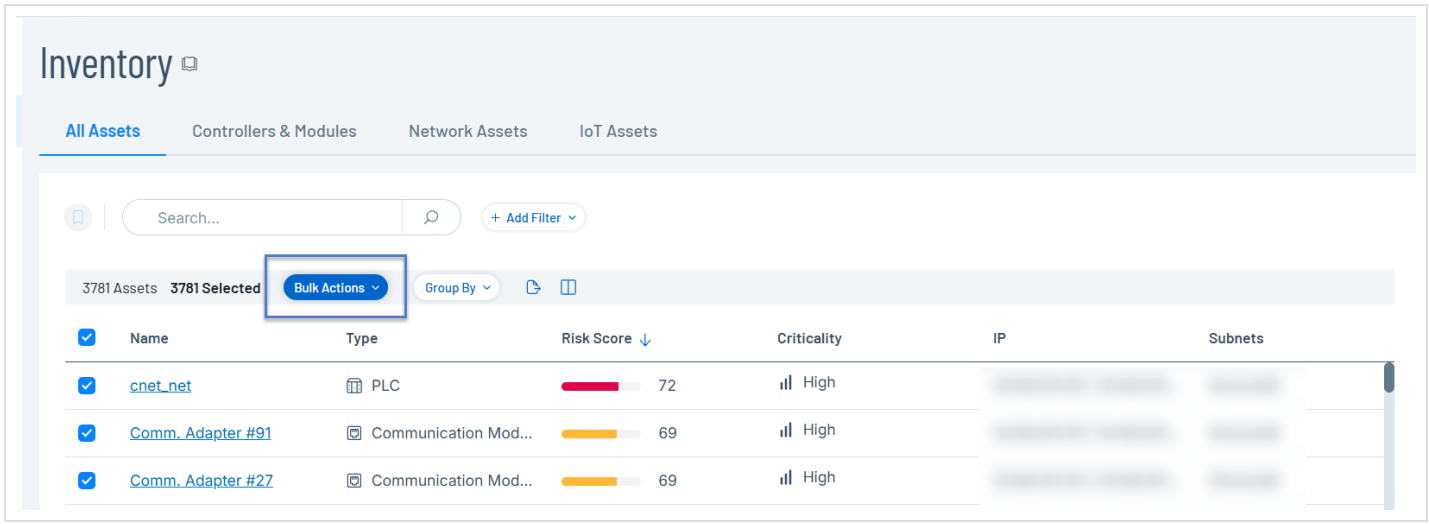
Each screen has a series of actions that you can take for the elements on the screen. For example, in the Policies screen, you can **View**, **Edit**, **Duplicate** or **Delete** a Policy. In the Events screen, you can **Resolve** or **Download Capture File** for an event.

To access the Actions menu:

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

Bulk Actions

When you select multiple elements on a page, OT Security enables the Bulk Actions option in the header.



OT Security Overview

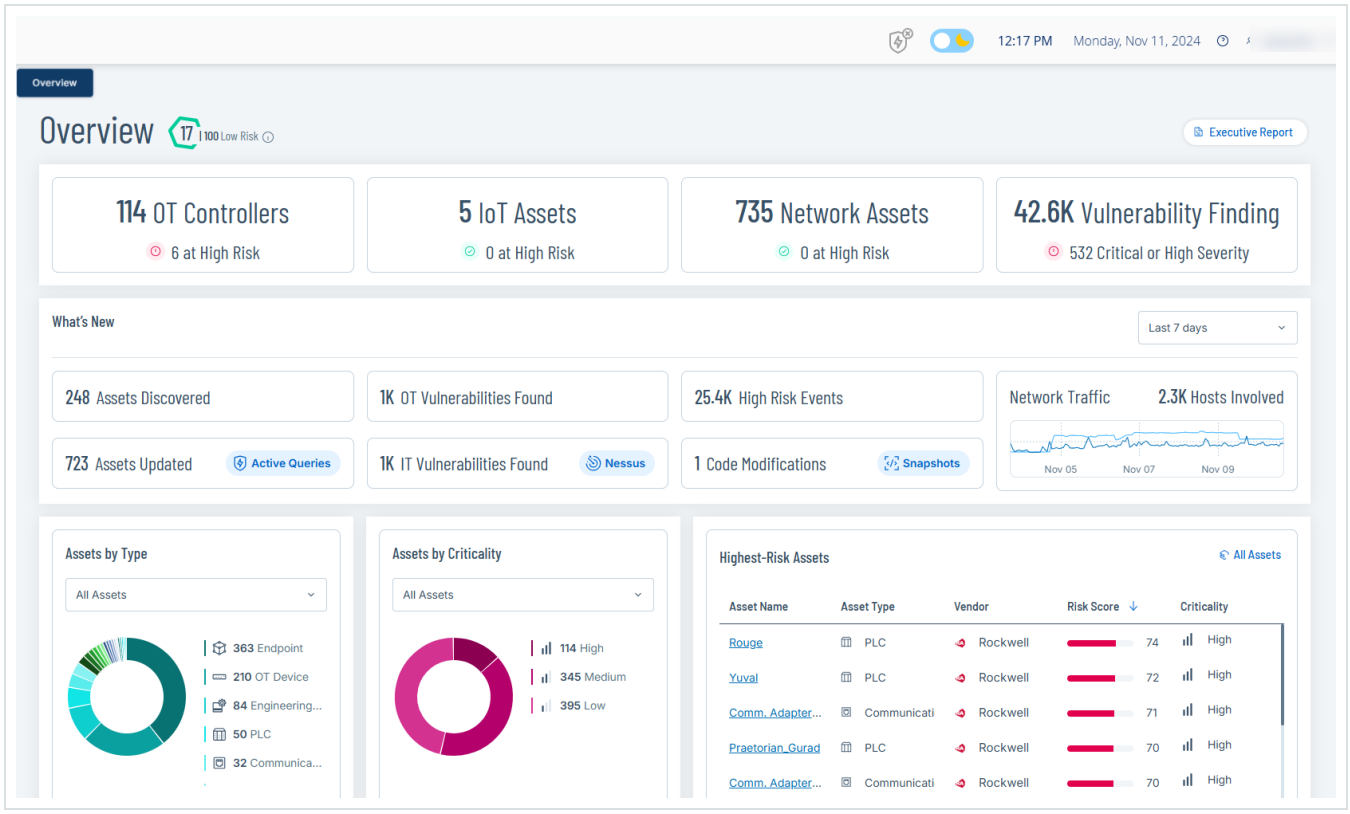
Use the Overview page to view key insights of your OT environment through interactive widgets. The widgets on this page provide real-time insights into your environment such as:

- Information about your environment's security posture.
- A summary of what recently changed since your last login.
- A breakdown of the different types of assets in your inventory.
- The current state of assets and vulnerabilities.
- Assets that pose the highest risk.
- Timestamp of your last code revision.

To access the Overview page:

1. In the left navigation bar, click Overview.

   The Overview page appears.



The Overview page includes the following widgets:

Widget	Description
Risk Score	The Average Risk Score is the average of all asset scores in your environment. To view a breakdown of the score, hover over the value. The Average Risk Score uses the following color codes to indicate the severity of the risk: • Low (Green):0–29 • Medium (Yellow): 30–69 • High (Red): 70–100

	OT Security calculates the asset scores based on the following factors that changes with time (decaying events, firmware, and state changes): • Criticality - Based on the asset type and purdue level. For example, a PLC controls production, so it is considered critical, whereas a camera is typically less critical. • Vulnerabilities - Based on the Vulnerability Priority Rating (VPR) asset. • Events - Based on the events associated with the asset. Policies trigger events and each policy defines a severity. The severity is calculated based on the number of events, their severity, and how long they existed. Older events affect the score less than recent events. • Backplane - An asset that resides on a backplace affects the scores of its neighbor assets. For example, if one module is vulnerable, the entire backplane is also vulnerable.
Assets and Vulnerabilities	The current state of assets and vulnerabilities in your environment. Includes separate widgets for each asset type (OT Controllers, Network Assets, IoT Assets) that show the number of assets in that category and the number of assets that are at high risk. Note: Assets with a risk score of 70 and above are considered to be at high risk.
What's New	A summary of changes since your last login such as new assets, vulnerabilities, and high risk events. Drill-down to open the respective assets, events, or vulnerabilities page to view the filtered assets, vulnerabilities, or events.

	A summary of changes since your last login, such as new assets, vulnerabilities, high risk violations, and operational violations. Drill-down to open the respective assets, Findings, or Vulnerabilities page to view the filtered assets, vulnerabilities, or events. Use the filter drop-down to filter the results by Last 1 day, Last 7 days (default), or Last 30 days.
Assets by Type	The number of assets by type, such as endpoint, PLC, and OT device.
Assets by Criticality	The number of assets by their criticality: High, Medium, or Low.
Highest Risk Assets	Lists all high risk assets with details such as asset name, type, vendor, risk score, and criticality. To go to the All Assets page: in the upper-right corner, click the All Assets link.
Executive Report	Generates a risk assessment report of your OT environment. For more information, see Generate an Executive Report.

Generate an Executive Report

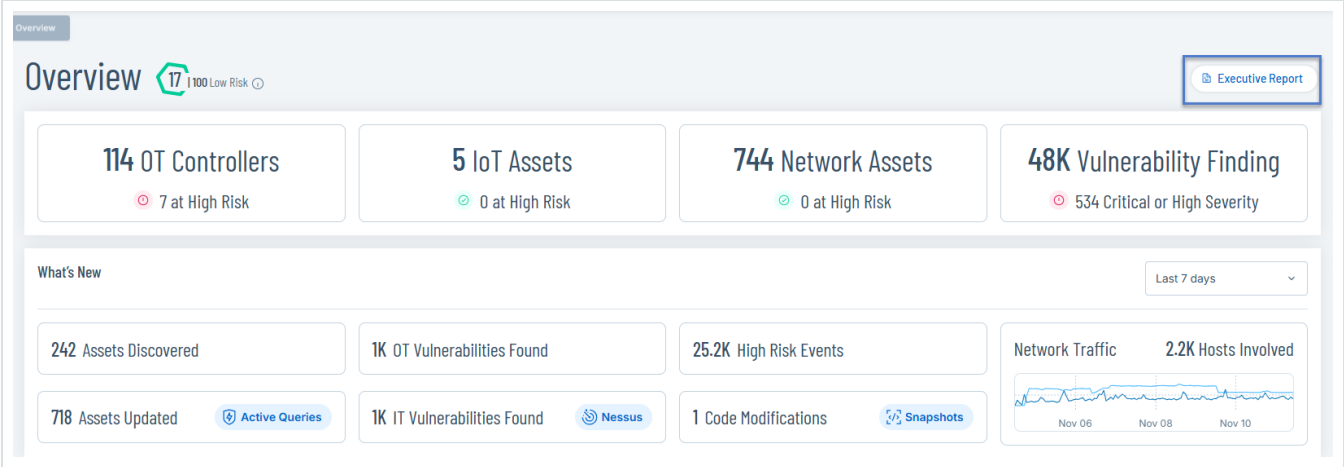
You can generate a risk assessment report for your environment based on the data from the last 30 days. OT Security uses key widgets from the Risk, Inventory, and Events and Policies dashboards to create a high-level graphical overview highlighting high risk assets, critical and common vulnerabilities,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

   The Overview page appears.



2. In the upper-right corner, click Executive Report.

   OT Security opens the report on your browser.

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

   The Print dialog box appears.

4. In the Destination drop-down box, select Save as PDF.

5. Browse to the location where you want to save the report.

6. Click Save.

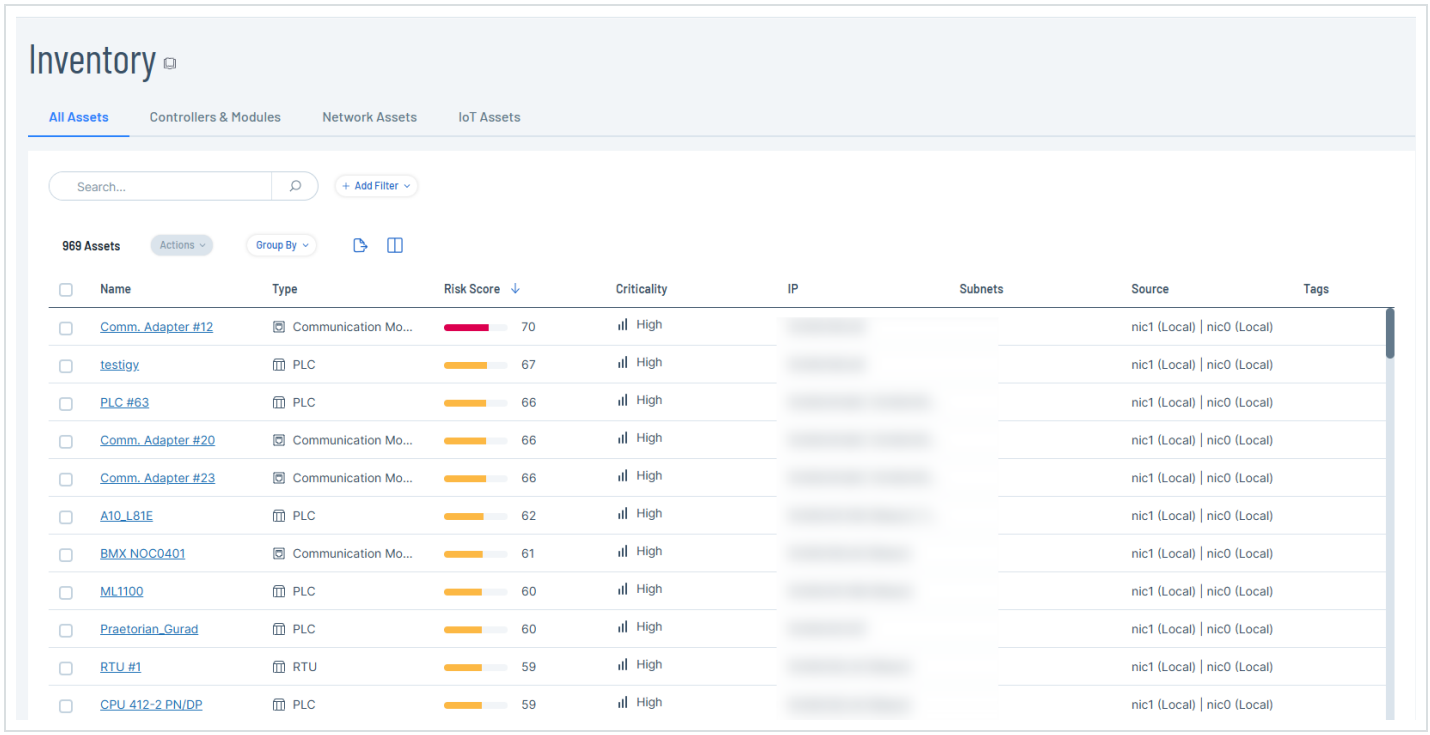
   OT Security saves the report in the PDF format.

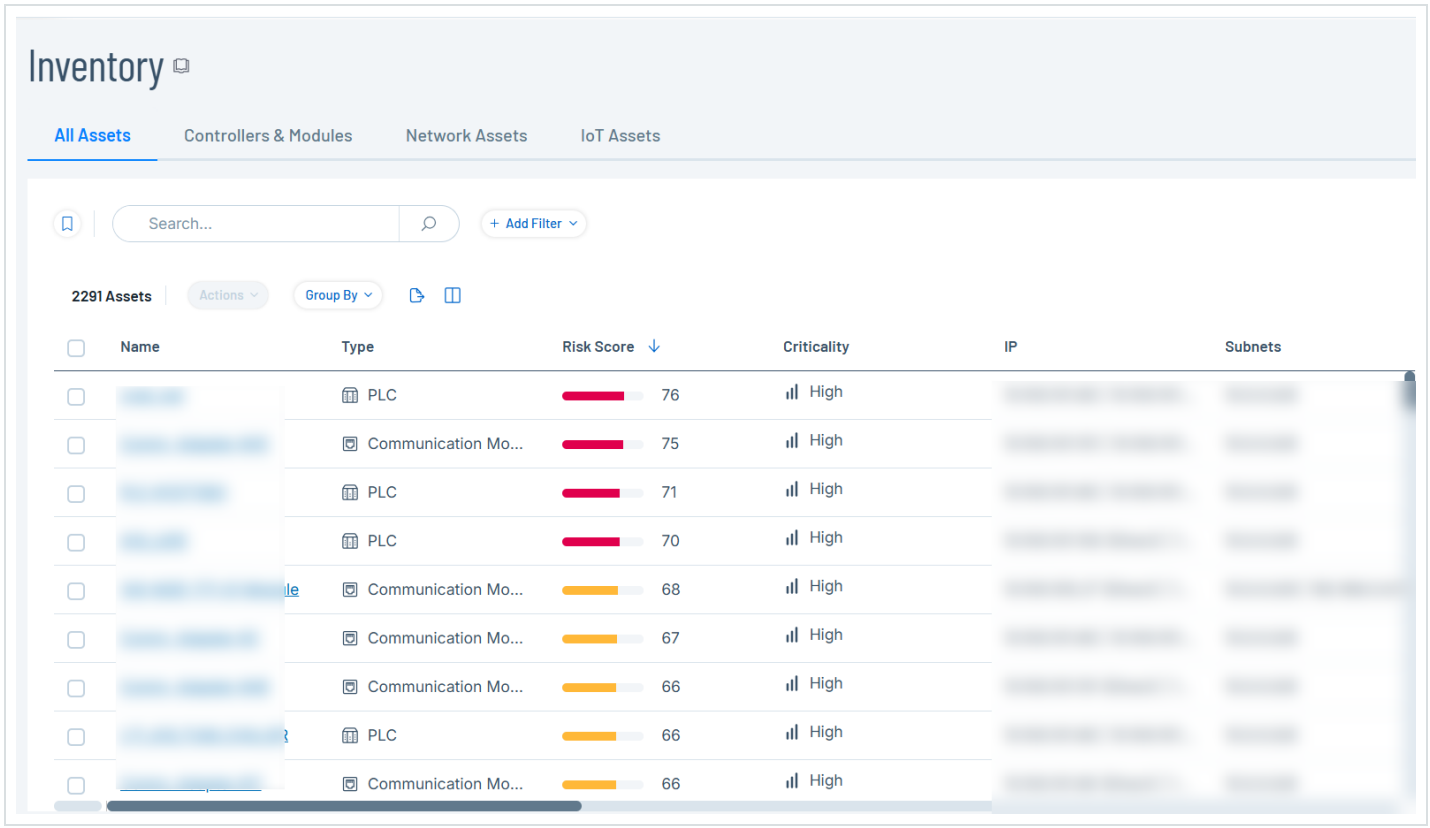
Inventory

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. > Note: An asset may have multiple IP addresses. > 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. > Note: Assets can be filtered by IP range. For more on filtering, see Management Console User Interface Elements.

Parameter	Description
Subnets	The subnets discovered by querying network devices through SNMP.
Source	The name of the source. For example, nic 1 or nic 2 for a local source or the sensor name if the source is a sensor.
MAC	The MAC address of the asset.
Tags	The tags you create for the asset in the Asset Groups & Tags page.
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 Edit Asset Details.
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.

Parameter	Description
Model Name	The model name of the asset.
State*	The device state. Possible values: • Backup – the controller is running as a backup to a primary controller. • Fault – the controller is in fault mode. • NoConfig – no configuration has been set for the controller. • Running – the controller is running. • Stopped – the controller is not running. • Unknown – the state is unknown.
Description	A brief description of the asset, as configured by the user in the OT Security asset details. See Edit Asset Details.
Risk	A measure of the degree of risk related to this asset on a scale from 0 (no risk) to 100 (extremely high risk). For an explanation of how the Risk score is calculated, see Risk Assessment.
Criticality	A measure of the importance of this asset to the proper functioning of the system. A value is assigned automatically to each asset based on the asset type. You can manually adjust the value.
Purdue Level	The Purdue level of the asset (0=Physical process, 1=Intelligent devices, 2=Control systems, 3=Manufacturing operations systems, 4=Business logistics systems).
Custom Field	You can create custom fields to tag your assets with relevant info. The custom field can be a link to an external resource.

Asset Types

The following table describes the various types of assets identified by 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

Category	Default Criticality Level / Purdue Level	Description	Sub-Types	
				I/O Module
				CNC
				PowerSupply
				BackplaneModule
Field Devices	High / 1	An industrial device (for example sensor, actuator, electric motor) that uses industrial protocols to send information to ICS systems.		FieldDevice
				PowerMeter
				RemoteI/O
				Relay
				Inverter

Category	Default Criticality Level / Purdue Level	Description	Sub-Types	
				
				IndustrialSensor
				Drive
				Actuator
OT Devices	Medium / 2	This category includes all types of OT devices.		OTDevice
				IndustrialRouter
				IndustrialSwitch
				IndustrialGateway

Category	Default Criticality Level / Purdue Level	Description	Sub-Types	
				
				IndustrialNetwork Device
				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

Category	Default Criticality Level / Purdue Level	Description	Sub-Types	
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

Category	Default Criticality Level / Purdue Level	Description	Sub-Types	
				
				WirelessAccess Point
				Firewall
				Converter
				Repeater
				Radio
Workstations	Low / 3	A computer that is connected to the network and used to control the PLCs. This category		Workstation

Category	Default Criticality Level / Purdue Level	Description	Sub-Types	
		includes all types of workstations and their related components.		
				OT Workstation
				EngineeringStation
				VirtualWorkstation
Servers	Low / 3	This category includes various types of IT servers.		Server
				FileServer
				WebServer

Category	Default Criticality Level / Purdue Level	Description	Sub-Types	
				

Category	Default Criticality Level / Purdue Level	Description	Sub-Types	
				VirtualServer
				SecurityAppliance
				TenableICP
				TenableEM
				TenableSensor
				Domain Controller
				IoT

Category	Default Criticality Level / Purdue Level	Description	Sub-Types	
IoTs	Low / 3	This category includes various type of interrelated devices.		Camera
				Panel
				Projector
				VOIPDevice
				3DPrinter
				Printer
				UPS

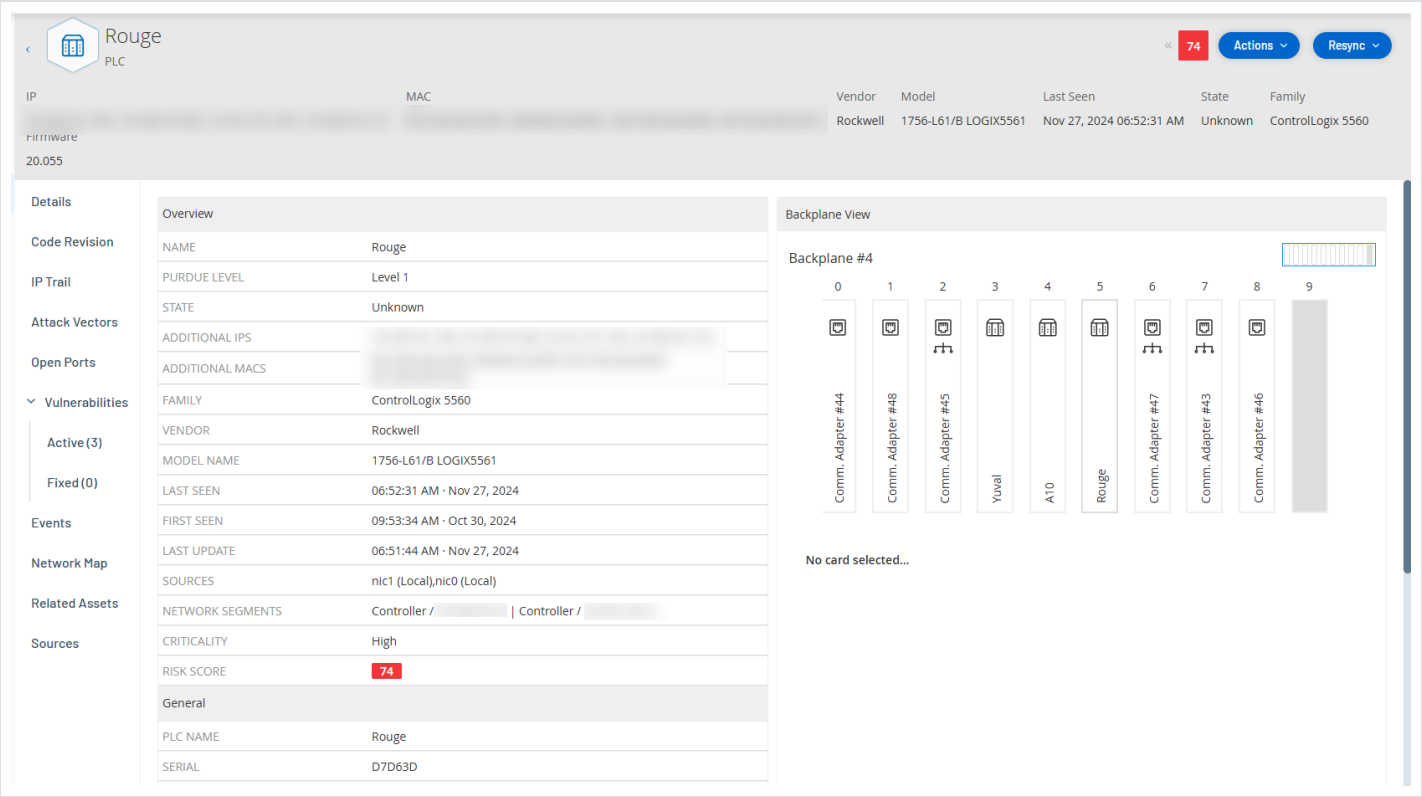
Category	Default Criticality Level / Purdue Level	Description	Sub-Types	
				IP Phone
				SmartSensor
				BarcodeScanner
				AccessControl System
				LightingControl
				HVACModule
				SmartHub

Category	Default Criticality Level / Purdue Level	Description	Sub-Types	
				SmartTV
				MedicalDevice
				Tablet
				MobileDevice
				StorageDevice
Endpoints	Low / 3	An unidentified IP address in the network.		Endpoint

View Asset Details

Required OT Security User Role: Administrator, Supervisor, Security Manager, Security Analyst, Site Operator, Read Only

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.

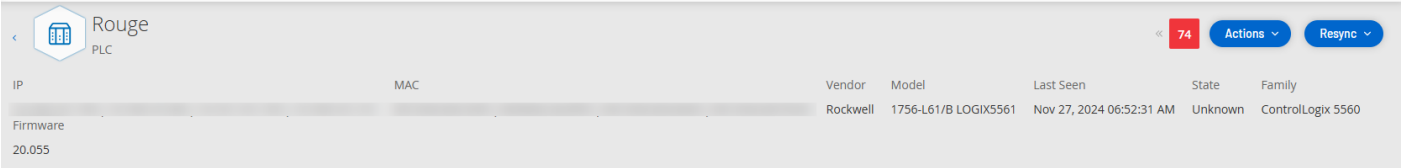
    - On the Inventory page, click Actions > View.

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 fixed and active 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.
- Related Assets – shows the list of all nested assets.
- Sources – shows all information related to the source of the asset such as the location, type, the IP and Mac addresses of the asset, and the first and last reported time.

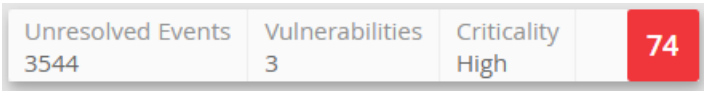
Header Pane

The Header Pane shows an overview of the current state of the asset.



The display includes the following elements:

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



- Actions menu – Allows you to edit the asset details or run a Tenable Nessus scan.
- Resync – Click to manually run one or more of the queries that are available for this asset. See Perform Resync.

Details

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. OT Security displays only the sections relevant to the specified asset. The following list includes all possible section categories for various asset types: Overview, General, Project, Memory, Ethernet, Profinet, OS, System, Hardware, Devices & Drives, USB Devices, Installed Software, IEC-61850, and Interface Status.

> Note: OT Security displays only those details that it extracts from the asset. Not all sections may appear for all the assets. For example, General, Nessus Scan Information.

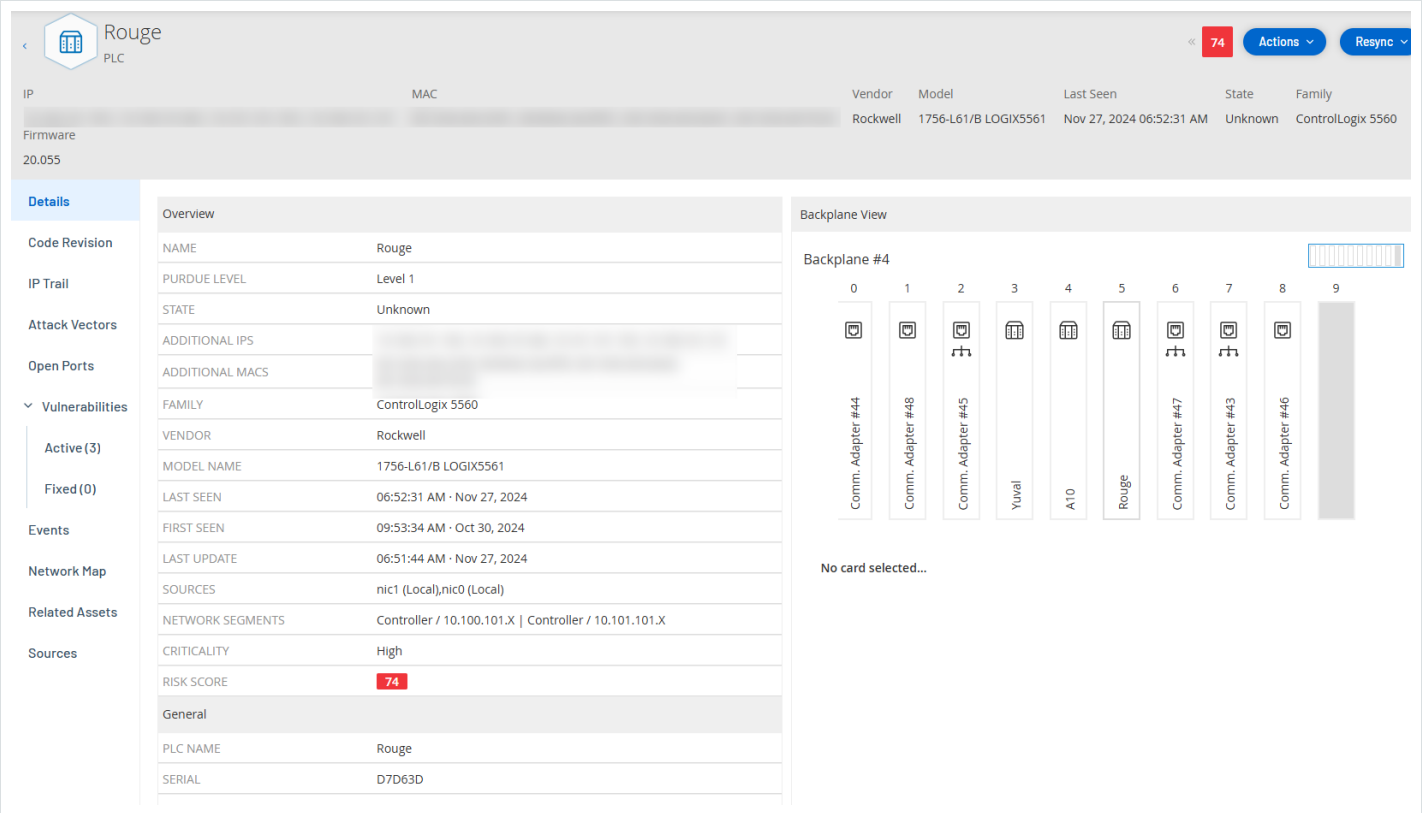
The following table shows the details in the Overview section:

Section	Description
Name	The asset name obtained either through passive monitoring or active query, or automatically generated using asset type and a unique identifier.
Description	The description of the asset from the user.
Purdue Level	The Purdue Model level assigned to the asset.
State	The current operational status of the asset. The field is relevant for specific asset types, typically controllers.
Direct IP	The IP address present on or configured for that specific asset or module.
Direct Mac	The Mac address physically present on or configured for that specific asset or module.
Additional IPs	IP addresses associated with other modules sharing a backplane or similar infrastructure with the asset used to access the asset indirectly. For example, a PLC (controller module) may lack its own network interface and is accessed via an IP address configured on a communication module

Section	Description
	installed in a different slot. Note that the asset may have connections other than a backplane.
Additional Macs	Mac addresses associated with other modules sharing a backplane or similar infrastructure used to access the asset indirectly.
Family	The device family or product line to which the asset belongs.
Vendor	The manufacturer or supplier of the asset.
Model Name	The specific model number of the asset.
Last Seen	The date and time when OT Security most recently detected the asset. OT Security may update this field when replaying a PCAP (traffic capture file) or performing a similar analysis.
First Seen	The date and time when the asset was initially detected, which may be the same as or earlier than the Last Seen value.
Last Update	The date and time or the most recent update of any of the asset's details. Note: Any manual change to the asset information, such as updating the description updates this value, whether or not the asset is currently active or recently detected.
Sources	The sources (such as sensors, PCAPs, local interfaces) identified or are associated with the asset.
Network Segments	The network segments assigned or associated with the asset.
Criticality	The importance of the asset assessed as High, Medium, or Low.

Section	Description
Risk Score	Reflects the potential impact of risk associated with the asset. The score is influenced by factors such as criticality, vulnerabilities, unresolved events (and their duration), related assets (for example, via backplane), and other relevant considerations.
Tags	The tags associated with the asset. See Asset Groups & Tags.

Backplane View



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.

Nessus Scan Information

The Nessus scan information helps you:

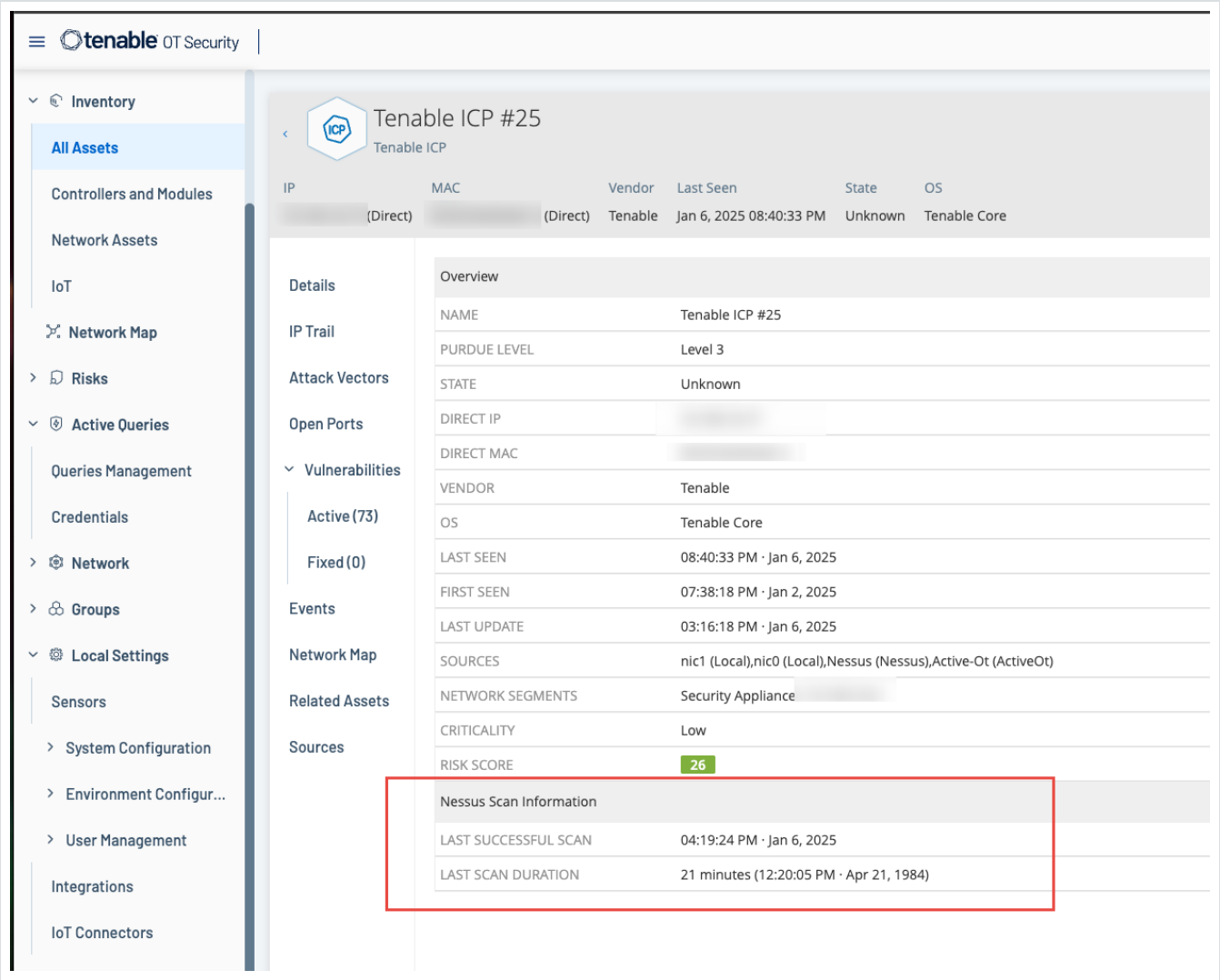
- Understand assessed and unassessed assets.
- Understand if your assets are targeted with credentialed or non-credentialed scans.
- Perform best practices with scanning and vulnerability management. For example, you can perform vulnerability assessment scans against IT type assets running Windows, Linux. Scanning, whether with or without credentials, helps assess how much of your organization's attack surface is exposed both internally and externally.

For more information about Nessus Scans, see Create Nessus Plugin Scans .

The Nessus Scan Information section on the Details page provides the following details:

- Last Successful Scan
- Last Authenticated Scan

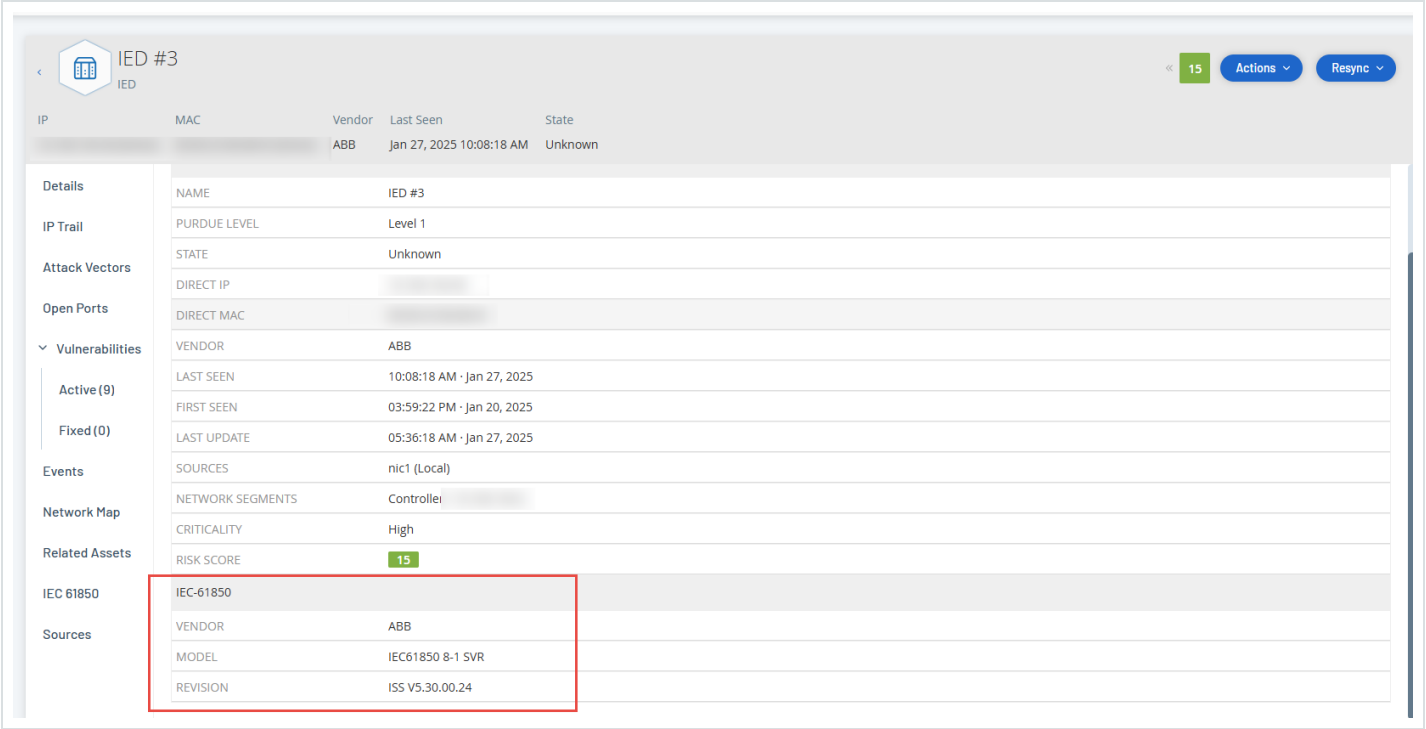
- Last Scan Duration



IEC 61850

The IEC 61850 section on the Details page shows the following configuration for the specific IED asset.

- Vendor
- Model
- Revision

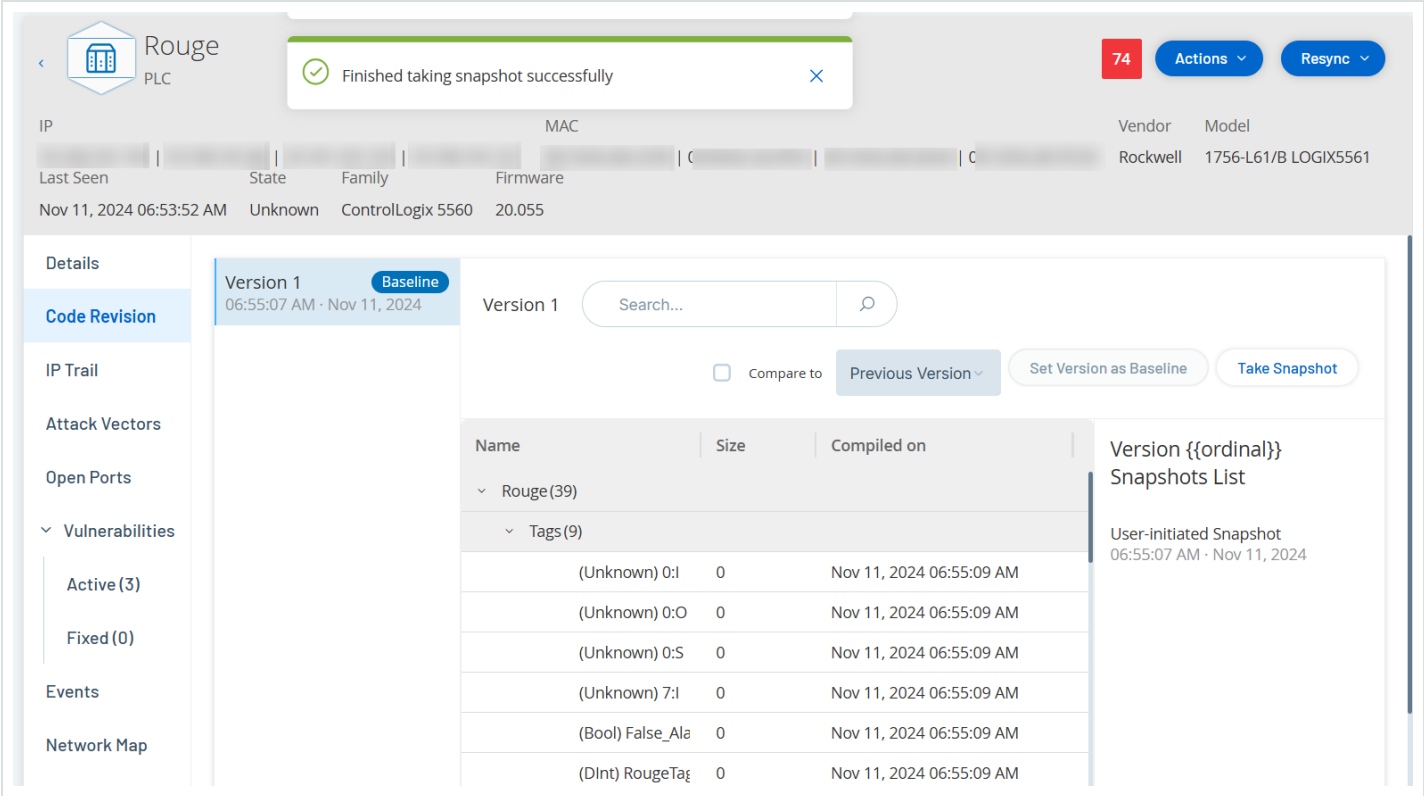


For more information about the SCD files, see the following:

- SCD Files
- IEC 61850

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.



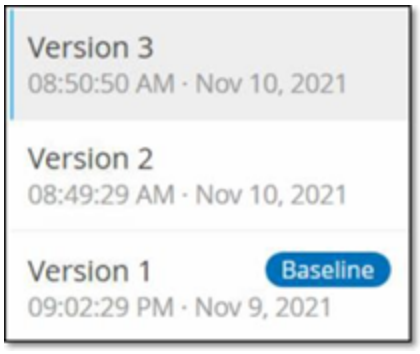
A snapshot can be triggered in the following ways:

- 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.

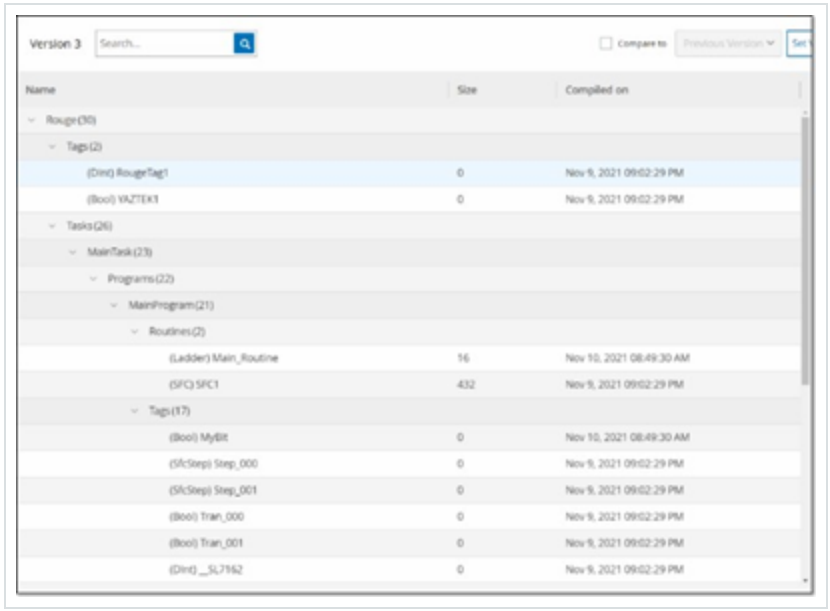
The following sections describe the various sections of the Code Revision display as well as how to compare different "snapshot" versions.

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.

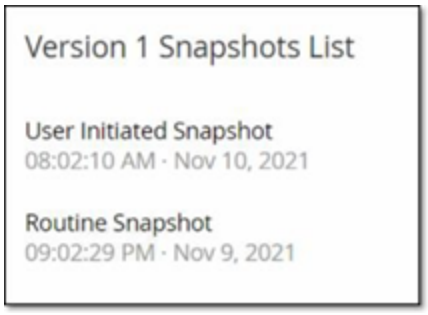
Snapshot Details Pane



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



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.

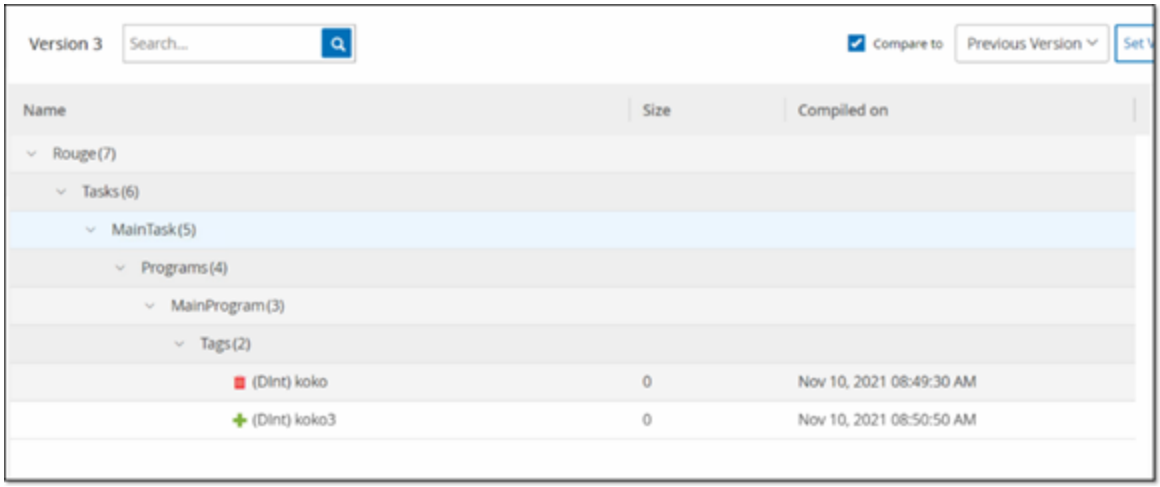
Deleted – code that was deleted from the selected version.

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.



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.
7. In the field next to the Compare to checkbox, select Baseline Version from the drop-down menu.

   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

You can manually initiate a snapshot. Tenable recommends that you perform a snapshot before and after a technician services a controller.

To create a snapshot of a controller:

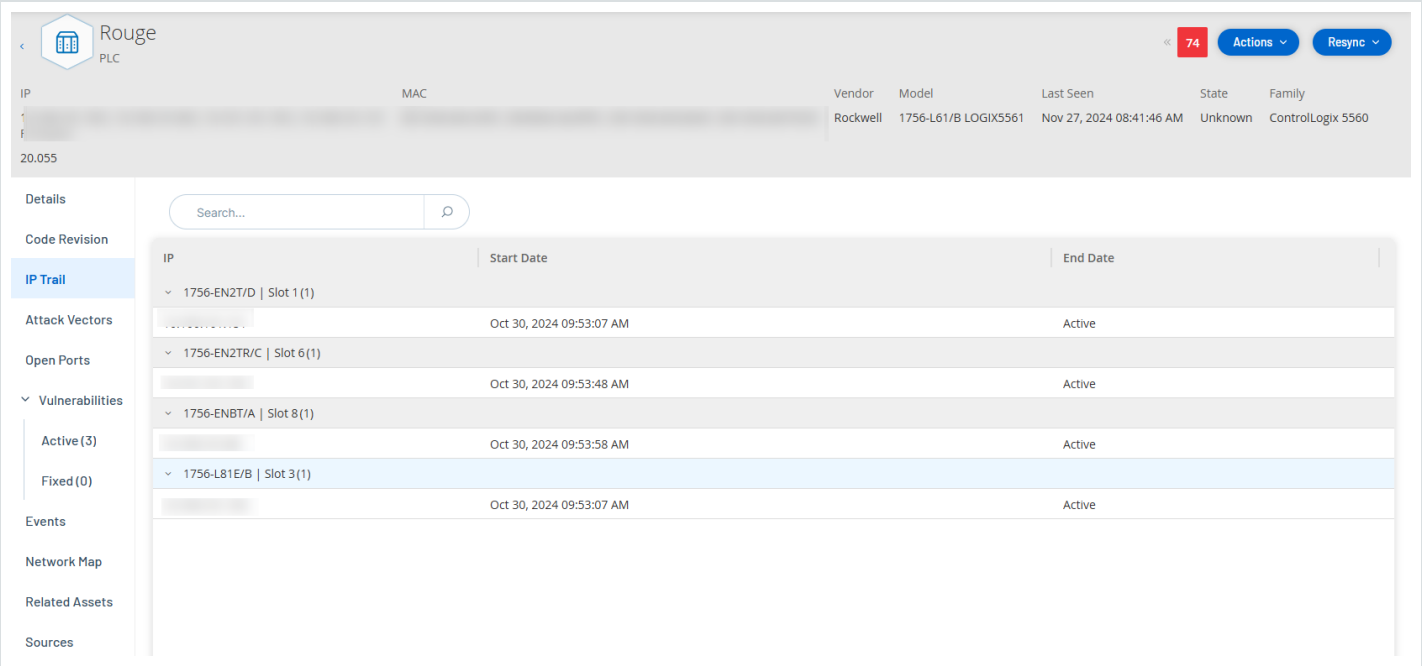
1. On the Inventory > Controllers screen, select the desired controller.
2. Click on the Code Revision tab.
3. In the upper right-hand corner of the Snapshot Details pane, click Take Snapshot.

   The User Initiated Snapshot is created.

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.

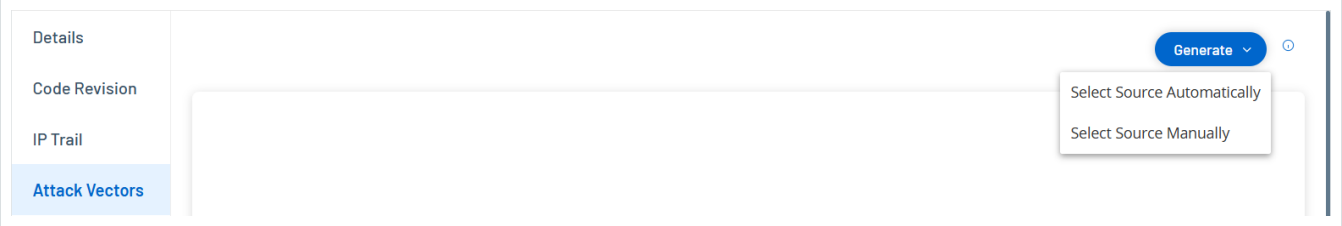
Generate Attack Vectors

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.

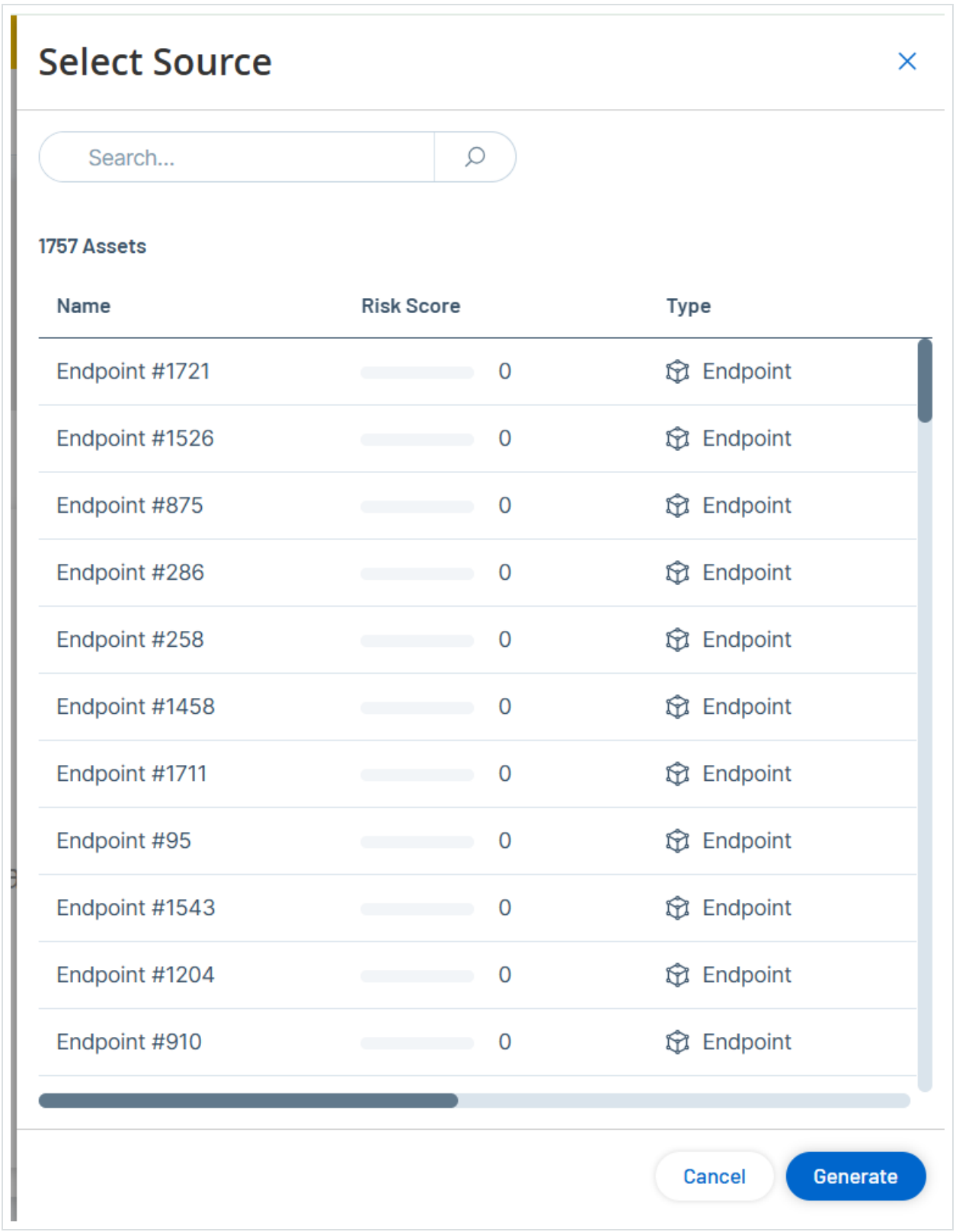


The Attack Vector is generated automatically and is displayed in the Attack Vector tab.

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.

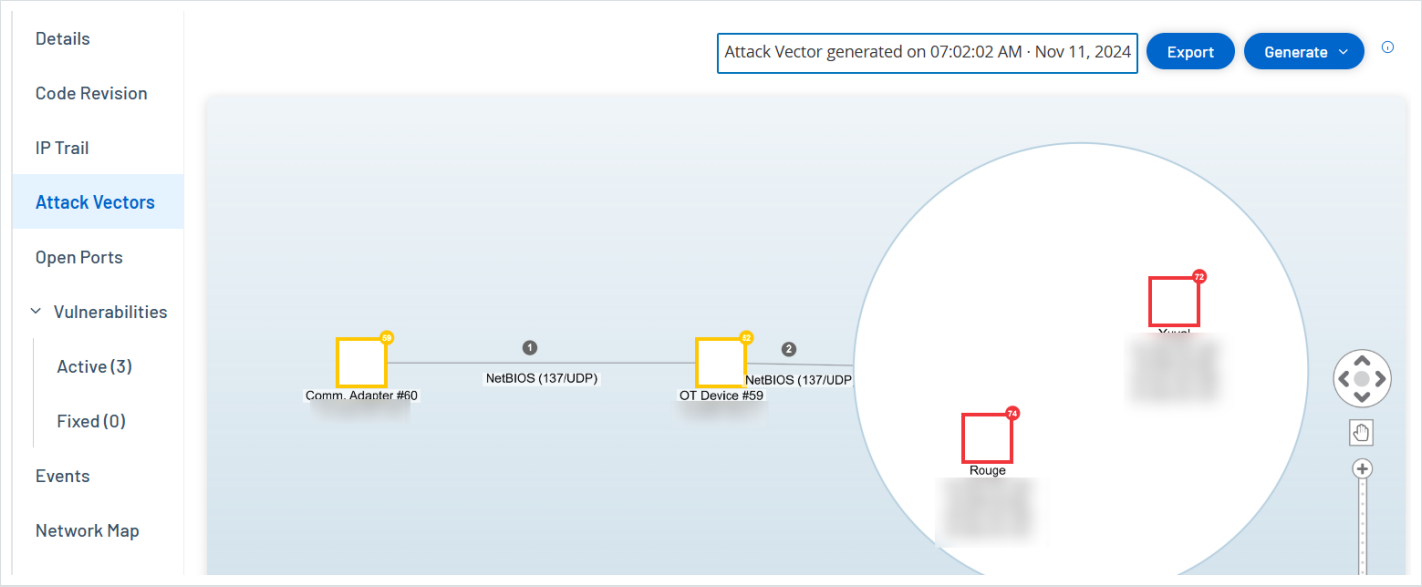

Select Source
Search...
1757 Assets
Name
Risk Score
Type
Endpoint #1721 0 Endpoint
Endpoint #1526 0 Endpoint
Endpoint #875 0 Endpoint
Endpoint #286 0 Endpoint
Endpoint #258 0 Endpoint
Endpoint #1458 0 Endpoint
Endpoint #1711 0 Endpoint
Endpoint #95 0 Endpoint
Endpoint #1543 0 Endpoint
Endpoint #1204 0 Endpoint
Endpoint #910 0 Endpoint
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



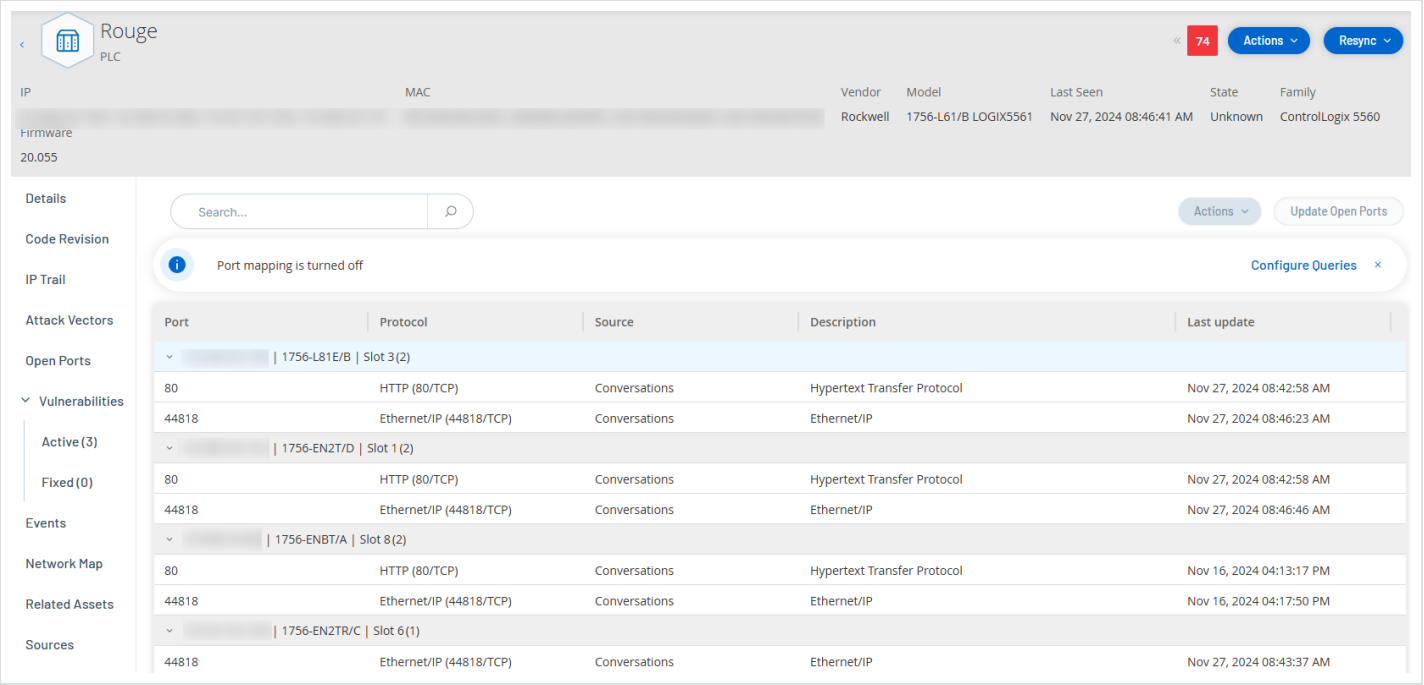
The Attack Vectors tab shows a diagram of the most recently generated Attack Vector for the specified target asset. The box next to the Generate button shows the date and time that the displayed Attack Vector was generated. The Attack Vector diagram includes the following elements:

- 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 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.

Update Open Ports

> Required OT Security User Role: Administrator, Supervisor, Security Manager, Security Analyst, Site Operator

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 on 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.

Run a Scan

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.

View the Asset Portal

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.

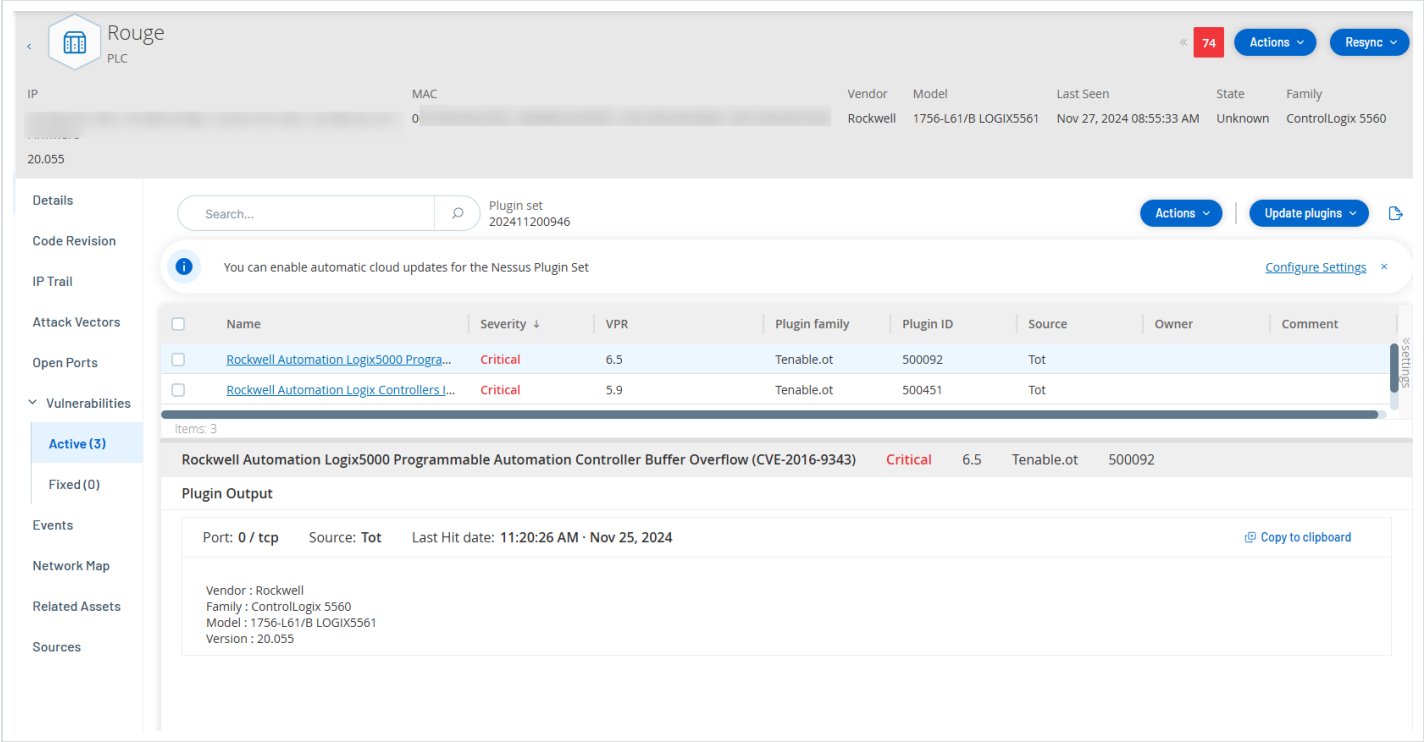
   The Asset Details screen is displayed.
2. Click on the Open Ports tab.
3. Select a specific port.
4. Click on the Actions menu.
5. From the drop-down menu, select View.

   A new browser tab opens showing the asset portal of that asset.

Vulnerabilities

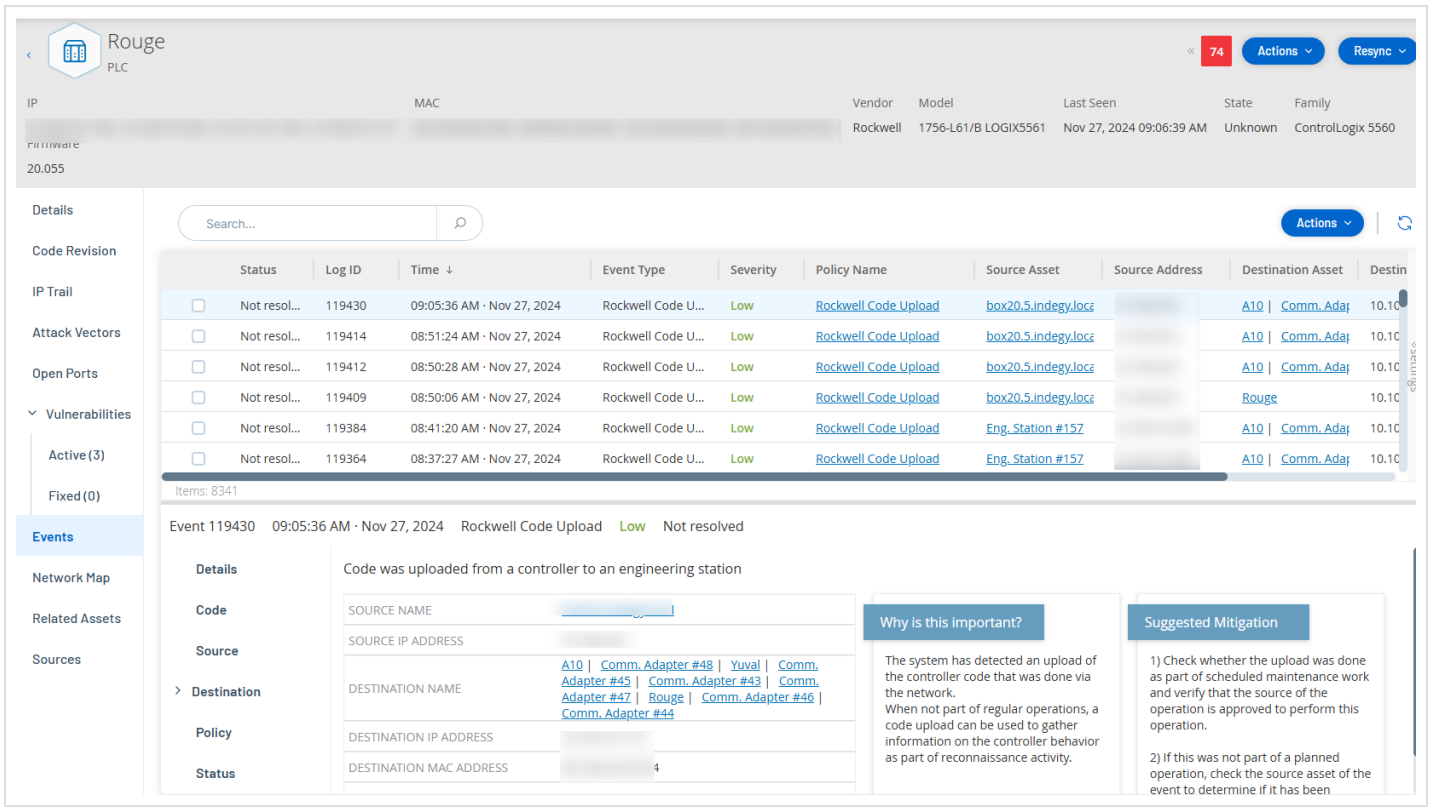
The Vulnerabilities tab shows a list of all vulnerabilities that affect the specified asset, as detected by OT Security Plugins. The system identifies vulnerabilities such as obsolete Windows operating systems, usage of vulnerable protocols and open communications ports which are known to be risky or non-essential for specific types of devices. The vulnerabilities are listed in two categories: Active and Fixed. 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 this page lists only vulnerabilities relevant to the specified asset. 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.



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 Capture File – Download the PCAP file for this Event.
- Exclude from Policy – 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:

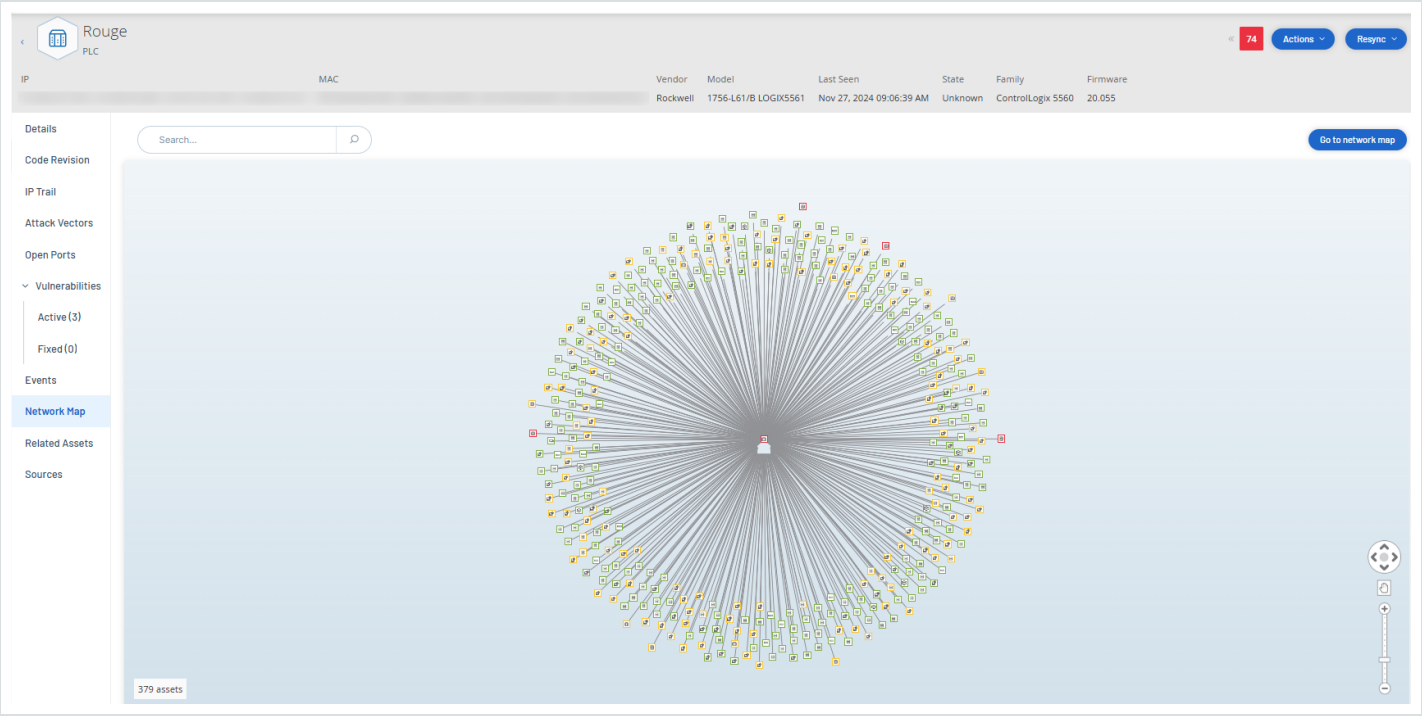
Parameter	Description
Log ID	The ID generated by the system to refer to the Event.
Time	The date and time that the Event occurred.
Event Type	Describes the type of activity that triggered the Event. Events are generated by Policies that are set up in the system. For an explanation of the various types of Policies, see Policy Types.
Severity	Shows the severity level of the Event. The following is an explanation of the possible values: • 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.

Parameter	Description
Destination Asset	The name of the asset that was affected by the Event. This field is a link to the Asset listing.
Destination Address	The IP or MAC of the asset that was affected by the Event.
Protocol	When relevant, this shows the protocol used for the conversation that generated this Event.
Event Category	Shows the general category of the Event. NOTE: On the All Events screen, Events of all types are shown. Each of the specific Event screens shows only Events of the specified category. The following is a brief explanation of the Event categories (for a more detailed explanation see Policy Categories and Sub-Categories): • Configuration Events – this includes two sub-categories • Controller Validation Events – These policies detect changes that take place in the controllers in the network. • Controller Activity Events – Activity Policies relate to the Activities that occur in the network (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

Parameter	Description
	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

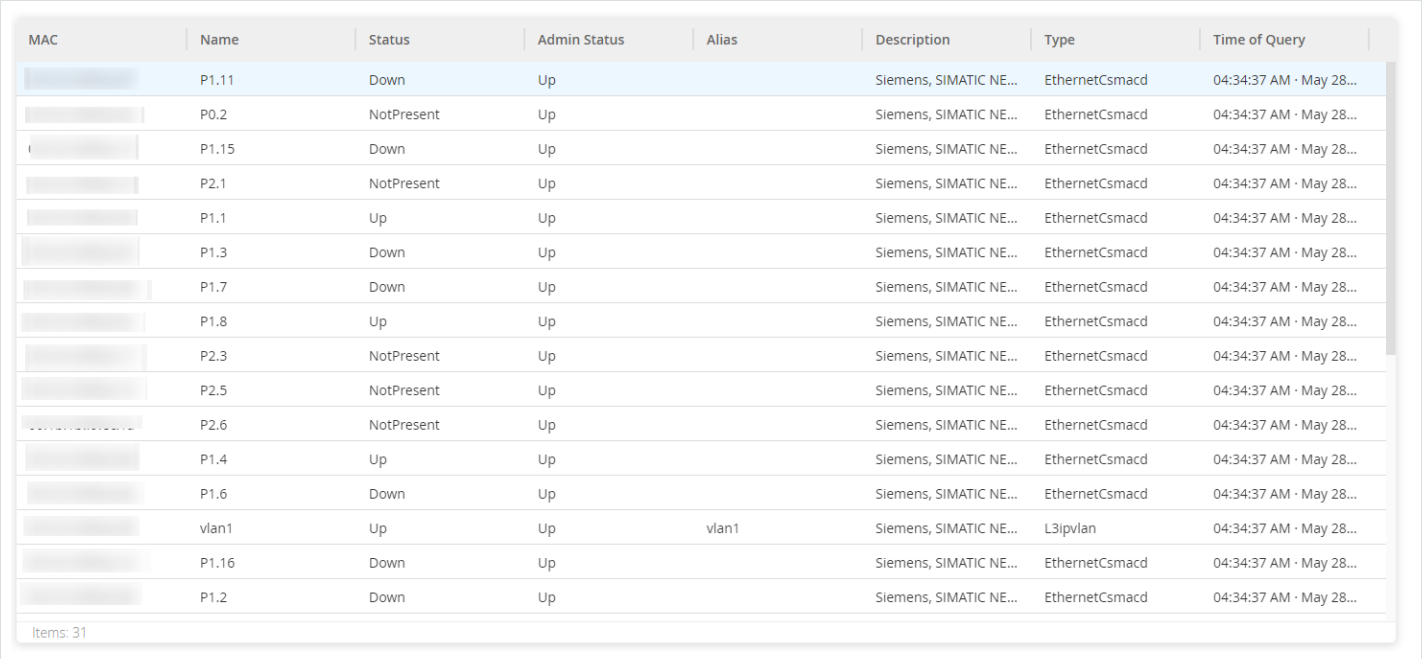
individual assets and not to groups of assets as shown in the main Network Map screen. For an explanation of the information shown in this tab, see Network Map.

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.

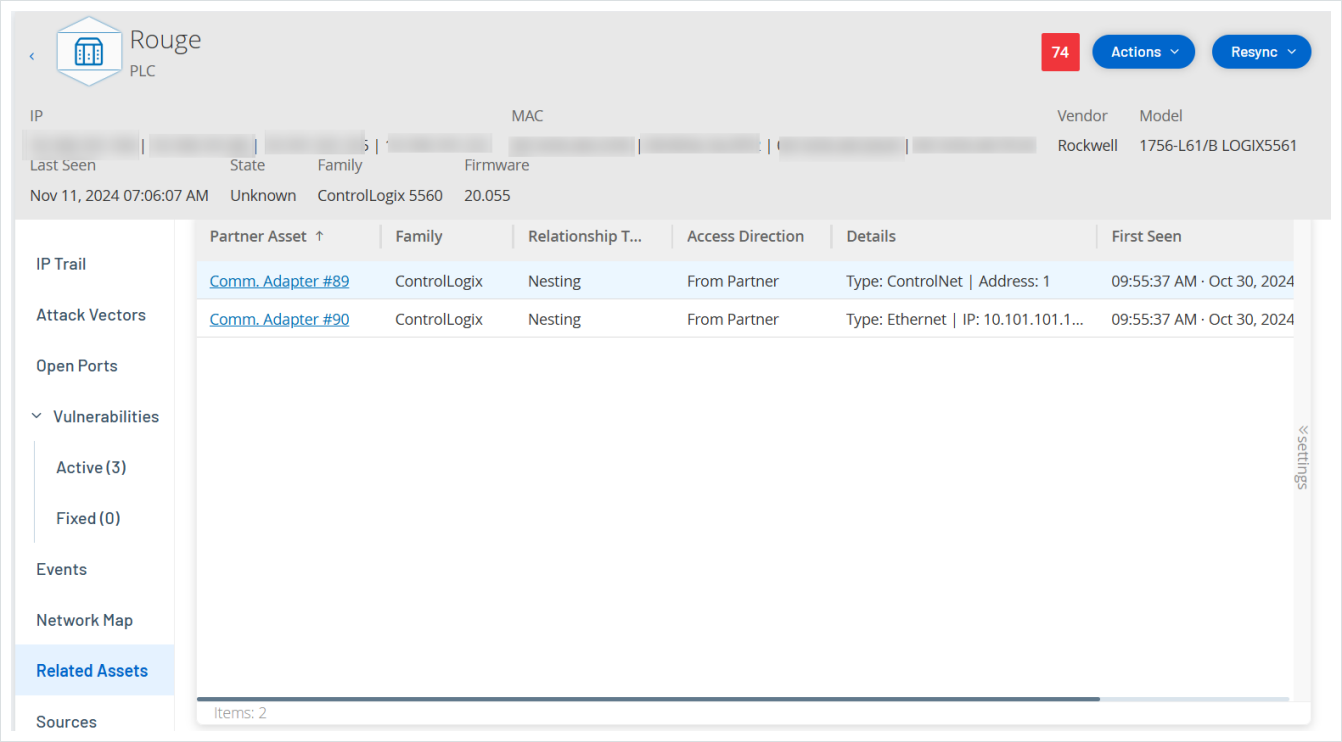
Related Assets

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.



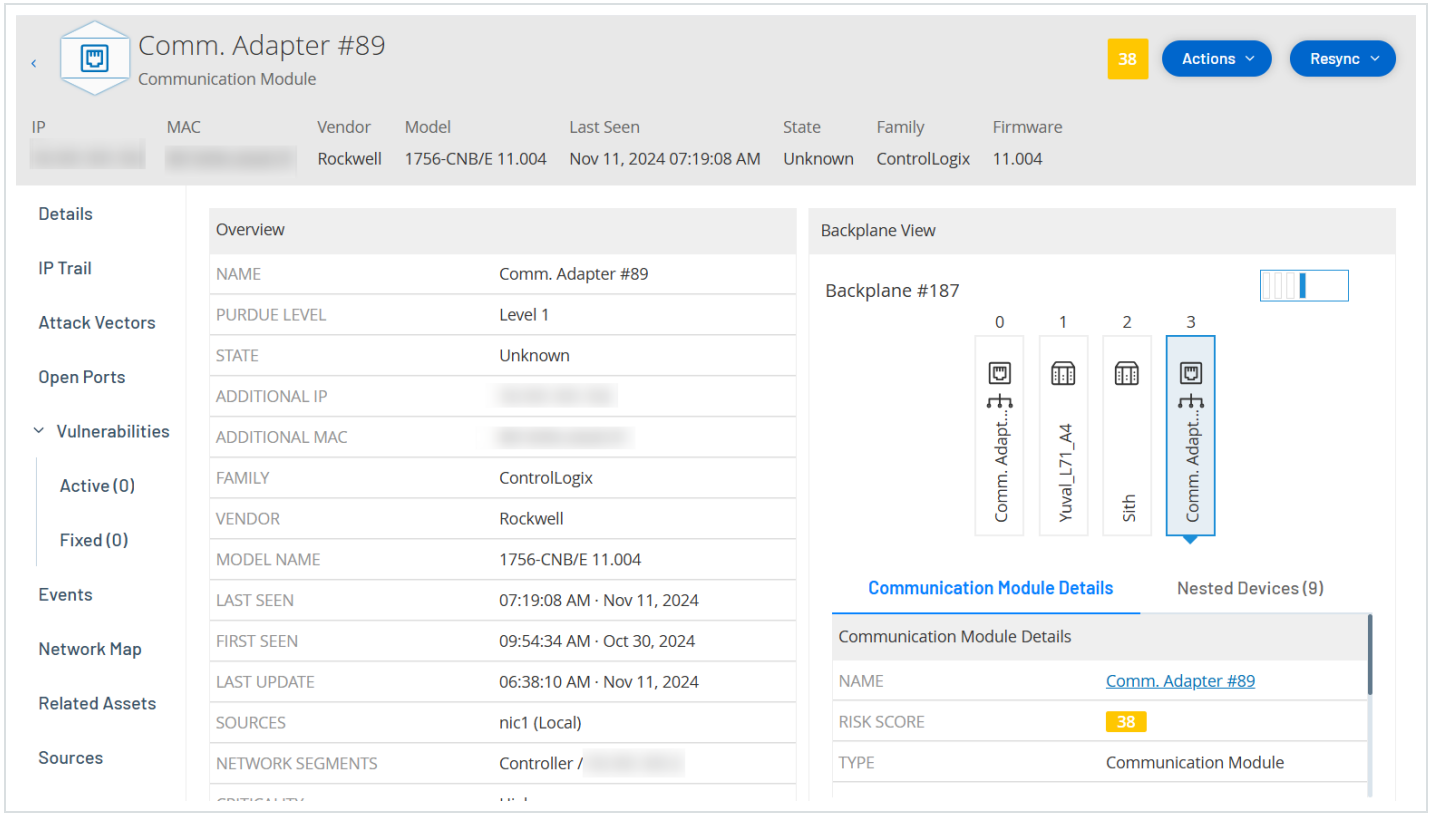
The Related Assets page appears with the following details:

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, and additional IP.
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.

IEC 61850

Based on the Substation Configuration Description (SCD) file you upload, OT Security generates the list of Manufacturing Message Specification (MMS) reports that describe the communication between the substation assets. OT Security displays an error message when it detects unauthorized access in the SCD file configuration. For more information about uploading SCD files, see SCD Files.

To access the IEC 61850 page:

1. Go to Inventory > All Assets.

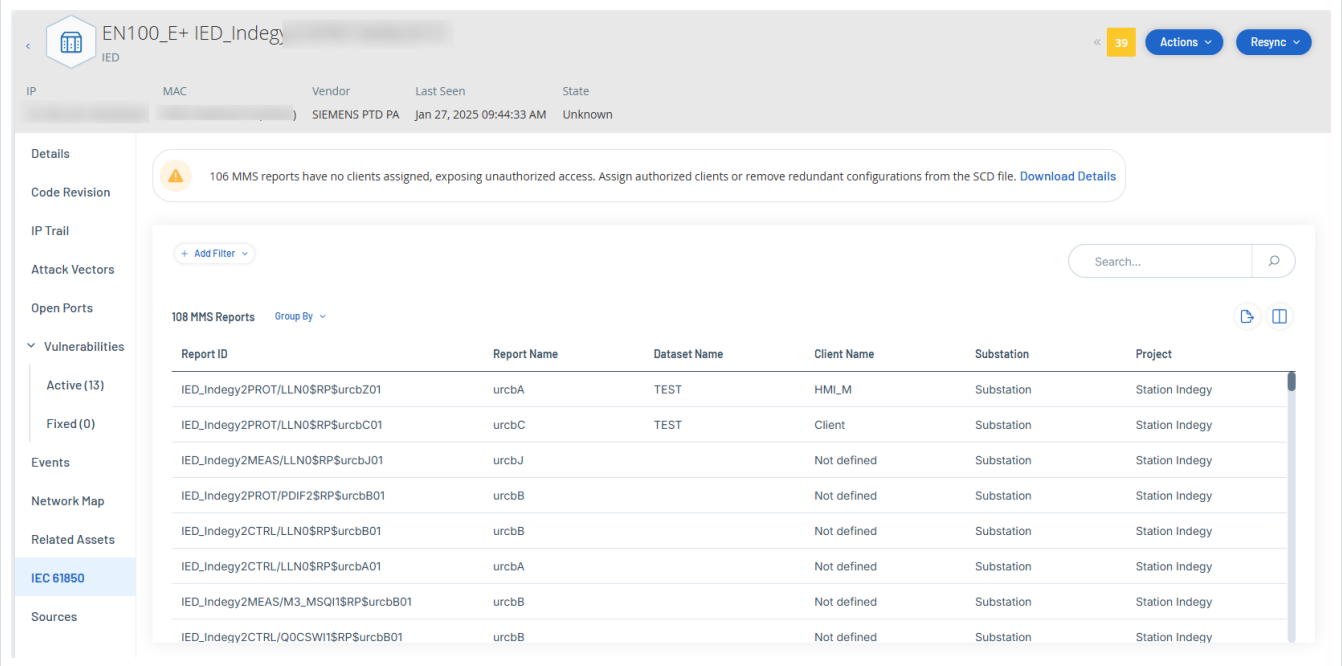
   The All Assets page appears.

2. Search for and select the asset or substation for which you want to view the IEC 61850 configuration.

   The asset details page appears.

3. In the left navigation bar, select IEC 61850.

The IEC 61850 page appears with the following details.

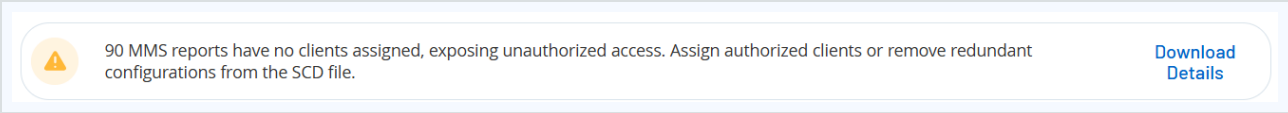


Column	Description
Report ID	The MMS report ID serving as a unique identifier for the report.
Report Name	The MMS report ID serving as a unique identifier for the report.
Dataset Name	The name of the data set linked to the MMS report defining the group of data points included in the report.
Client Name	The name of the client application or system that subscribes to and receives the report.
Substation	The substation where the IED (Intelligent Electronic Device) generating the MMS report is located.
Project	The overarching IEC 61850 project or system configuration to which the report and its associated components belong.

4. To view details of the findings that OT Security detects: In the error message at the top of the page, click Download Details.

   OT Security downloads the details in the CSV format.

   > Note: The number of MMS reports in the error message applies to the specific asset while the downloaded CSV file includes details of all the assets.

Sources

The Sources page for an asset provides all information related to the source of the asset such as the location, type, and the first and last reported time. You can also view the source of the asset in the Sources column on the Inventory > All Assets page.

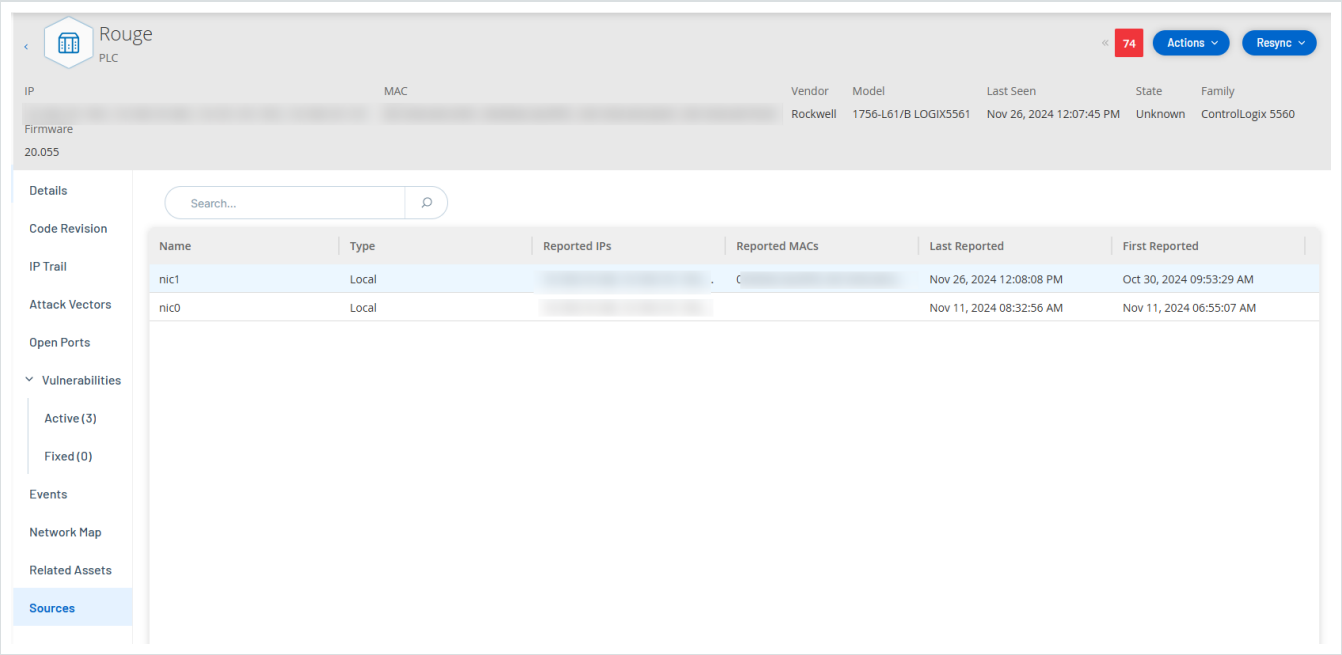
To access the Sources page:

1. In the Inventory > All Assets table, click an asset to open the asset details page.

   The asset details page appears.

2. In the left navigation pane, click Sources.

The Sources page appears.



The Sources page appears with the following details:

Column	Description
Name	The name of the source, for example nic 1 or nic 2 for a local source or the sensor name if the source is a sensor.
Type	The type of source: local ICP or sensor.
Reported IPs	The IP addresses that originate from the source asset.
Reported MACs	The Mac addresses that originate from the source asset. OT Security reports a Mac address if the sensor is close enough to observe the asset. If the sensor is far from the asset, but observes a conversation between them, OT Security reports only the observed IP addresses.
Last Reported	The time when the source asset was last reported.

First Reported	The time when the source asset was first reported.

Edit Asset Details

> Required OT Security User Role: Administrator, Supervisor, Site Operator

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.
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.
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.

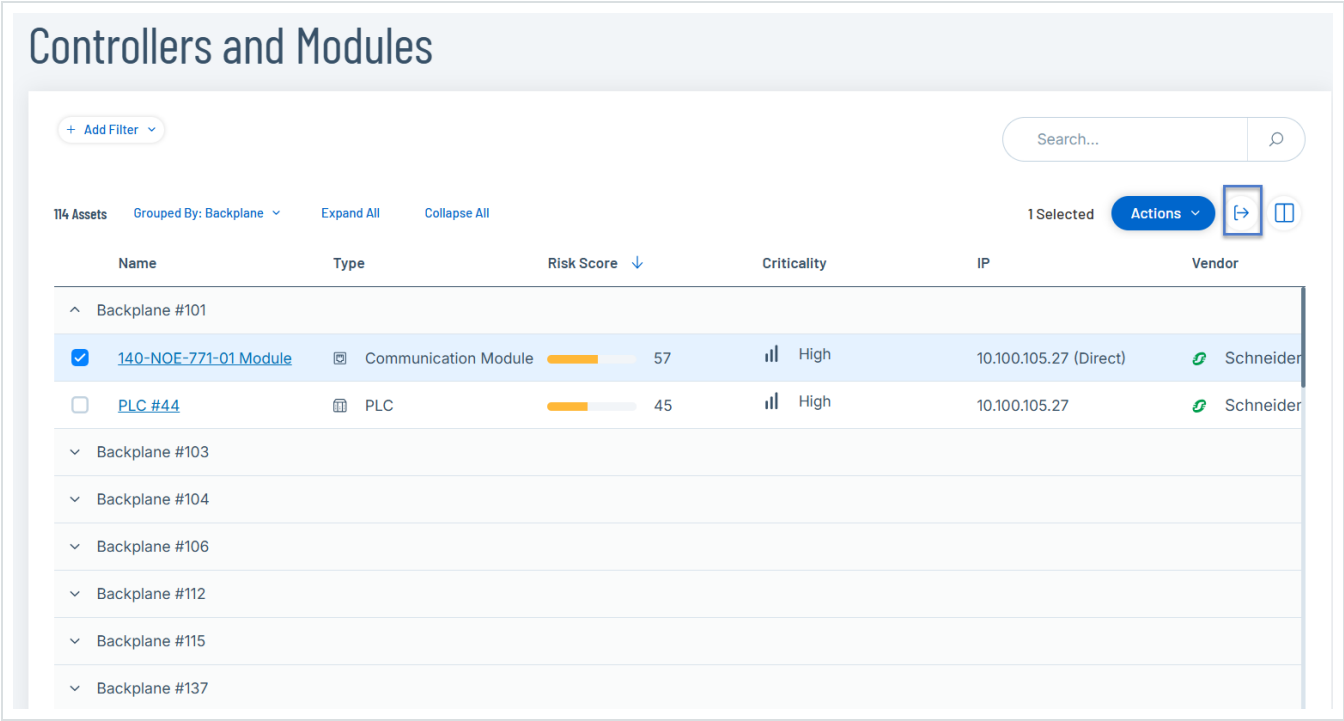
   OT Security saves the assets with the new configuration.

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.

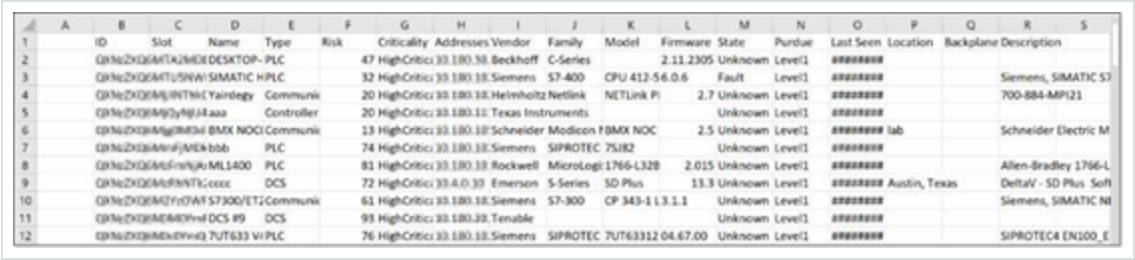
To edit asset details through a CSV:

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				DESKTOP-	PLC		47 High	10.180.50.	Beckhoff	C-Series		2.11.2305	Unknown	Level1	########				
3				SIMATIC H	PLC		32 High	10.180.10.	Siemens	S7-400	CPU 412-5	6.0.6	Fault	Level1	########			Siemens, SIMATIC S7	
4				Yairdegy	Communic		20 High	10.180.10.	Helmholtz	Netlink	NETLink PI	2.7	Unknown	Level1	########			700-884-MPI21	
5				aaa	Controller		20 High	10.180.11.	Texas Instruments				Unknown	Level1	########				
6				BMX NOC	Communic		13 High	10.180.10.	Schneider	Modicon P	BMX NOC	2.5	Unknown	Level1	########	lab		Schneider Electric M	
7				bob	PLC		74 High	10.180.10.	Siemens	SIPROTEC	7SJ82		Unknown	Level1	########				
8				ML1400	PLC		81 High	10.180.10.	Rockwell	MicroLogi	1766-L32B	2.015	Unknown	Level1	########			Allen-Bradley 1766-L	
9				cccc	DCS		72 High	10.4.0.10	Emerson	S-Series	SD Plus	13.3	Unknown	Level1	########	Austin, Texas		DeltaV - SD Plus Soft	
10				S7300/ET2	Communic		61 High	10.180.10.	Siemens	S7-300	CP 343-1 L	3.1.1	Unknown	Level1	########			Siemens, SIMATIC NI	
11				DCS #9	DCS		93 High	10.180.10.	Tenable				Unknown	Level1	########				
12				7UT633 V	PLC		76 High	10.180.10.	Siemens	SIPROTEC	7UT63312	04.67.00	Unknown	Level1	########			SIPROTEC4 EN100_E	

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

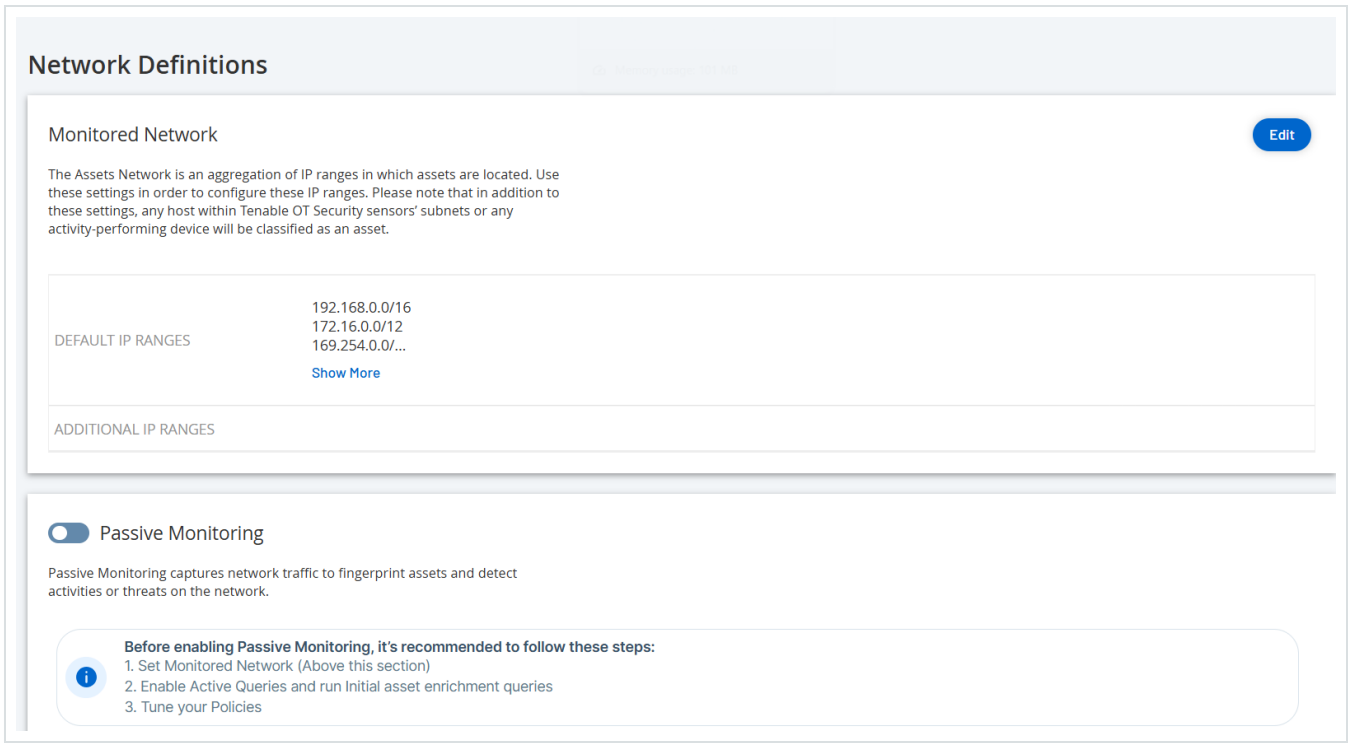
   > Note: You must enter valid data for parameters that require specific options (for example Type, Criticality, Purdue Level). Otherwise, the corresponding asset will fail to update.

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 Settings, go to Environment Settings >Network Definitions.

   The Network Definitions 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 Settings > Environment **Settings** > 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 Settings > Environment Settings > Hidden Assets page.
6. Click Hide.

   OT Security hides the assets from 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. Depending on your needs, you can pull diagnostics directly from the asset inventory or through the Tenable Core management interface.

Export an Asset Diagnostics Report

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.

Export Tenable OT Security Diagnostic Report (Tenable Core)

You can generate and export an Tenable OT Security-specific diagnostic report from Tenable Core for troubleshooting.

Before you Begin

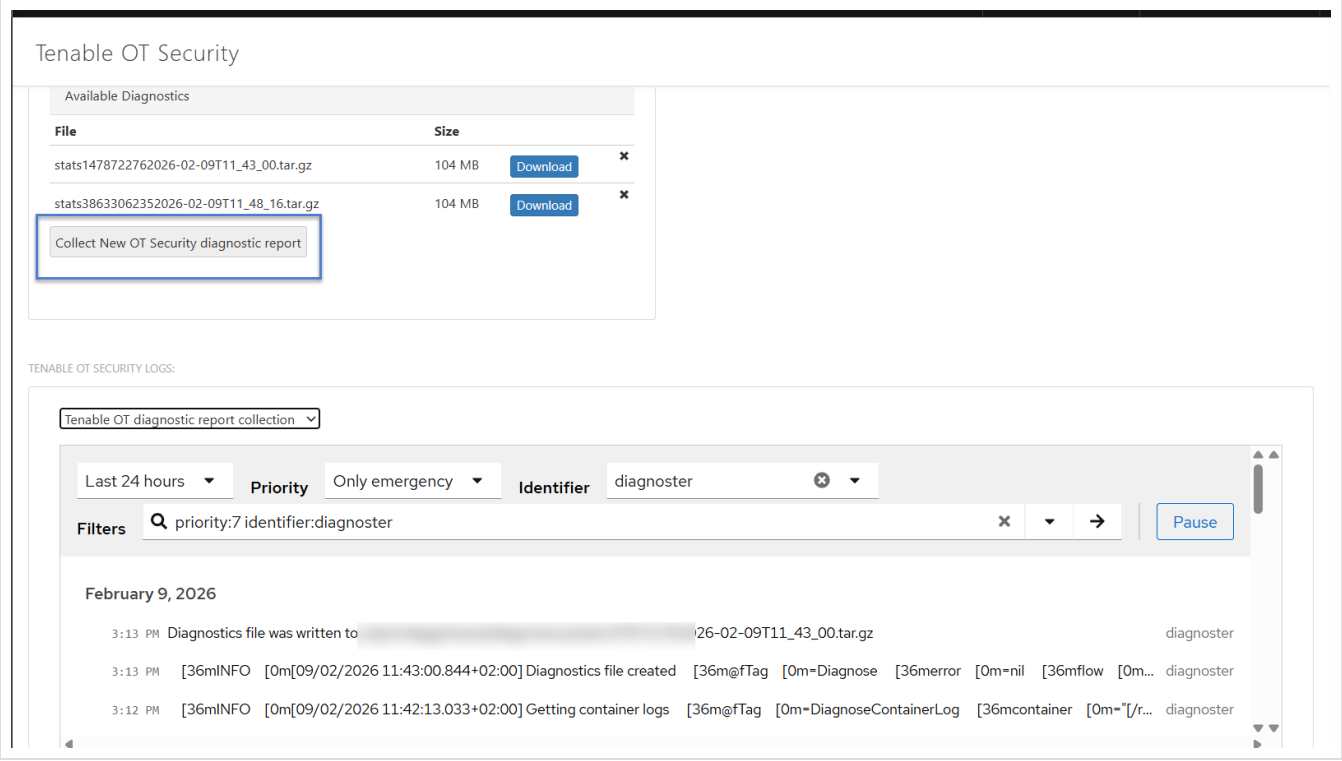
- Make sure you have Administrative access.

To generate the diagnostic report:

1. Log in to Tenable Core.
2. In the left navigation bar, click **Tenable OT Security**.

   The **Tenable OT Security** page appears.
3. In the OT Diagnostics section, click Collect New OT Security Diagnostic Report.

   The system generates the diagnostic report.



4. Click Download next to the report that you want to download.

   Tenable Core downloads the report to your system. After Tenable Core generates the logs, it may take several minutes before the data appears in the debug logs.

Merge Assets

Required OT Security User Role: Administrator, Supervisor, Site Operator

Devices in your network may appear as two or more separate assets in OT Security due to passive traffic observation, routing configurations, or insufficient asset details information, which prevents the automatic merging of assets internally.

For example, multi-homed devices such as workstations, servers, or controllers typically have multiple IP addresses enabling them to communicate across various networks. Alternatively, consider virtual network interfaces on a Switch, Router, or Firewall. Even though they are virtual extensions of a single physical network device, each of these might register as a distinct asset.

In such cases, you can use the Merge Assets option to merge two assets together and remove duplicates. You can access this option either from the Inventory page or from the single asset details page.

> Caution: This action is irreversible.

To merge assets:

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

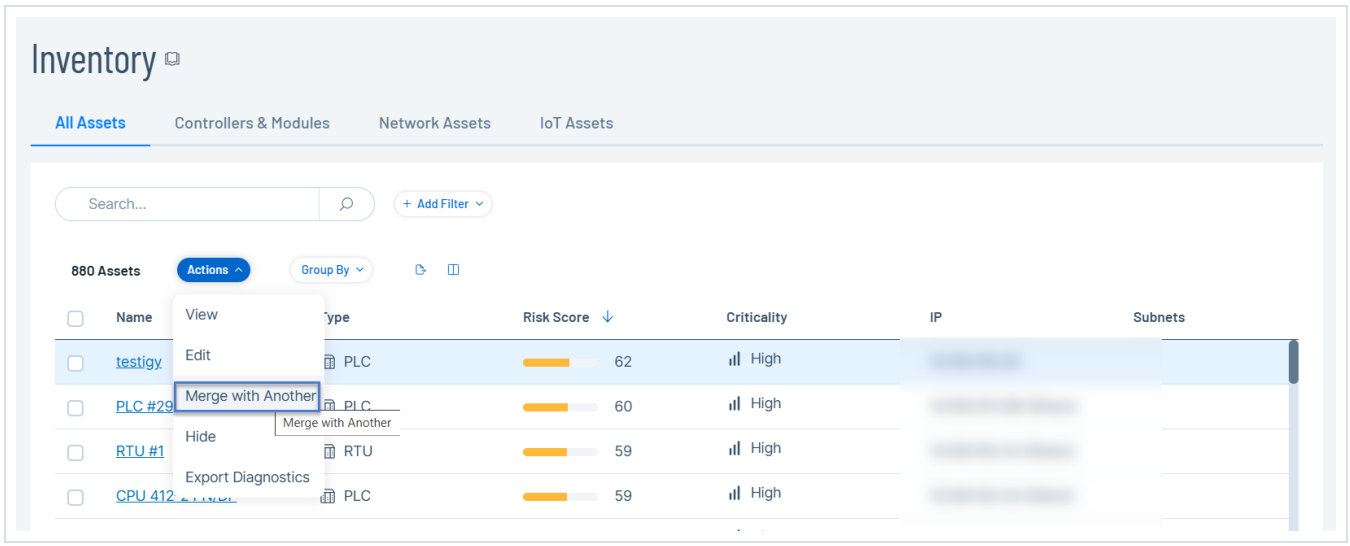
   The All Assets page appears.

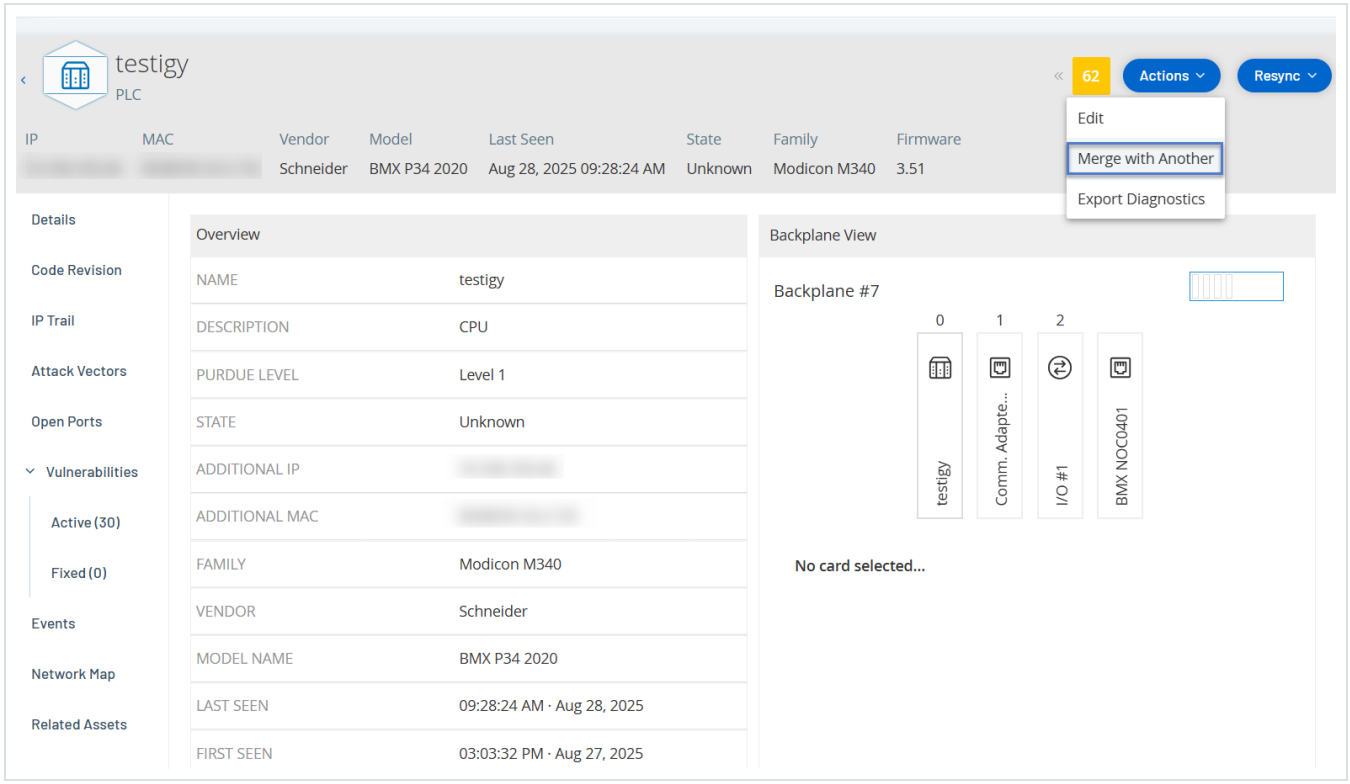
2. In the All Assets table, do one of the following:

   - Select the target asset to merge.
   - Click the asset link to open the asset details page.

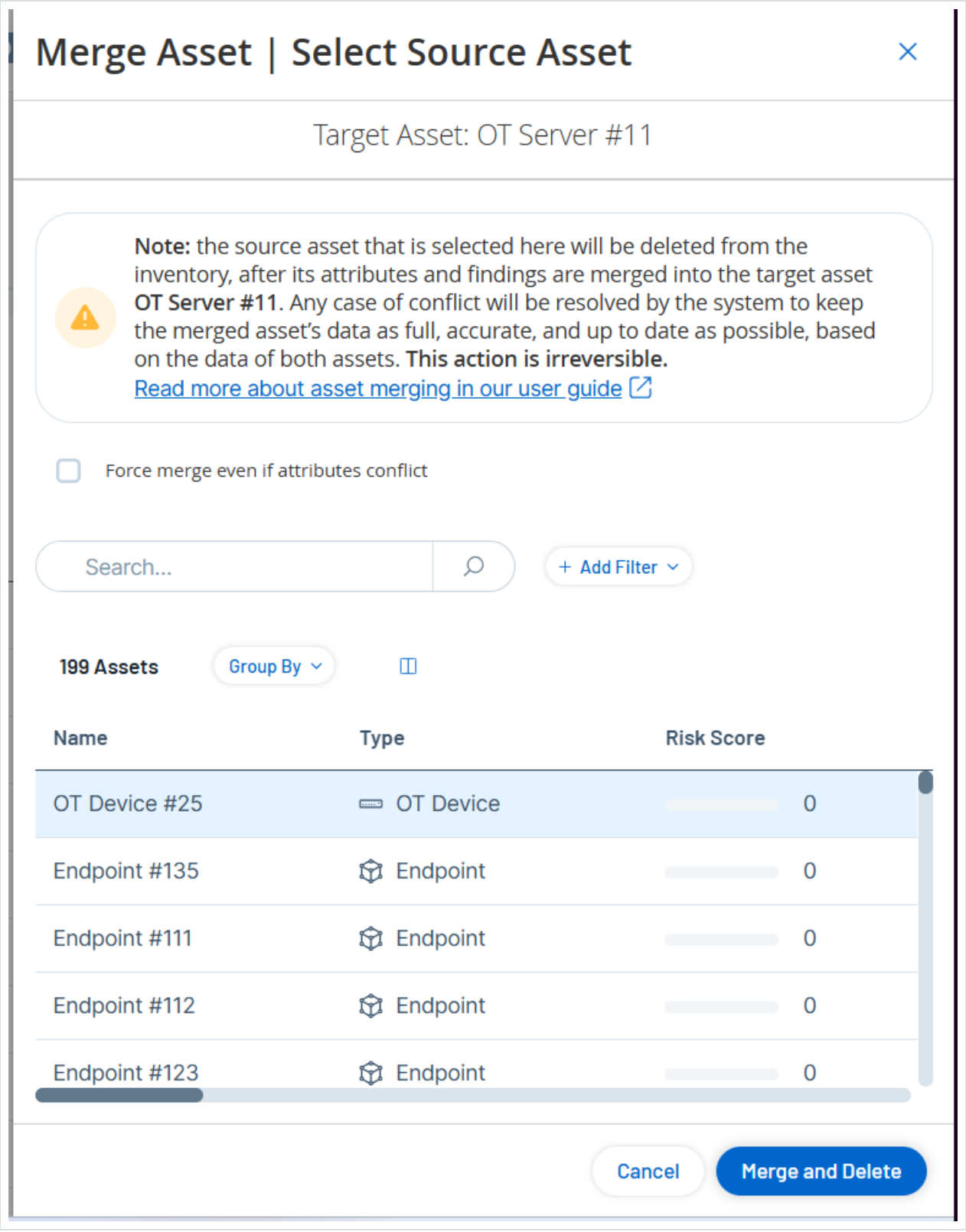
   OT Security enables Actions.

3. Click Actions > Merge with Another.





The Merge Asset | Select Source Asset panel appears.



4. Filter or search for the source asset.

5. Select the source asset to be merged with the target asset.
6. (Optional) Select the Force merge even if attributes conflict checkbox to bypass conflicts.
7. Click Merge and Delete.

   OT Security deletes the source asset and merges its attributes and findings to the target asset.

What Happens When You Merge Assets

The asset merging process combines two assets into a single entity while maintaining data integrity across the system.

This operation involves these key stages:

- Asset Properties Consolidation: When assets are merged, their properties are merged into the destination asset. If both assets have a different value for the same property, the system uses a priority mechanism to decide which value to keep. This process ensures the merged asset retains the most accurate or recent information.
- Connection Preservation: Network connections previously pointing to either asset now reference the merged asset. This includes:
  - Direct connections to other devices
  - Slot-based connections within backplanes
  - Network interface mappings, including IP and MAC addresses. The system ensures that all historical address information is retained, and duplicate entries are removed.
- Finding Consolidation: The system consolidates all findings, vulnerabilities, and security events under the new one, thereby preserving its complete security history.

Merge Conflicts and Forced Merge

The following assets cannot be merged:

- Special assets such as ICP, Sensor, or broadcast assets.
- Assets from different backplanes (only one of them is allowed to have a backplane).
- Assets that have different slots (if both assets have slots, it must be the same slot).
- Assets that have different serial numbers.

Force Merge: Selecting the Force Merge checkbox bypasses the system's checks for backplane, slot, and serial conflicts. While this option does not guarantee a successful merge and the merge engine may still block invalid operations, the system proceeds with the merge before it might be blocked.

How to Rectify an Accidental Merge

If an asset merge was performed in error, or you need to revert both assets to an unmerged state, delete the asset. Deleting it allows the system to rediscover the individual asset as they were before the merge. For information on how to delete a single asset or a group of assets from OT Security, see this knowledge base article.

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.

The Nessus scan in OT Security uses the same policy settings as a basic network scan in Tenable Nessus, Tenable Security Center, and Tenable Vulnerability Management. The only difference is the performance options in OT Security. The following are the performance options for the Nessus

scan in OT Security. These options also apply to the Nessus scan you launch from the Active Queries Management page.

- 5 simultaneous hosts (max)
- 2 simultaneous checks per hosts (max)
- 15 second network read timeout

> 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:

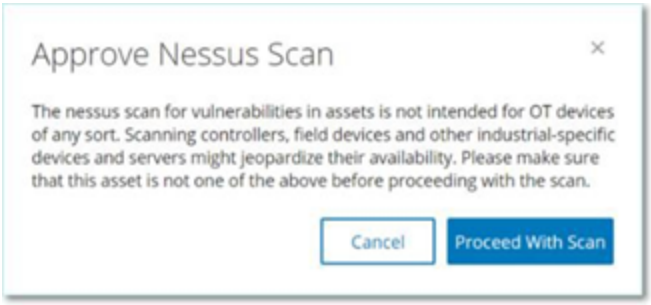
1. Go to Inventory > Network Assets.

   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

Required OT Security User Role: Administrator, Supervisor, Security Manager, Security Analyst, Site Operator

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:

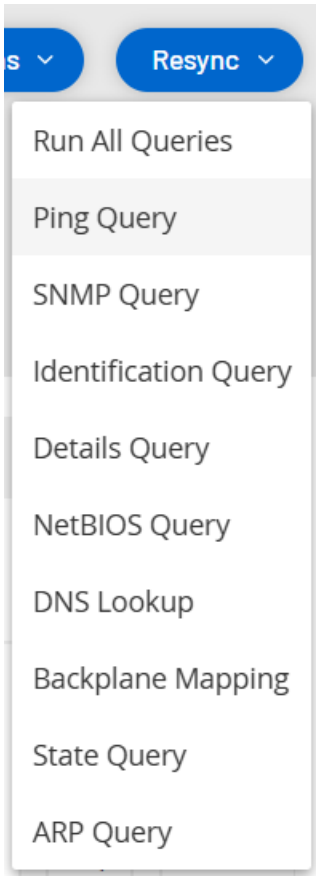
- The device is unreachable or lacks available queries.
- Permission configured on the Active Queries page may restrict non-administrator accounts from initiating certain queries.
- Queries are not enabled on this OT Security deployment.

- All queries in the Active Queries > Manual section are disabled.
- The asset lacks a known IP address for querying.

To run Resync asset data:

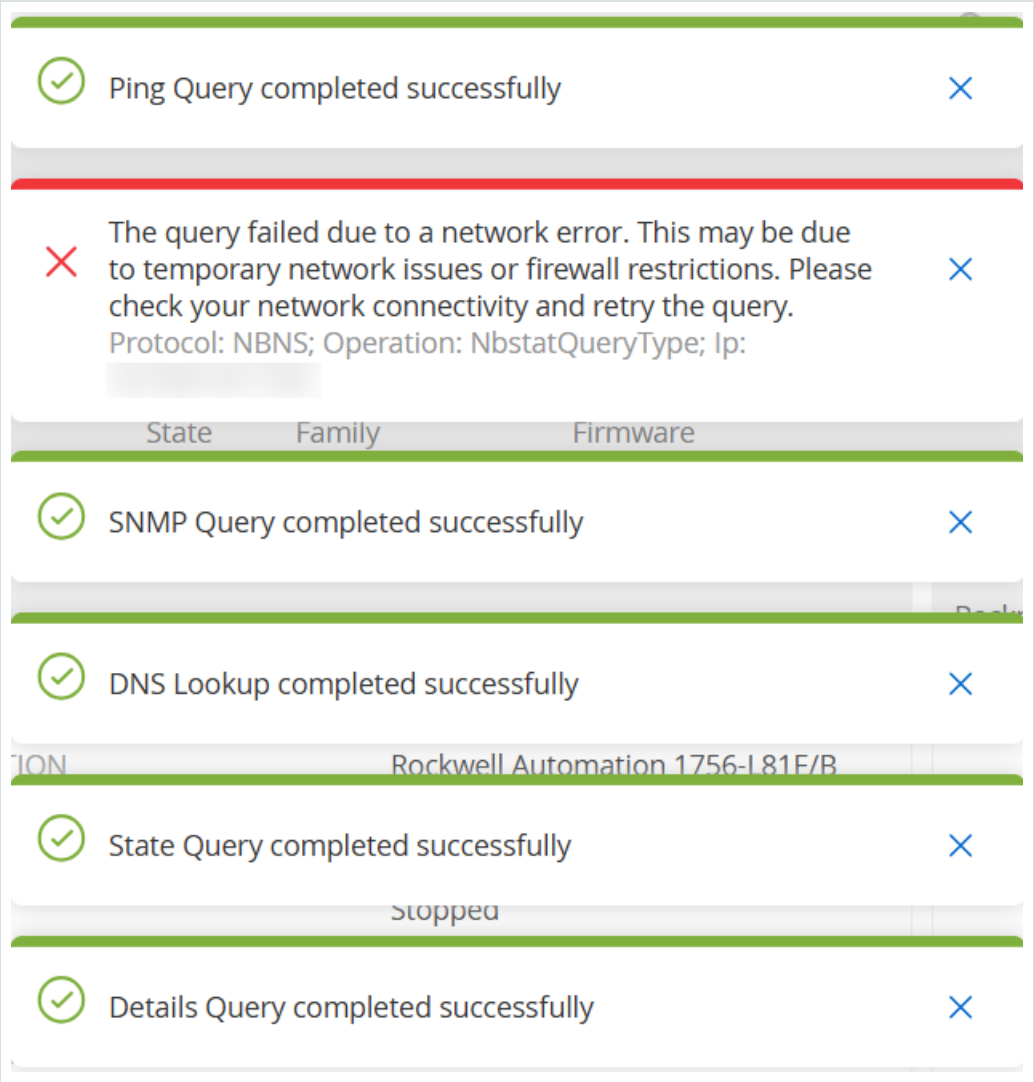
1. On the Asset Details page for the required asset, in the upper-right corner, click Resync.

   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.



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

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, and vulnerable open ports.

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 Settings.

View Vulnerabilities

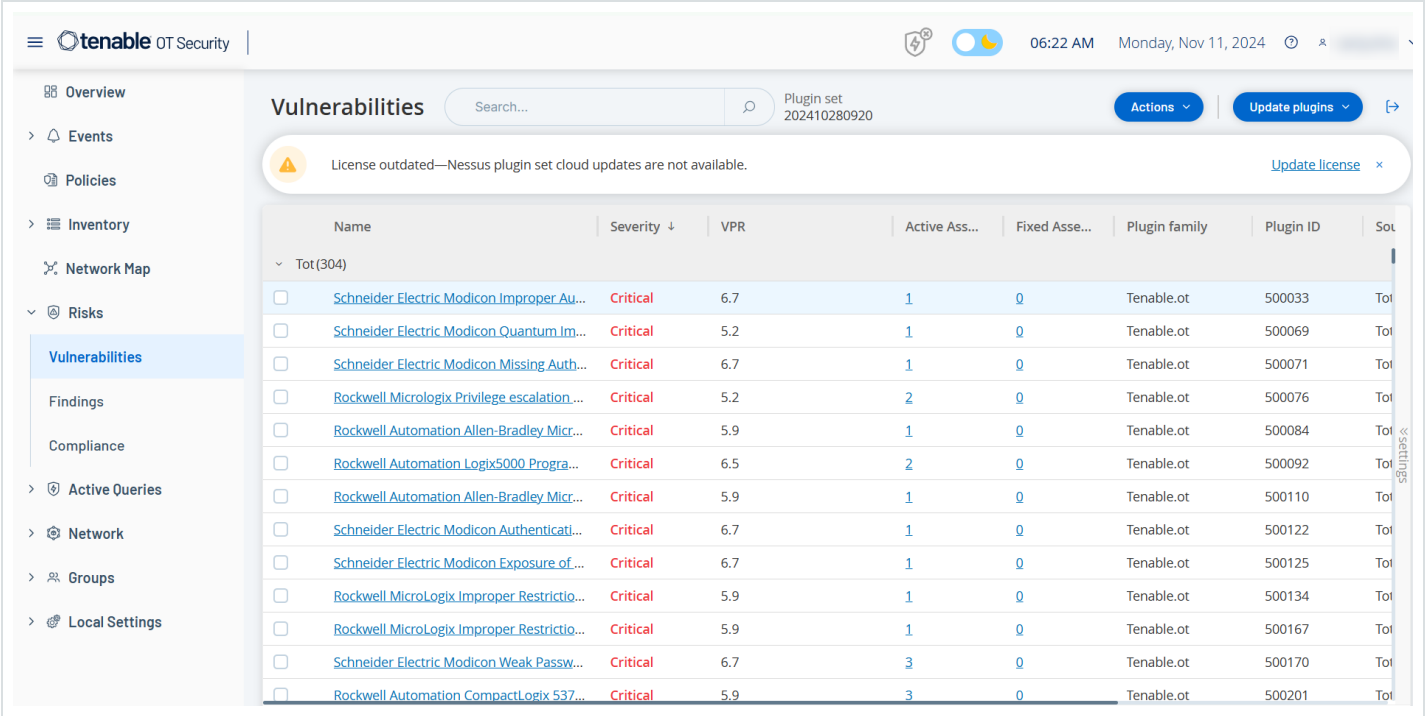
> Required OT Security User Role: Administrator, Supervisor, Security Manager, Security Analyst, Site Operator, Read Only

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.

> 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.

Active Assets	The number of assets in your network that are currently affected by this vulnerability.
Fixed Assets	The number of assets in your network affected by this vulnerability and remediated recently, over a defined period of time (by default, one year). Contact Tenable Support to customize this period.
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

Required OT Security User Role: Administrator, Supervisor, Security Manager, Security Analyst

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.

View Plugin Output from Vulnerabilities

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.

View Plugin Output from Inventory

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.

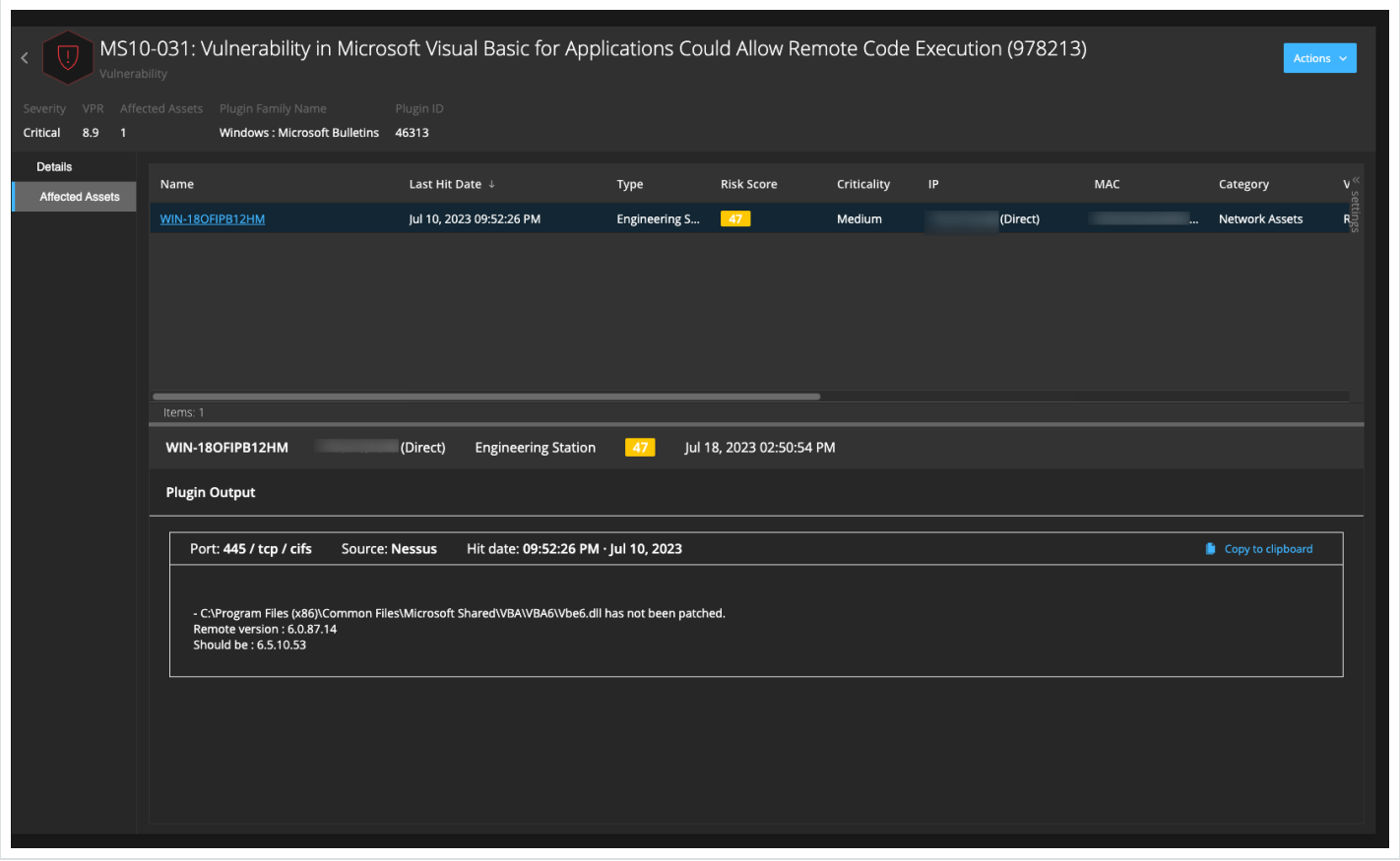
3. Click the Vulnerabilities tab.

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

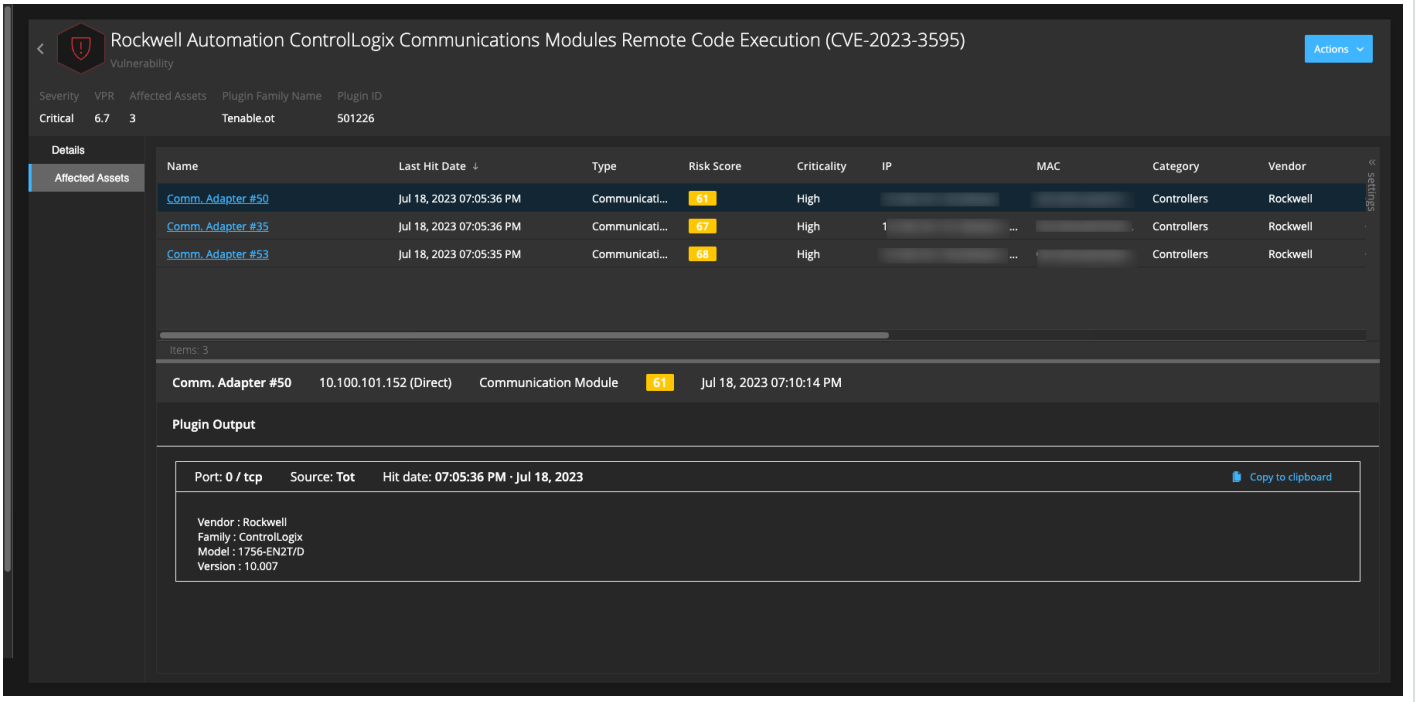
   - Hit date
   - Source
   - Port
   - Plugin output

> Note: Plugin output is not available for all plugins.

Example of a plugin output for a Tenable Nessus Plugin



Example of a plugin output for OT Security Plugin



Findings

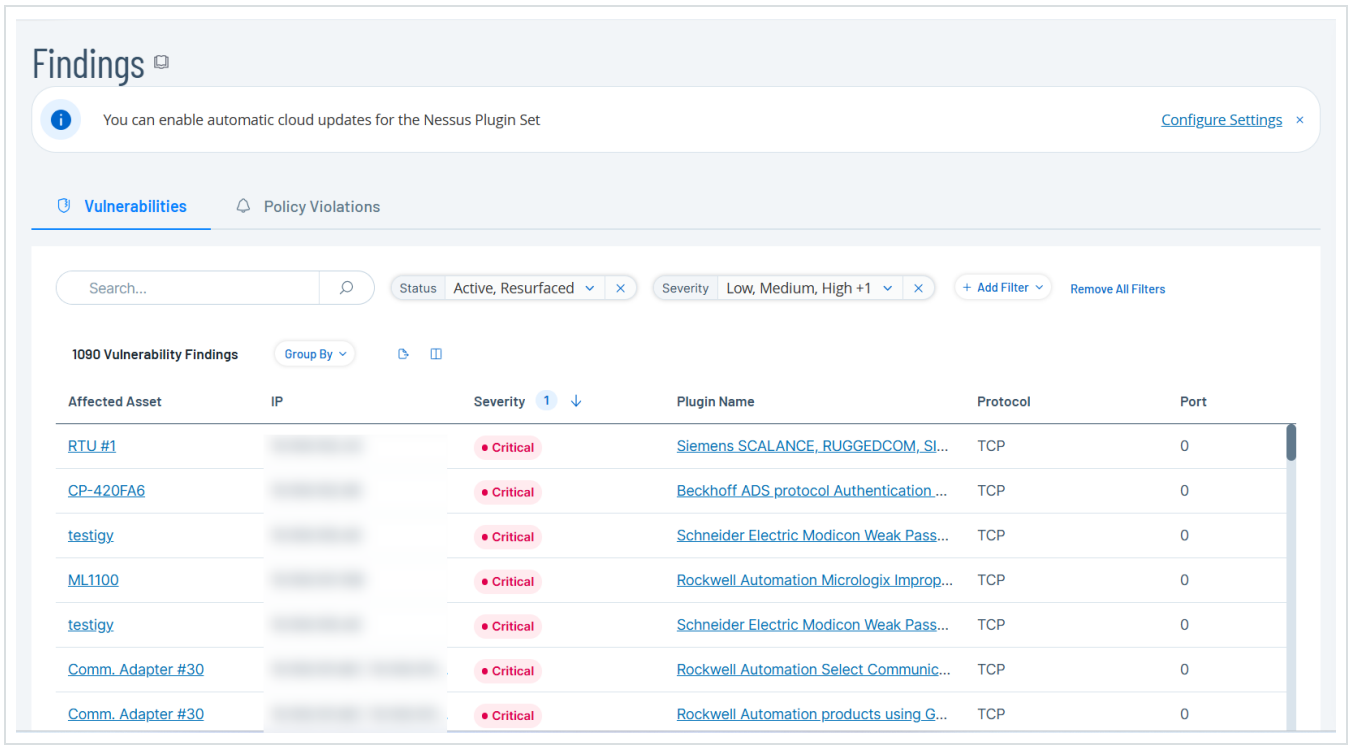
Use the Findings page to review the list of individual instances of vulnerabilities that affect your environment per asset. The Findings page allows you to do the following:

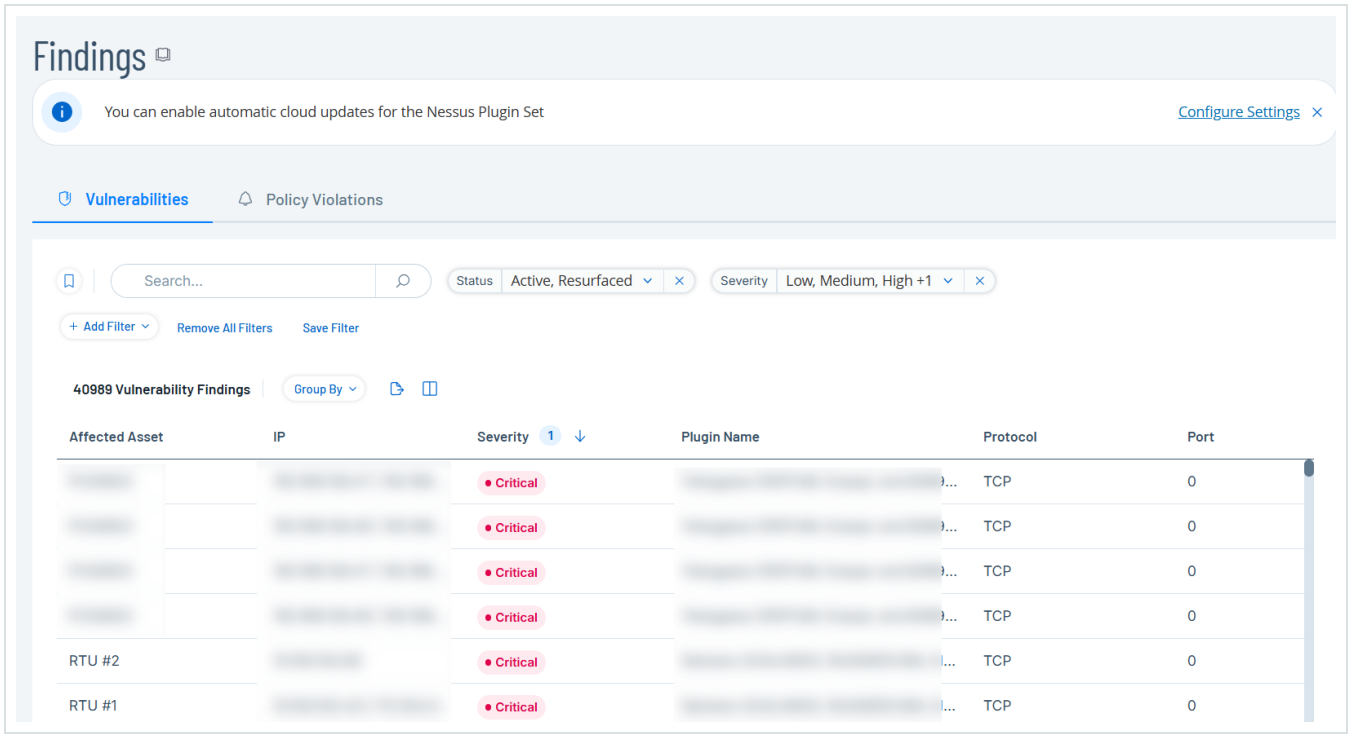
- View detailed evidence for each specific “hit” of a vulnerability in your environment.
- Filter the list of vulnerabilities by either properties of the plugin, the affected asset, the specific instance such as Status, Last hit, or any combination of the properties.
- Export the filtered list of findings to assign them for remediation.

To access the Findings page:

1. In the left navigation menu, go to Risks > Findings.

   The Findings page appears with the vulnerabilities in a table format.





The Findings table includes the following details:

Column	Description
Affected Asset	The asset where the vulnerability is detected.
IP	The IP address of the asset.
Severity	The severity of the vulnerability: Critical, Medium, Low, or Info.
Plugin Name	The plugin that detected the vulnerability.
Plugin ID	The ID of the plugin.
Port	The port where the vulnerability is detected.
Protocol	The protocol used to communicate with the asset.
VPR	Vulnerability Priority Rating for the vulnerability.
Status	The status of the vulnerability. The possible values are: Active – Indicates that the vulnerability continuously appeared since its initial detection. Fixed – Indicates that the vulnerability initially appeared and disappeared and not resurfaced. Resurfaced – Indicates that the vulnerability appeared and disappeared and then reappeared.
Plugin Source	The plugin source.
First Hit	The time when the vulnerability was first detected.
Last Hit	The time when the vulnerability was last detected.

Column	Description
Asset Tags	The tags associated with the asset. See Asset Tags & Groups.
Fixed at	The time when the vulnerability was remediated.
Plugin Family	The family of the plugin.
Asset Type	The asset type, such as PLC and OT device.
Asset Risk Score	The risk score of the asset.
Asset Category	The category to which the asset belongs to, such as Controller, Network Assets.
Asset Vendor	The name of the vendor of the asset.
Asset Criticality	The criticality of the asset based on the severity of the vulnerability: High Criticality, Medium Criticality, or Low Criticality.
Asset Family	The family of the asset.
Asset Model	The model of the asset.
Firmware	The firmware of the asset.
OS	The operating system that the asset runs on.
Asset State	The current state of the asset.
Purdue Level	The purdue level of the asset.
Network Segment	The network segment that the asset belongs to.

Column	Description
Location	The asset's location.
Backplane Name	The name of the backplane where the vulnerability was detected.

View Findings Details

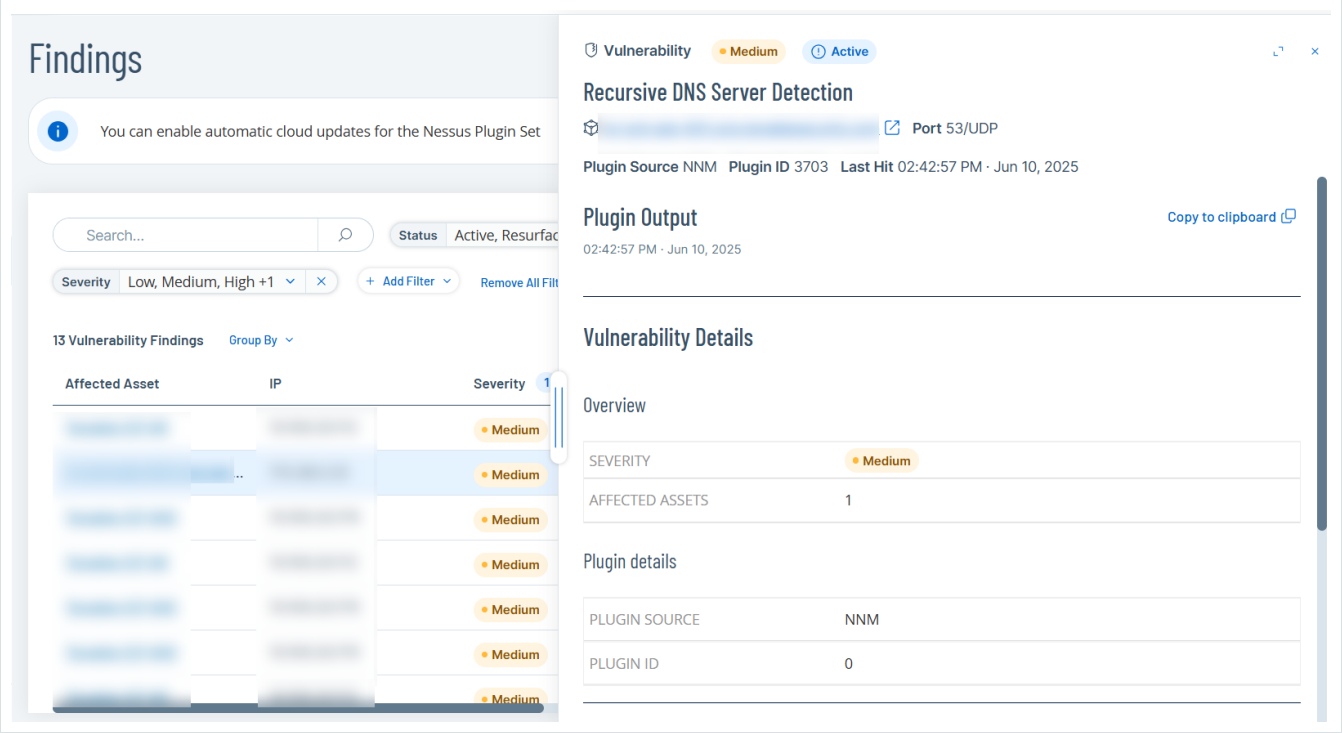
The Findings details comprises the following:

- Plugin Output
- Vulnerability Details
- Affected Asset Details

To view the findings details:

1. On the Findings page, click the link in the Affected Assets or the Plugin Name column.

   The Vulnerability Details panel appears.



You can view the following details:

- Severity
- Affected Assets
- Plugin Source
- Plugin ID
- Affected Asset details such as Name, Type, Criticality, Risk Score, IP Address, Purdue Level.

- To expand the Vulnerability Details panel, click the ⌜⌝ button in the upper-right corner.
- To close the panel, click the ✕ button in the upper-right corner.
- To view the complete asset details, in the Affected Asset section, click View Full Asset Details ⧉.

- OT Security opens a separate browser tab with the Inventory page with the single asset details.

Policy Violations

Use the Policy Violations page to view all the events associated with the same policy, source, and destination. Each finding on the page is an aggregation of multiple events resulting from the same policy hits sharing the same source and destination.

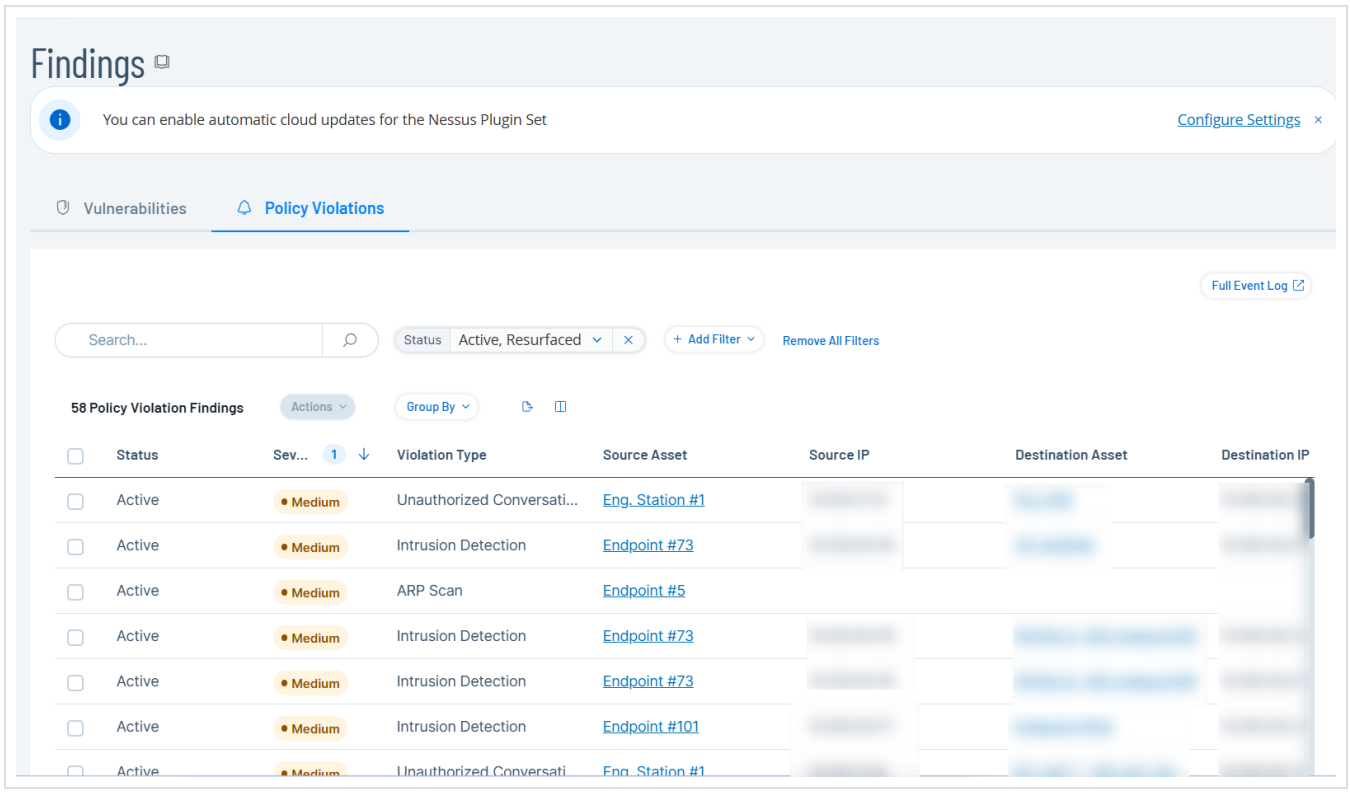
To access the Policy Violations page:

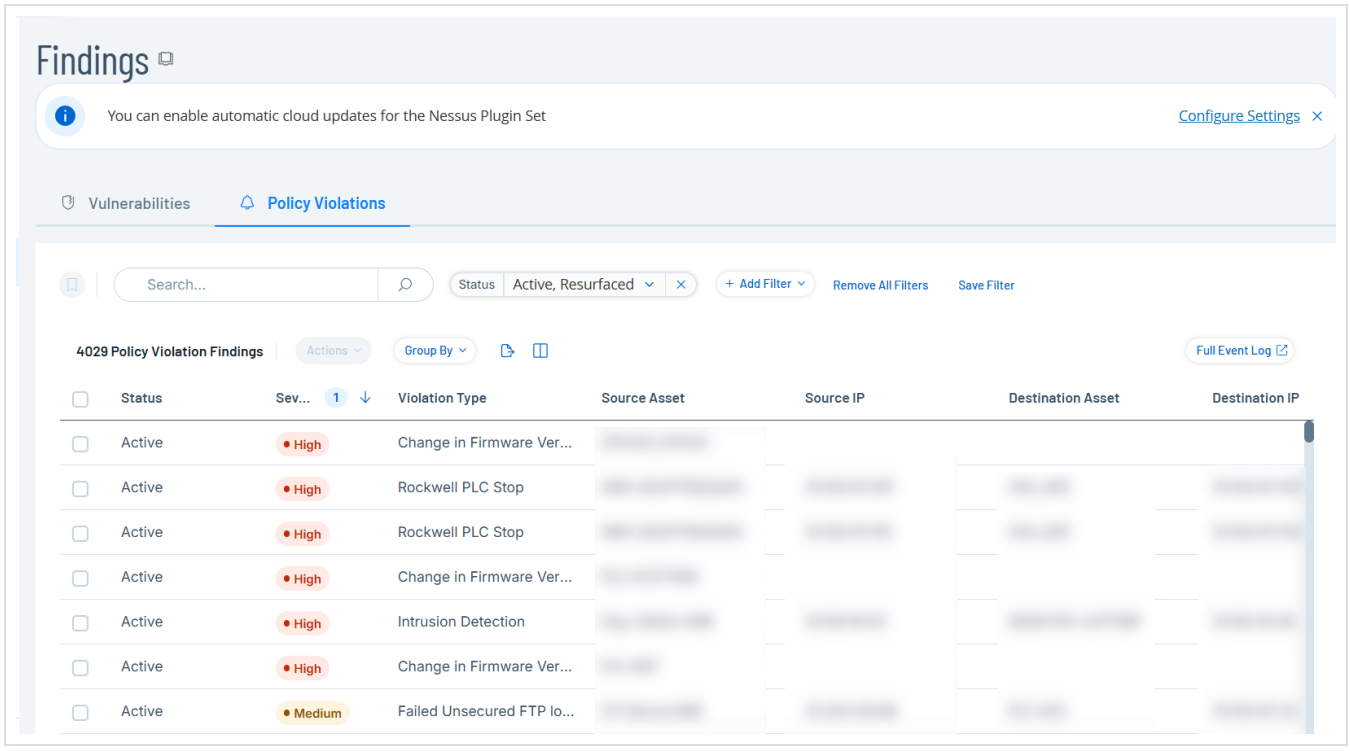
1. In the left navigation menu, click Risks > Findings.

   The Findings page appears.

2. Click the Policy Violations tab.

   The Policy Violations page appears with the list of events.





The Policy Violations tab includes the following details:

Column	Description
ID	The ID of the violation.
Status	The status of the violation: Active, Resurfaced, or Resolved.
Severity	The severity of the violation: High, Medium, or Low.
Violation Type	The type of violation. For example, Unauthorized Conversation and Intrusion Detection.
Violation Category	The category that the violation type belongs to.
Policy	The policy that caused the violation.
Plugin Name	The plugins associated with the violation.
Mitre ICS Tactics	The reason or "why" behind a specific Mitre Attack technique for Industrial Control Systems (ICS).
Mitre ICS Techniques	The method or the "how" an adversary achieves a tactical goal.
Source Asset	The asset where the violation originated.
Source IP	The IP address of the source asset.
Destination Asset	The asset where the violation terminated.
Destination IP	The IP address of the destination asset.
Protocol	The protocol associated with the violation.

Column	Description
First Hit	The time when the violation was first detected.
Last Hit	The time when the violation was last detected.
Active Hits	The number of events resulting in the violation.
Asset Type	The type of asset where the violation was detected.
Asset Critical	The criticality of the asset.
Asset Vendor	The vendor associated with the asset.
Asset Family	The family that the asset belongs to.
Asset Tags	The tags associated with the asset.
Purdue Level	The purdue level of the asset.
Asset Location	The region where the asset is located.
Resolved On	The date when the violation was resolved.
Resolved By	The user who resolved the violation.
Comment	The comments added by the user when resolving the violation.

3. (Optional) You can do the following on the Violations page:
    - Customize columns as described in Customize Tables.
    - Filter the findings table. See Filter tables.
    - Export the data in the CSV format.

Actions menu

Resolve a finding

- To resolve a finding:

  a. Select the row of the finding and click Actions > Resolve.

     The Resolve panel appears.

  b. Type a comment for resolving the finding.

  c. Click Save.

     OT Security resolves the finding and the Plugin Details panel shows the status as Resolved.

     > Note: If the event reoccurs, OT Security reopens the finding and status appears as Resurfaced.

Exclude from policy

- To exclude the finding from a policy:

  a. Select the row of the finding and click Actions > Exclude from Policy.

     The Exclude from Policy panel appears.

  b. Select the Exclude Conditions.

     > Note: The exclude conditions are based on the last and most recent event.

  c. Provide the Exclusion Description.

  d. Click Save.

     OT Security excludes the most recent event from the policy.

Download last capture file

- To download the last capture file:

    a. Select the row of the finding and click Actions > Download Last Capture File.

    OT Security downloads the capture file for the most recent event.

Plugin Details

To view the details of the plugin for the finding:

1. In the Policy Violations tab, click the row of the finding to view its plugin details.

    The plugin details panel appears with the violation details from the OT Security plugin page.

    The panel shows the details of the violation in four separate tabs: Details, Source, Destinations, and Policy.

Search for Events

To search for specific events that caused the violation:

a. To find the events for a specific finding, click Copy Finding ID.

b. To go to the Events page, click the Full Event Log link.

The All Events page appears.

c. In the Search box, paste the Finding ID that you copied earlier.

OT Security lists the events for the specific finding.

Compliance Dashboard

Required OT Security User Role: Administrator, Supervisor, Security Manager, Security Analyst, Site Operator, Read Only

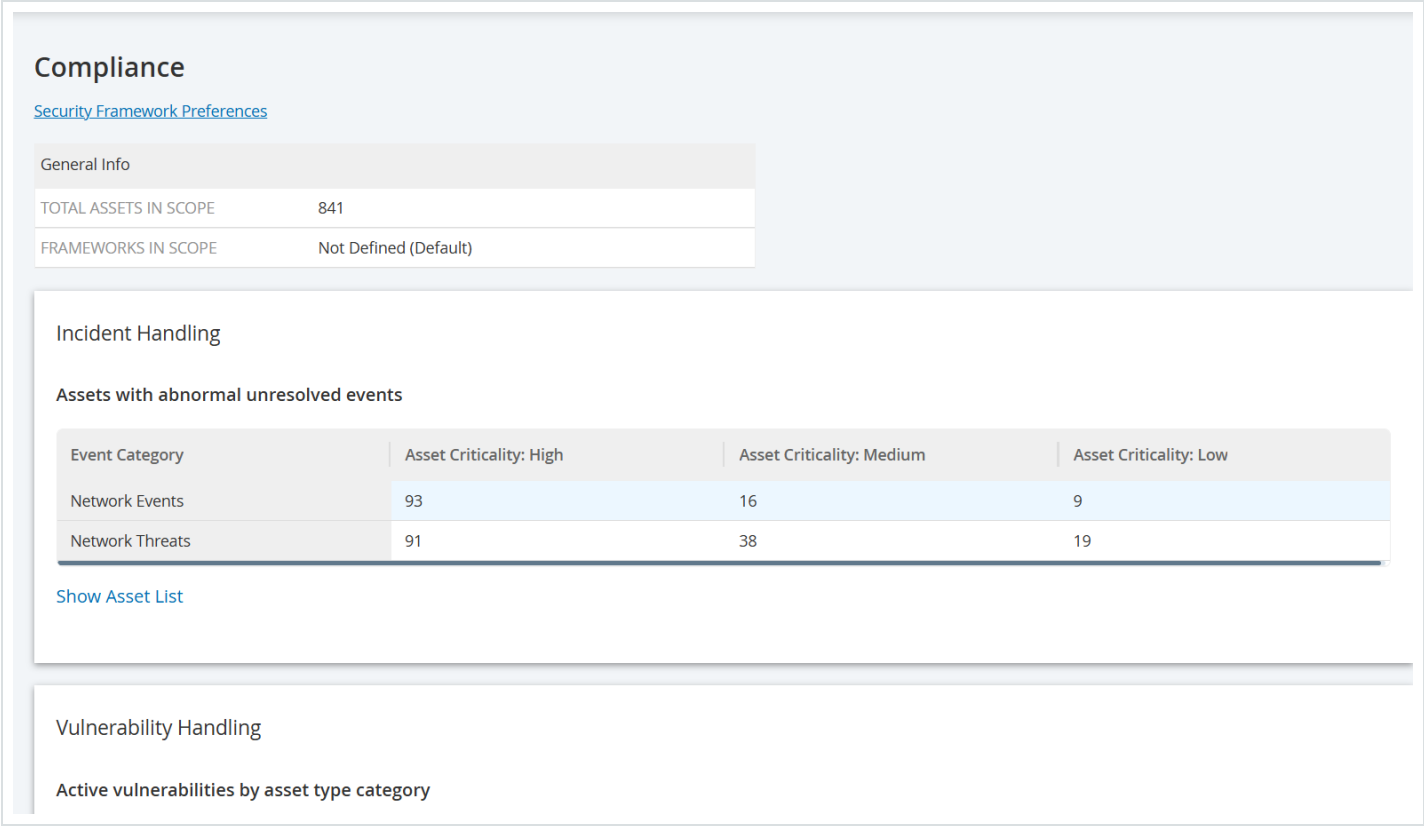
Compliance to security frameworks such as NIS 2 Directive, ISO 27001 Controls are now mandatory for most of the critical infrastructure companies to clear audit checks.

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.



To view the compliance dashboard:

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

   The Compliance dashboard appears.

2. In the left navigation bar, click Risks > 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	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. 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. 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.
Vulnerability Handling	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. 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. Note: To view all high-risk assets with active critical vulnerabilities, click Show Asset List. To close the assets list, click Hide Asset List.
Configuration & Change Management	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

Widget	Description
	thereby ensuring operational continuity and quick recovery during service disruptions. 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.
External Exposure Risk	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.
Insecure Cryptography	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. Note: To view all high-risk assets with insecure authentication events, click Show Asset List. To close the assets list, click Hide Asset List.
Insecure Communication Monitoring	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. Note: To view all high-risk assets with insecure authentication events, click Show Asset List. To close the assets list, click Hide Asset List.
Risk Assessment	Provides an overview of assets at risk by their criticality. This data helps

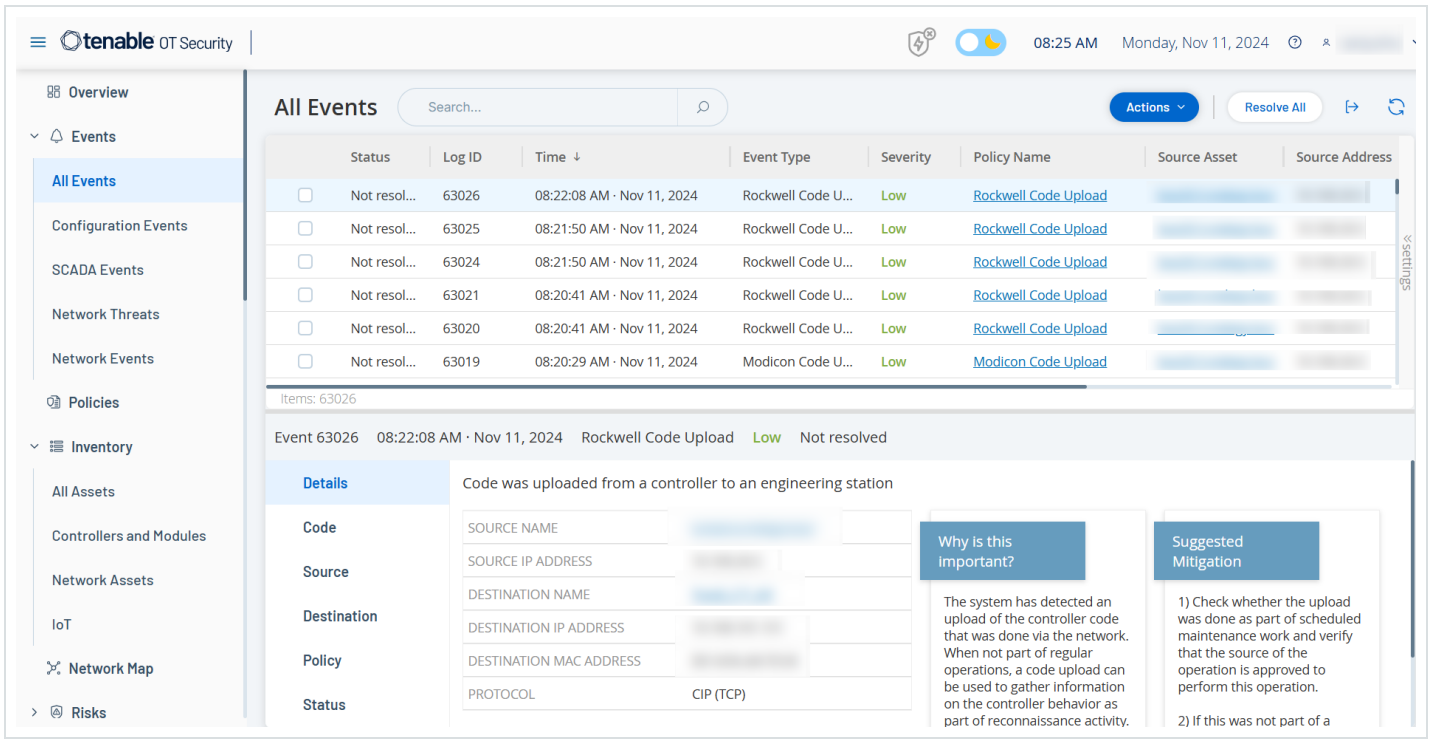
Widget	Description
	you assess and manage risks associated with OT, network, and IoT assets and proactively identify and mitigate potential threats. Note: To view all assets that are at high risk, click the Show Asset list link. To close the assets list, click Hide Asset List.

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



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 the 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, and Policy Name. You can also sort, filter, and search the event lists. For more information about the customization features, seeCustomize 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.

Parameter	Description
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	The IP or MAC of the asset that initiated the Event.

Parameter	Description
Address	
Destination Asset	The name of the asset that was affected by the Event. This field is a link to the Asset listing.
Destination Address	The IP or MAC of the asset that was affected by the Event.
Protocol	When relevant, this shows the protocol used for the conversation that generated this Event.
Event Category	Shows the general category of the Event. Note: On the All Events screen, Events of all types are shown. Each of the specific Event screens shows only Events of the specified category. The following is a brief explanation of the Event categories (for a more detailed explanation see Policy Categories and Sub-Categories): • Configuration Events – this includes two sub-categories • Controller Validation Events – These policies detect changes that take place in the controllers in the network. • Controller Activity Events – Activity Policies relate to the Activities that occur in the network (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.

Parameter	Description
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.)

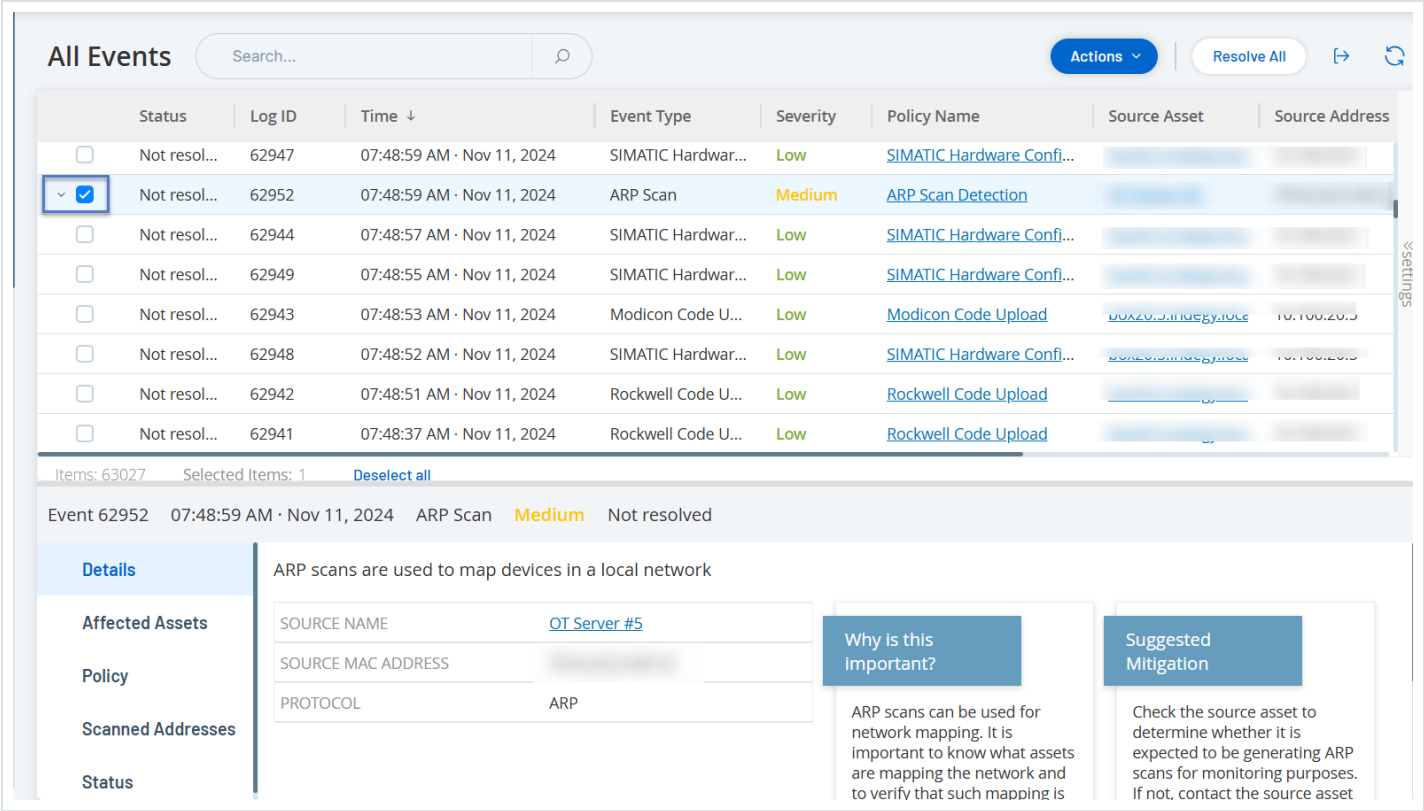
- Header – shows an overview of essential info about the Event.
- Details – gives a brief description of the Event as well as an explanation of why this information is important and suggested steps that should be taken to mitigate the potential harm caused by the Event. In addition, it shows the source 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.



Create Policy Exclusions

> Required OT Security User Role: Administrator, Supervisor, Security Manager

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:

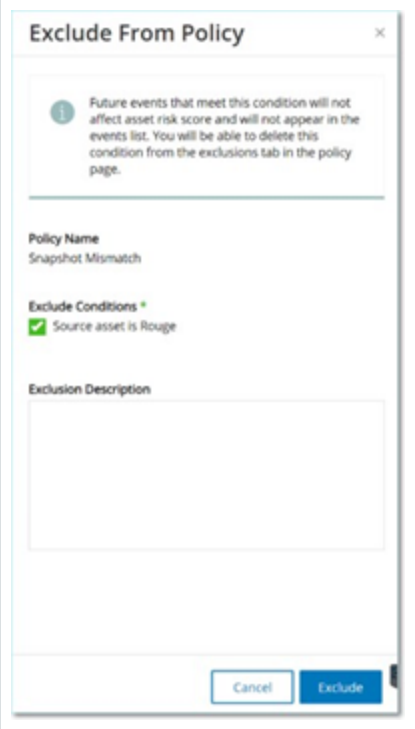
1. In the relevant Events page, (Configuration Events, SCADA Events, Network Threats, or Network Events), select the event for which you want to create an exclusion.
2. In the header bar, click Actions or right-click the event).

   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”.



Note: The set of conditions that can be excluded differ depending on the type of policy, see the following table.

5. (Optional) In the Exclusion Description box, you can add a comment about the exclusion.
6. 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)	• Source asset • Source IP • Destination asset • Destination IP
Controller Validation	Change in Key State	Source asset
	Change in Controller State	Source asset
	Change in FW Version	Source asset
	Module Not Seen	Source asset
	Snapshot Mismatch	Source asset
Network	Asset Not Seen	Source asset
	Change in USB Configuration	• Source asset • USB Device ID

Policy Category	Event Type	Excludable Conditions
	IP Conflict	• MAC Addresses • IP Address
	Network Baseline Deviation	• Source asset • Source IP • Destination asset • Destination IP • Protocol
	Open Port	• Source asset • Source IP • Port
	RDP Connection	• Source asset • Source IP • Destination asset • Destination IP
	Unauthorized Conversation	• Source asset • Source IP • Destination asset • Destination IP

Policy Category	Event Type	Excludable Conditions
		• Protocol
	FTP Log In (Failed and Successful)	• Source asset • Source IP • Destination asset • Destination IP
	Telnet Log In (Attempt, Failed and Successful)	• Source asset • Source IP • Destination asset • Destination IP
Network Threat	Intrusion Detection	• Source asset • Source IP • Destination asset • Destination IP • SID
	ARP Scan	• Source asset • Source IP
	Port Scan	• Source asset • Source IP

Policy Category	Event Type	Excludable Conditions
SCADA	Modbus Illegal Data Address	• Source asset • Source IP • Destination asset • Destination IP
	Modbus Illegal Data Value	• Source asset • Source IP • Destination asset • Destination IP
	Modbus Illegal Function	• Source asset • Source IP • Destination asset • Destination IP
	Unauthorized Write	• Source asset • Destination asset • Tag Name
	IEC60870-5-104 StartDT IEC60870-5-104 StopDT	• Source asset • Source IP • Destination asset

Policy Category	Event Type	Excludable Conditions
		• Destination IP
	IEC60870-5-104 function code-based events	• Source asset • Source IP • Destination asset • Destination IP • COT
	DNP3 events	• Source asset • Source IP • Destination asset • Destination IP • Source DNP3 address • Destination DNP3 address

Download Individual Capture Files

Required OT Security User Role: Administrator, Supervisor, Security Manager, Security Analyst

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). 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

Required OT Security User Role: Administrator, Supervisor, Security Manager

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.

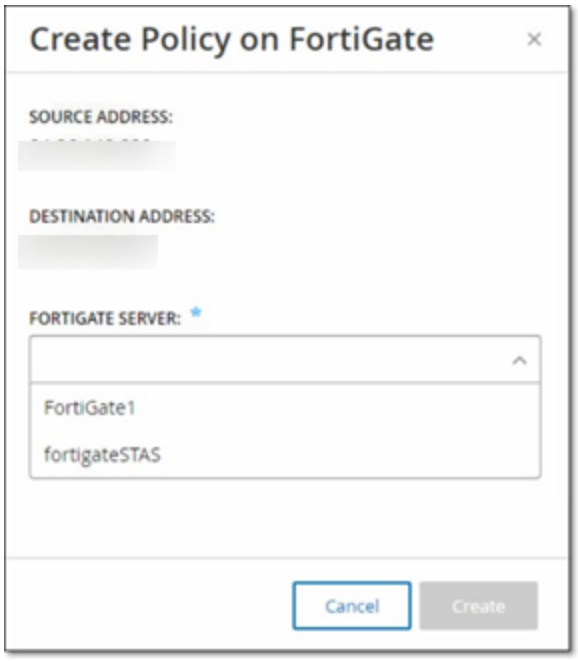
Before you suggest FortiGate policies, you need to set up the integration for your FortiGate Firewall server with OT Security. See FortiGate Firewalls.

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.



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.

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, and involved assets. See Conversations

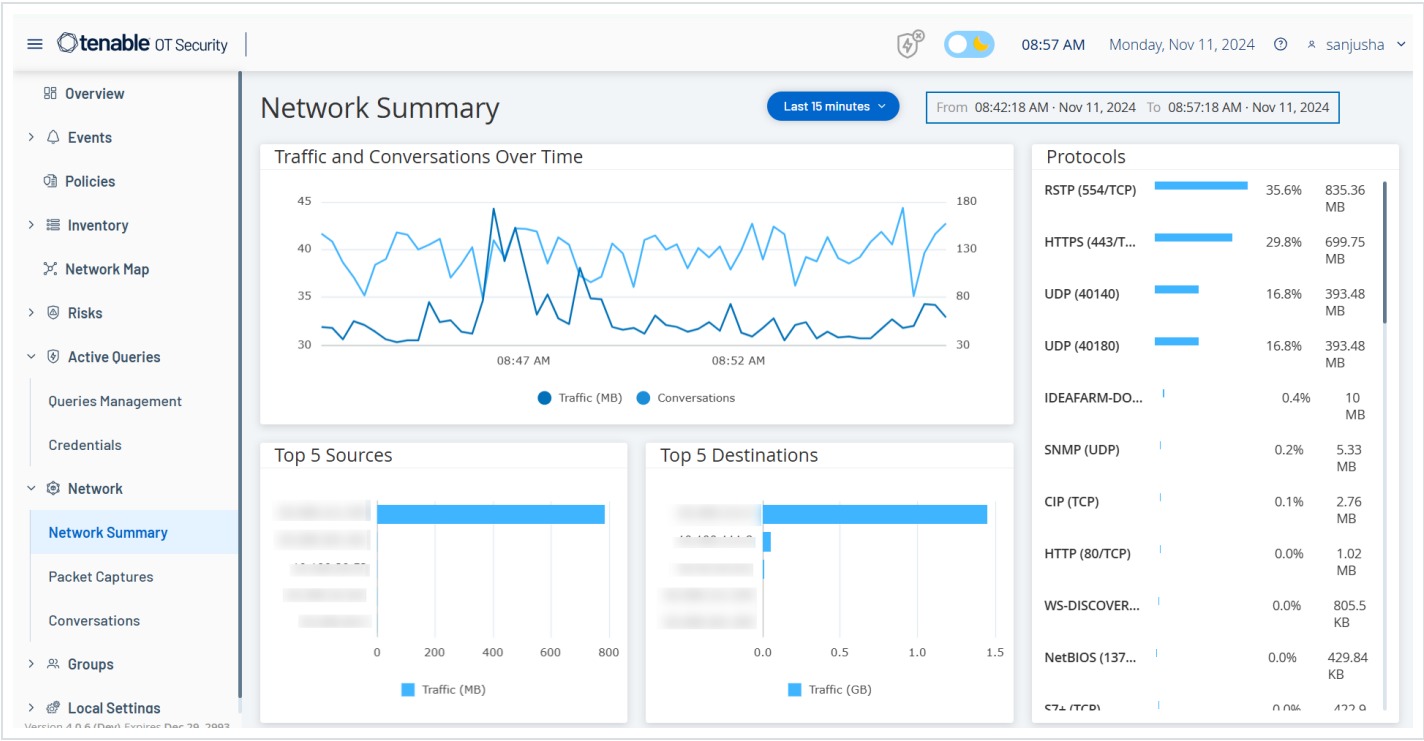
To access the Network page:

1. In the left navigation pane, select Network.

   The Network Summary page appears.

Network Summary

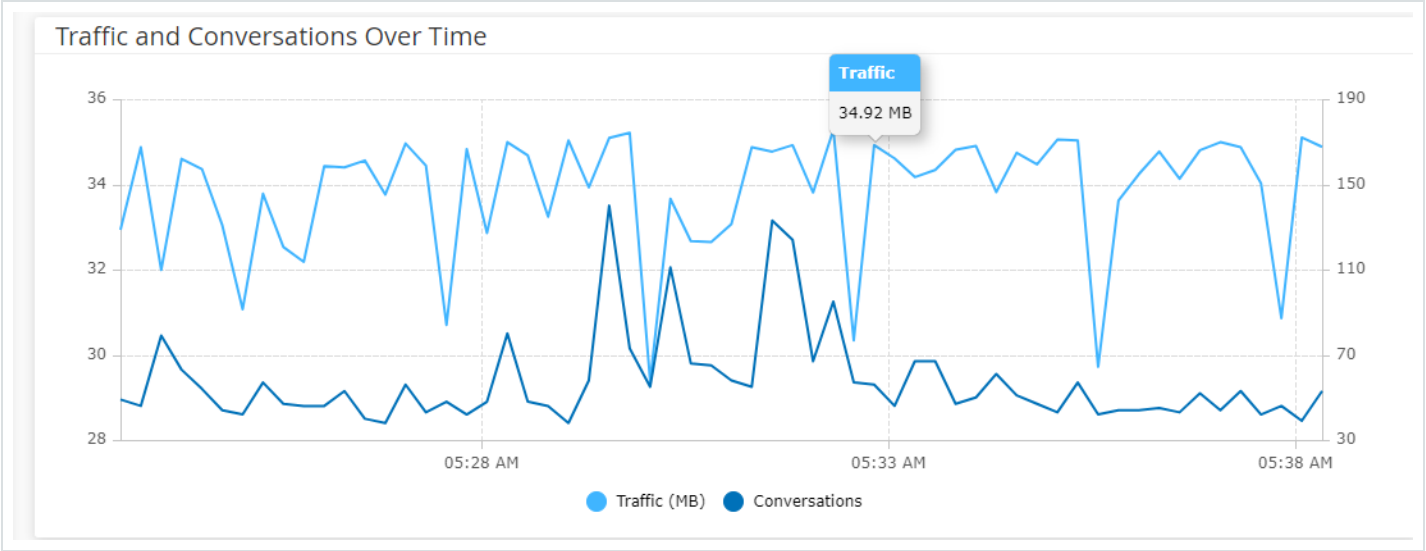
The Network Summary page shows visual graphs that summarize the network activity. You can view the data for a specific timeframe.



Interact with the following widgets to view additional details.

Traffic and Conversations over Time

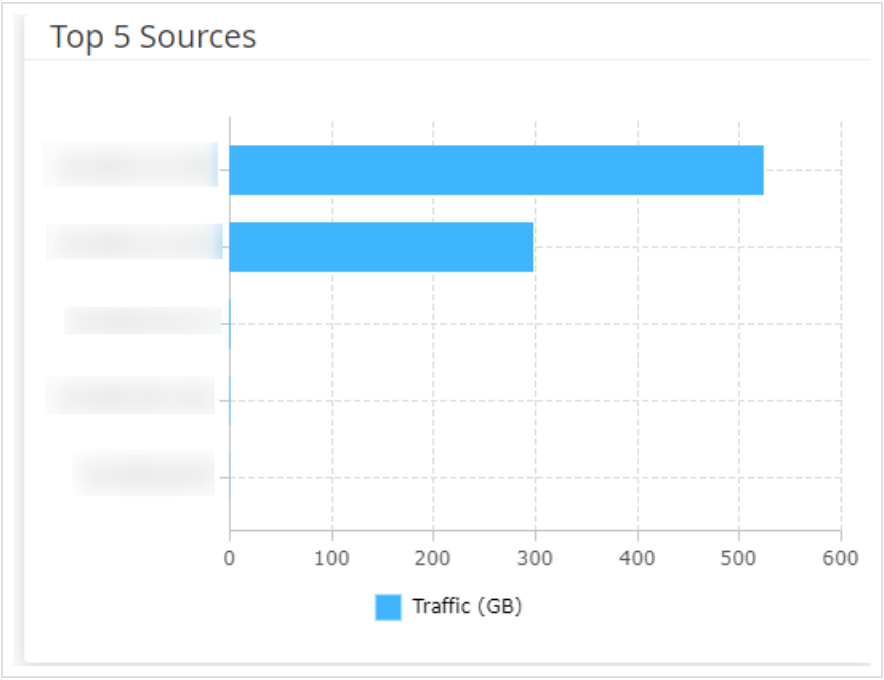
A line graph displays the volume of traffic (measured in KB/MB/GB) and the number of conversations in the network over time. The legend key appears at the top of the graph. Hover over a point on the graph to display specific data about the traffic and conversations during that time segment.



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.

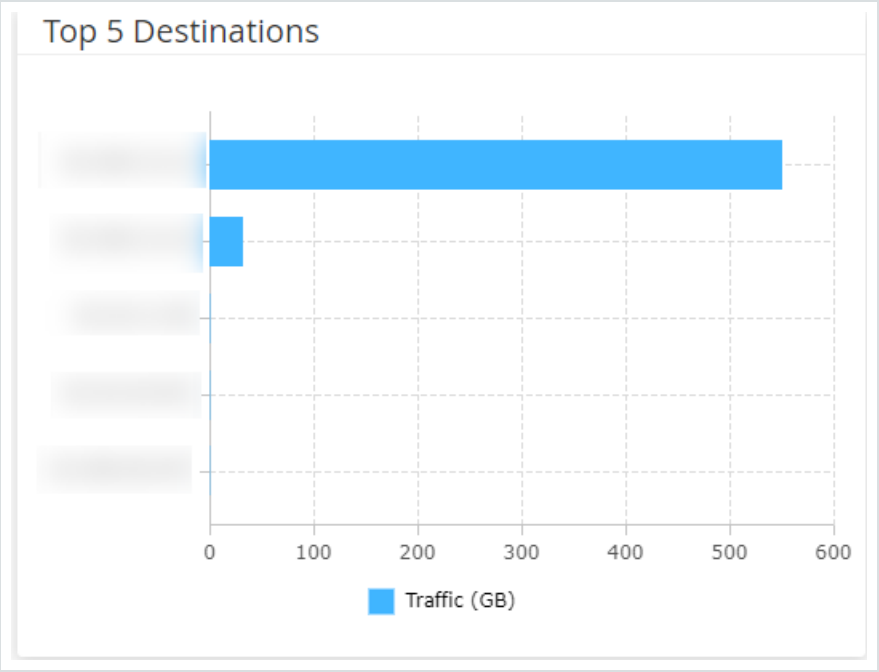
Top 5 Sources

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.



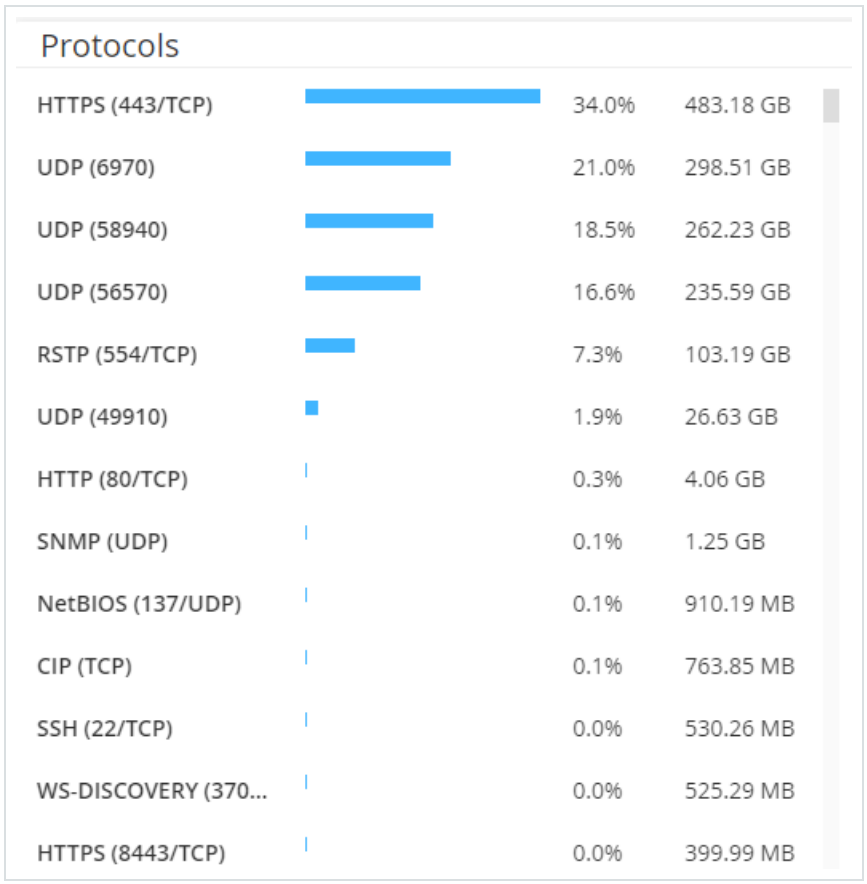
Top 5 Destinations

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.

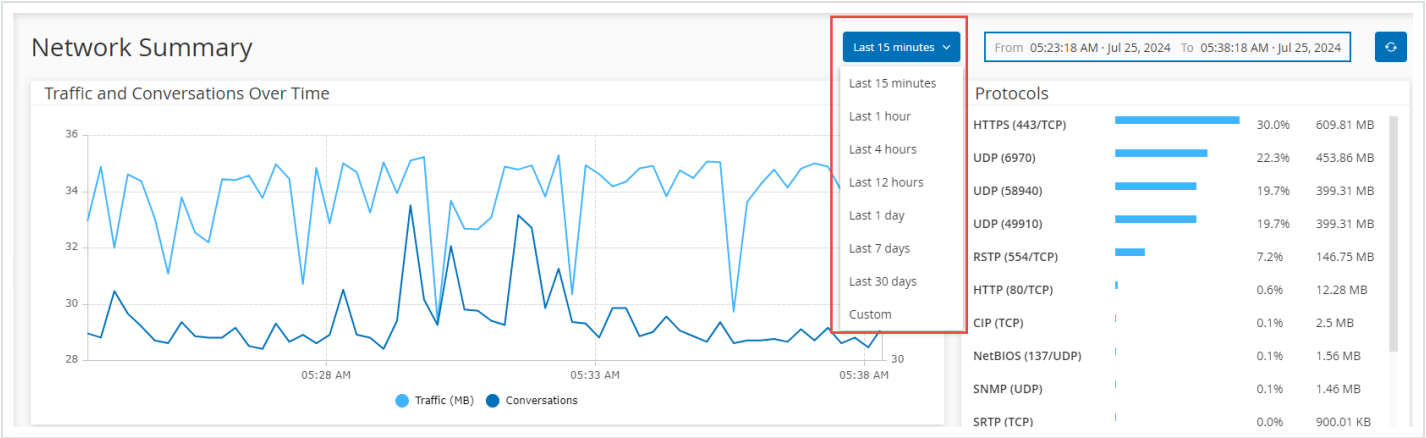
Set the Timeframe

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.
- 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 `local`.
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.

> 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

> Required OT Security User Role: Administrator, Supervisor, Security Manager, Security Analyst

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:

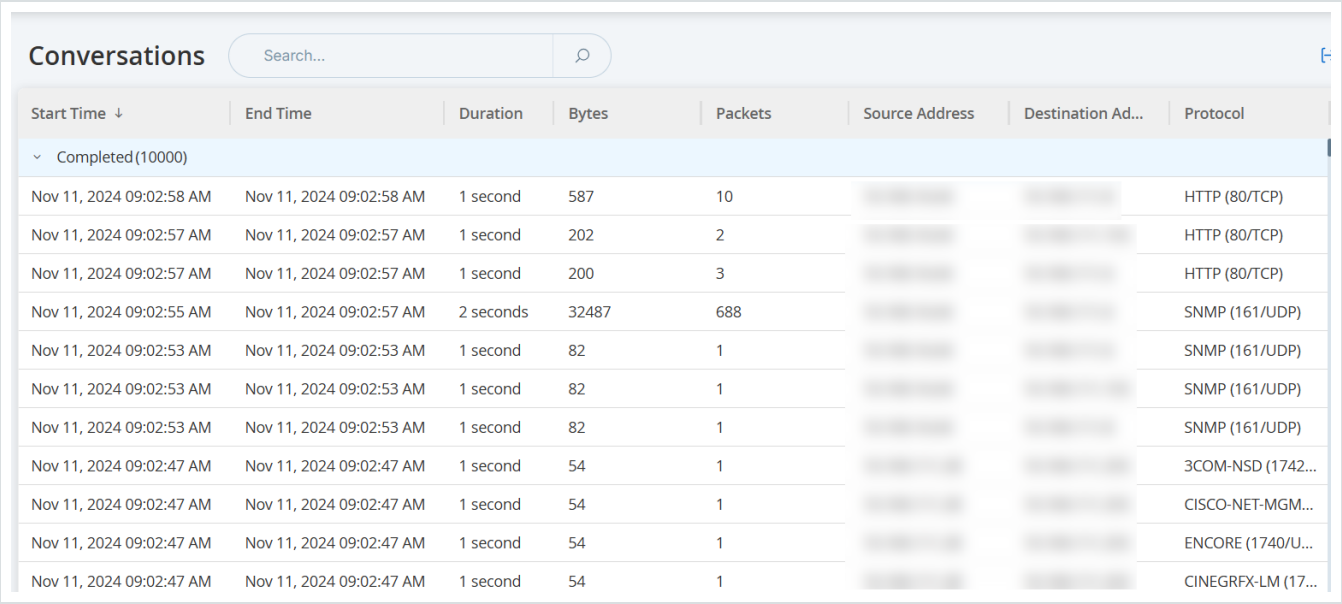
- Search – Use the Search box to search for specific conversations by providing identifying information.
- Export – Use the Export button to export all data from the Conversations tab onto your local machine as a `.csv` file.

> 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.



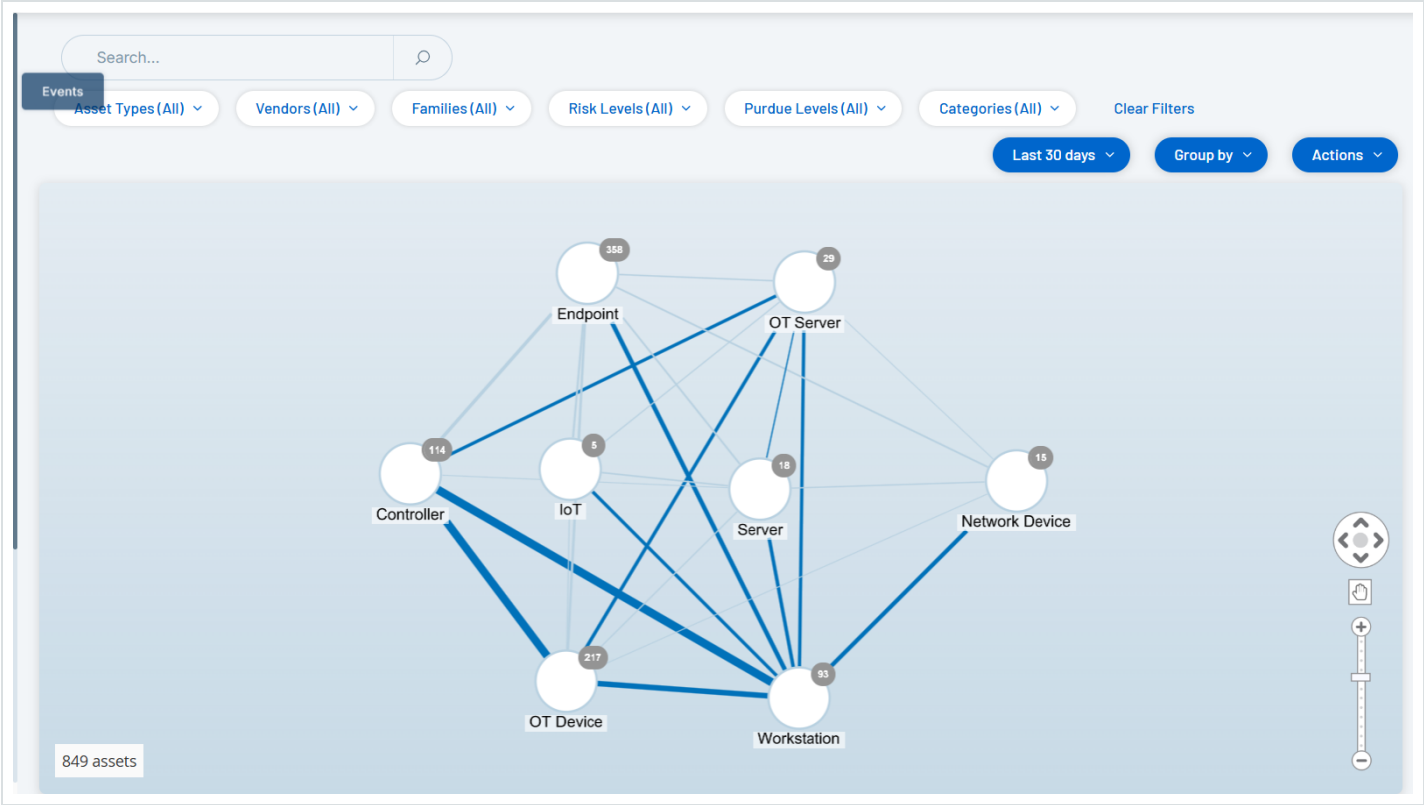
   The Conversations page includes the following details:

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.

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.

    The network map uses color codes to differentiate IT and OT protocols.

    - A gray line indicates IT-only protocols (for example, DNS, HTTP, and FTP).
    - A blue line indicates the presence of OT protocols (for example, HTTP, MODBUS, CIP, and FTP).
- 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.

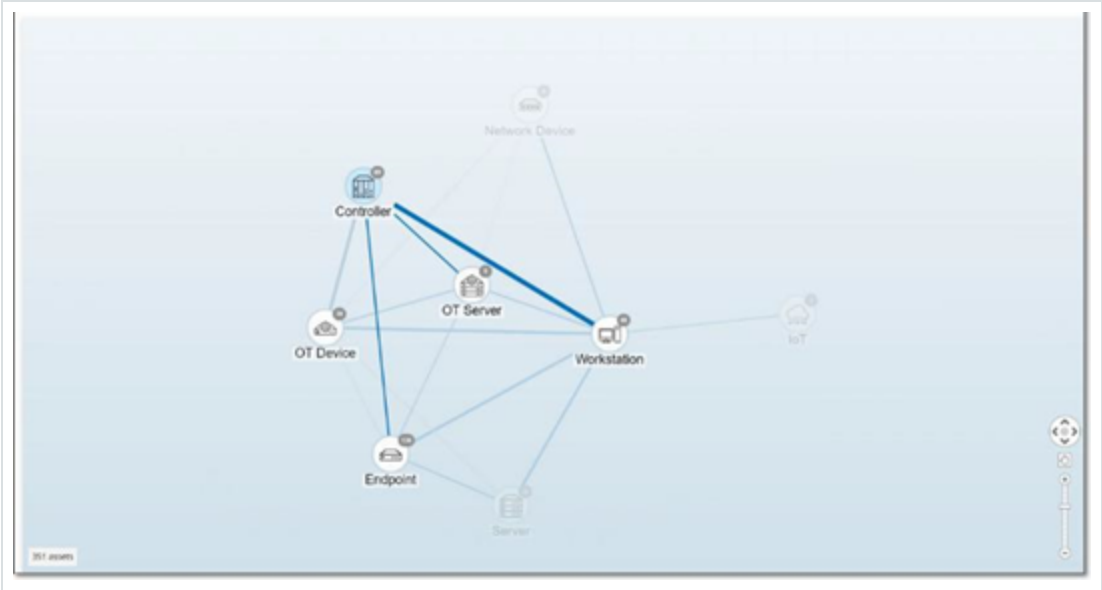
When the map displays groups by Asset Type (default), the drill-down hierarchy is as follows: Asset Type > Vendor > Family > Individual Asset.

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:

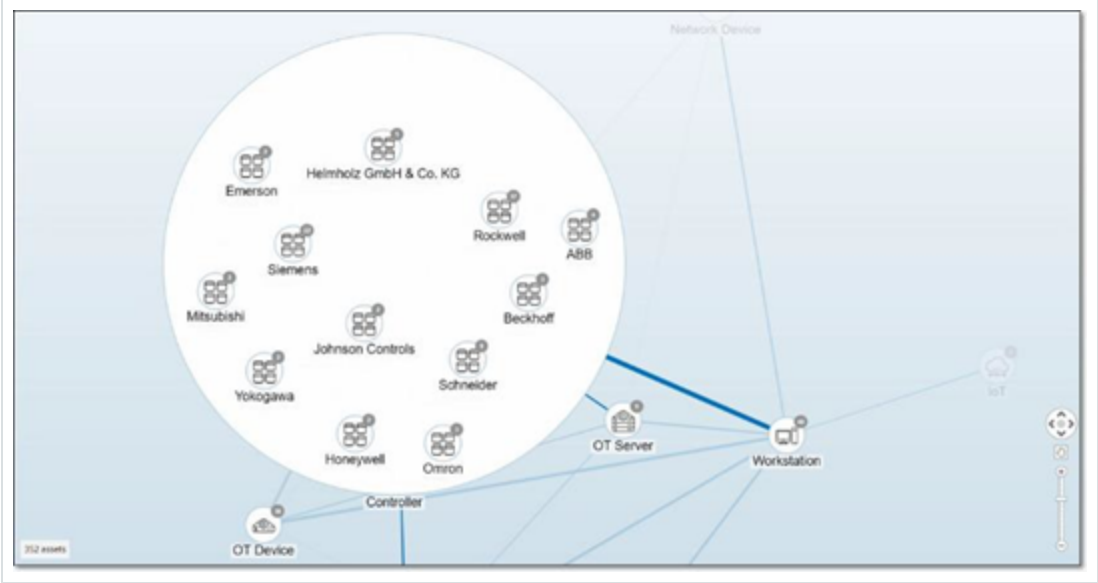
To drill down to an Asset Type Group:

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

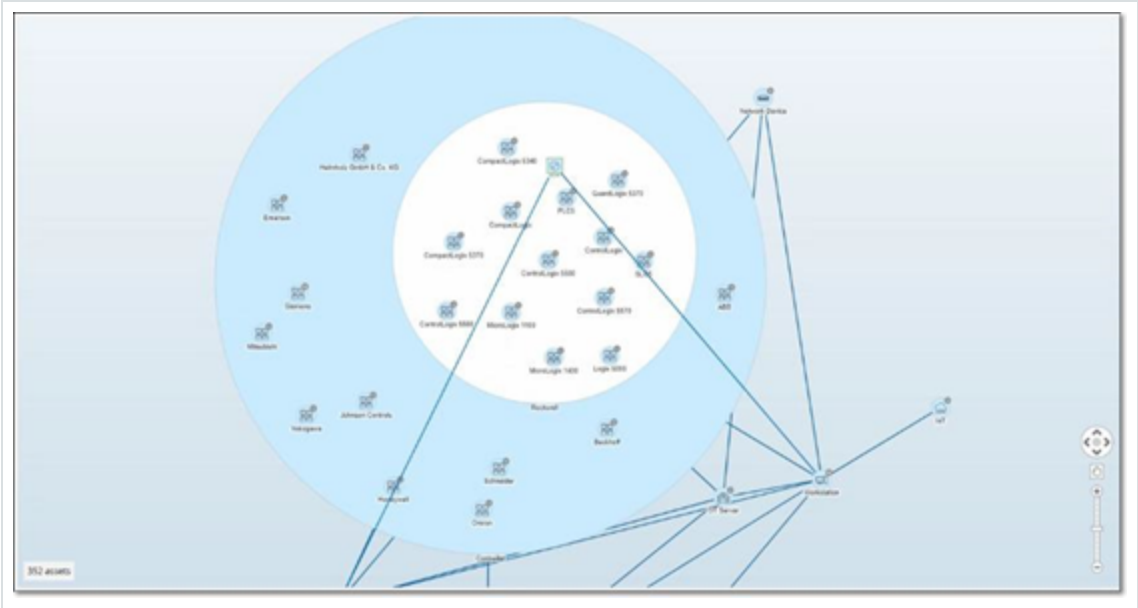


2. Double-click on the group icon that you want to drill down into (for example, Controller).

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

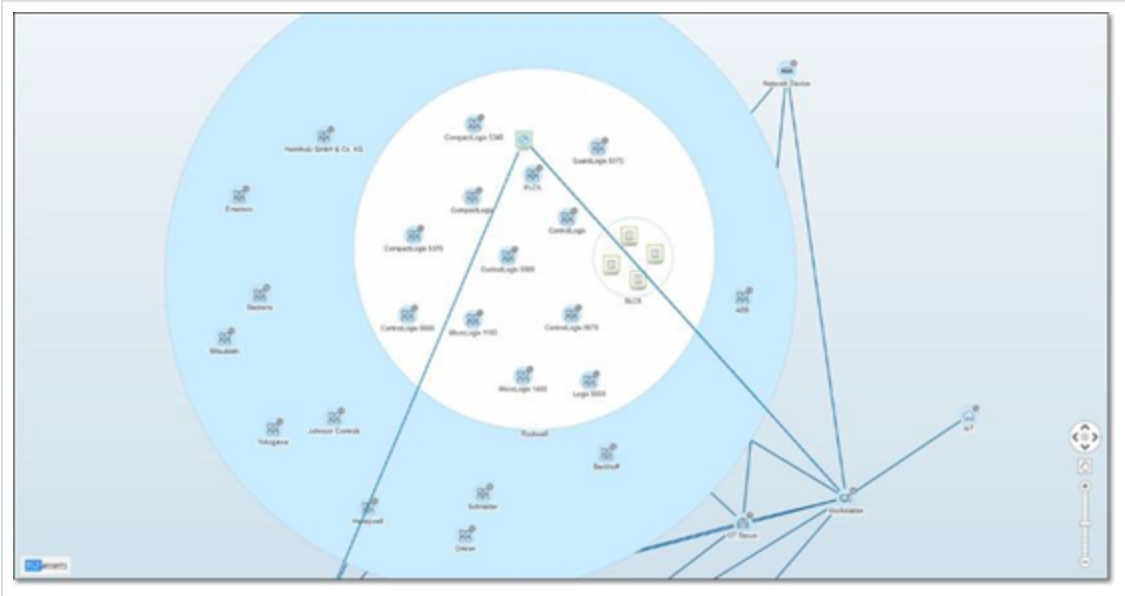


3. To drill down further, click a Vendor group (for example, Rockwell).



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.

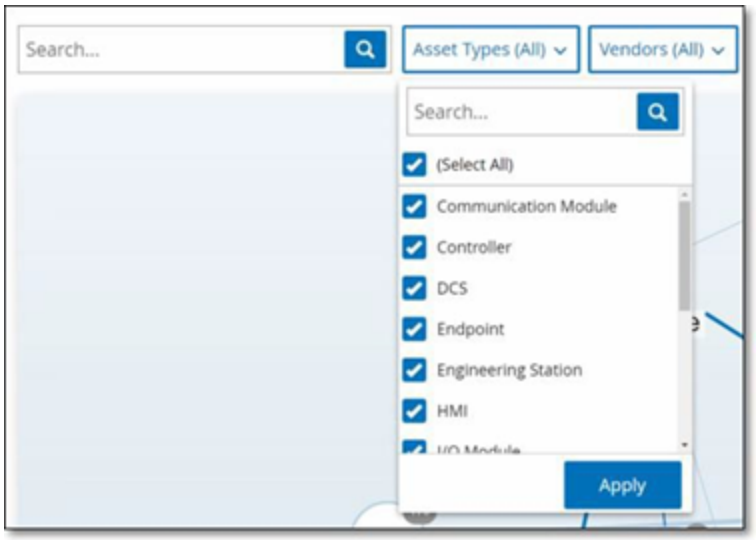
To remove all grouping:

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

   The map shows all single assets without any grouping.

Apply 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.

View 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.

Data Collection

The Data Collection section in OT Security includes the following configuration pages:

- Policies
- Manage Active Queries
- Data Sources

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, and criticality.
- 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, and department.
- 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), or the manufacturer (for example, Rockwell allowed protocols).

- Schedule Groups – Group several time ranges as a schedule group that has a certain common characteristic. For example, work hours and weekends.
- 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, and Modicon online session.

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, Schedule	The controller changed from one operational state to another. For example, running, stopped, and test.
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 Telnet login	Source, Destination, Schedule	OT Security considers Telnet as an unsecure 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 (ICS Attacks, Denial of Service, and Malware) and sub-categories (ICS Attacks - Stuxnet and ICS Attacks – Black Energy). 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, Destination Asset, Schedule	Detects SYN scans (network reconnaissance activity) that are run in the network to detect open (vulnerable) ports. The policy applies to communication from an asset in the Source Asset Group to an asset in the Destination Asset Group during the specified time range.

SCADA Event Types

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

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

Event Type	Policy Conditions	Description
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 and Warm/Cold Restart. Also detects errors originating from internal indicators such as unsupported function codes and parameter errors.

Enable or Disable Policies

Required OT Security User Role: Administrator, Supervisor, Security Manager

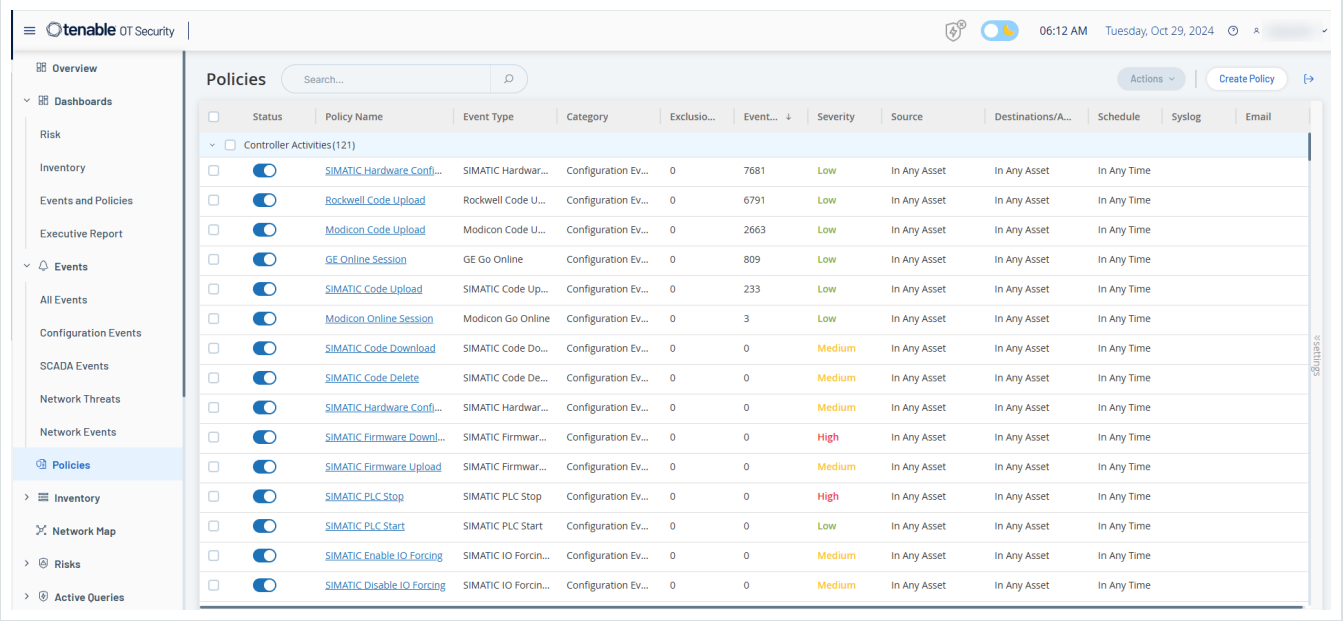
You can enable or disable any configured policy in your system (both pre-configured and user-defined). You can turn on/off individual policies or you can select multiple policies to turn on/off in a bulk process.

> 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.

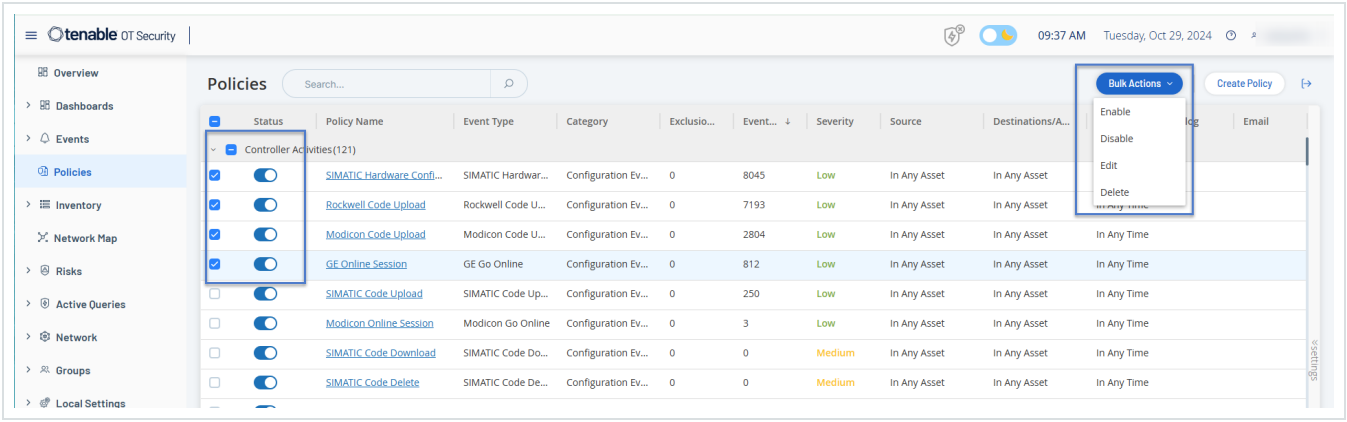


2. To enable or disable the policy, click the Status toggle next to the relevant policy.

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

> Required OT Security User Role: Administrator, Supervisor, Security Manager, Security Analyst, Site Operator, Read Only

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 and P2 for Network Events.
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.

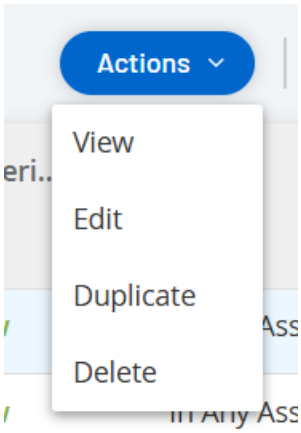
Syslog	The Syslog server (SIEM) that logs the events for this policy.
Email	The Email Group that sends the event notifications for this policy.
Sub Category	The sub-category classification of the event. The Configuration Events category comprises these sub-categories: Controller Activities and Controller 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

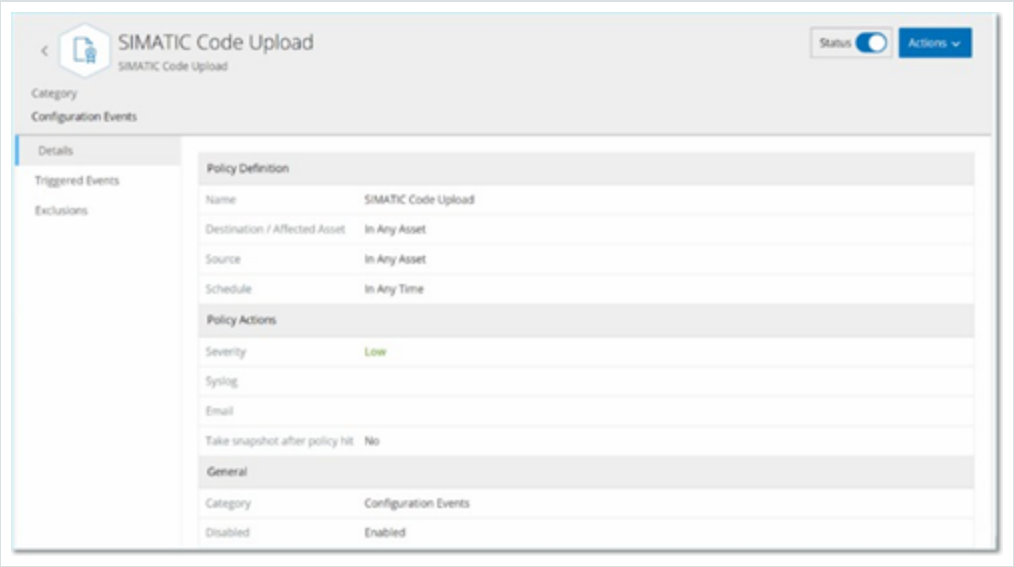
The Policy Details page for a policy shows additional details about the policy. This page lists all policy conditions and events that the policy triggered.

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

> Required OT Security User Role: Administrator, Supervisor, Security Manager

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.

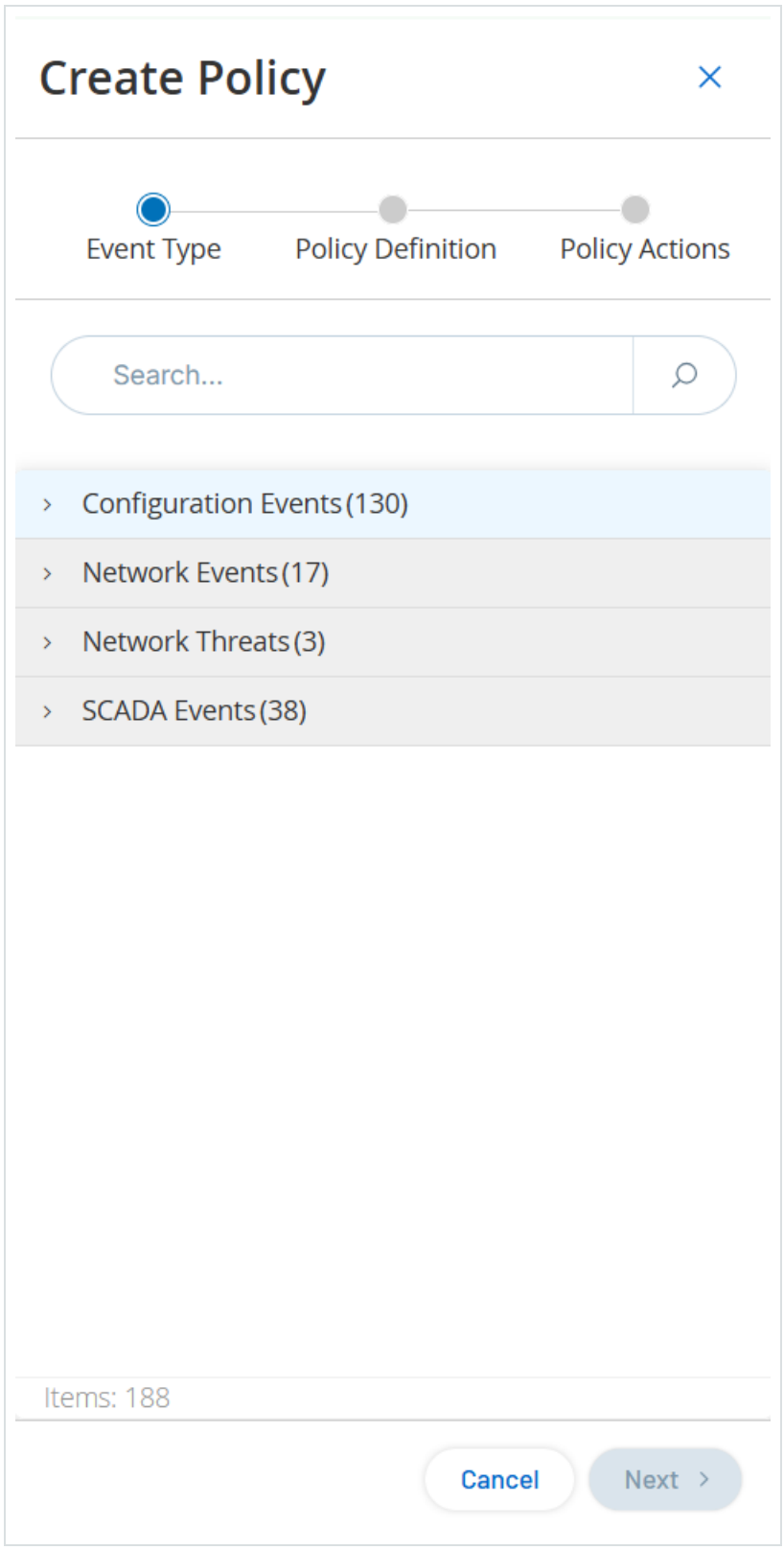
If you would like to create a new Policy with similar parameters to an existing Policy, you can Duplicate the original Policy and make the necessary changes, see section Create Policies.

> 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:

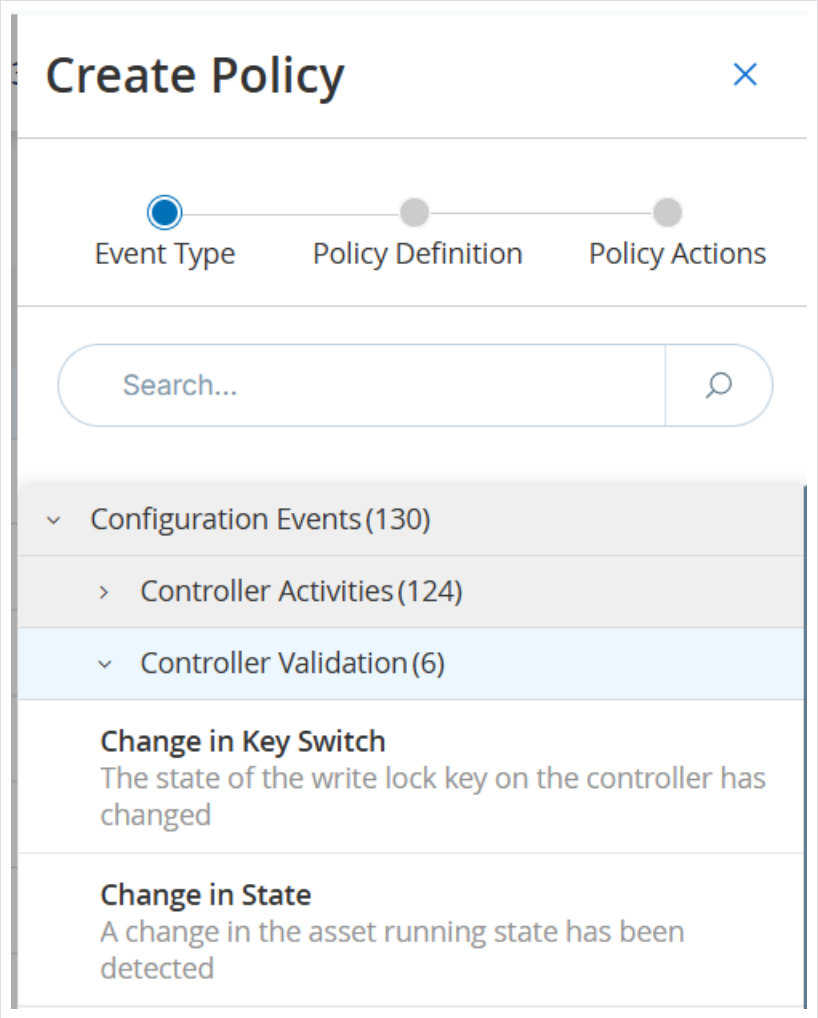
1. On the Policies screen, click Create Policy.

   The Create Policy wizard opens.

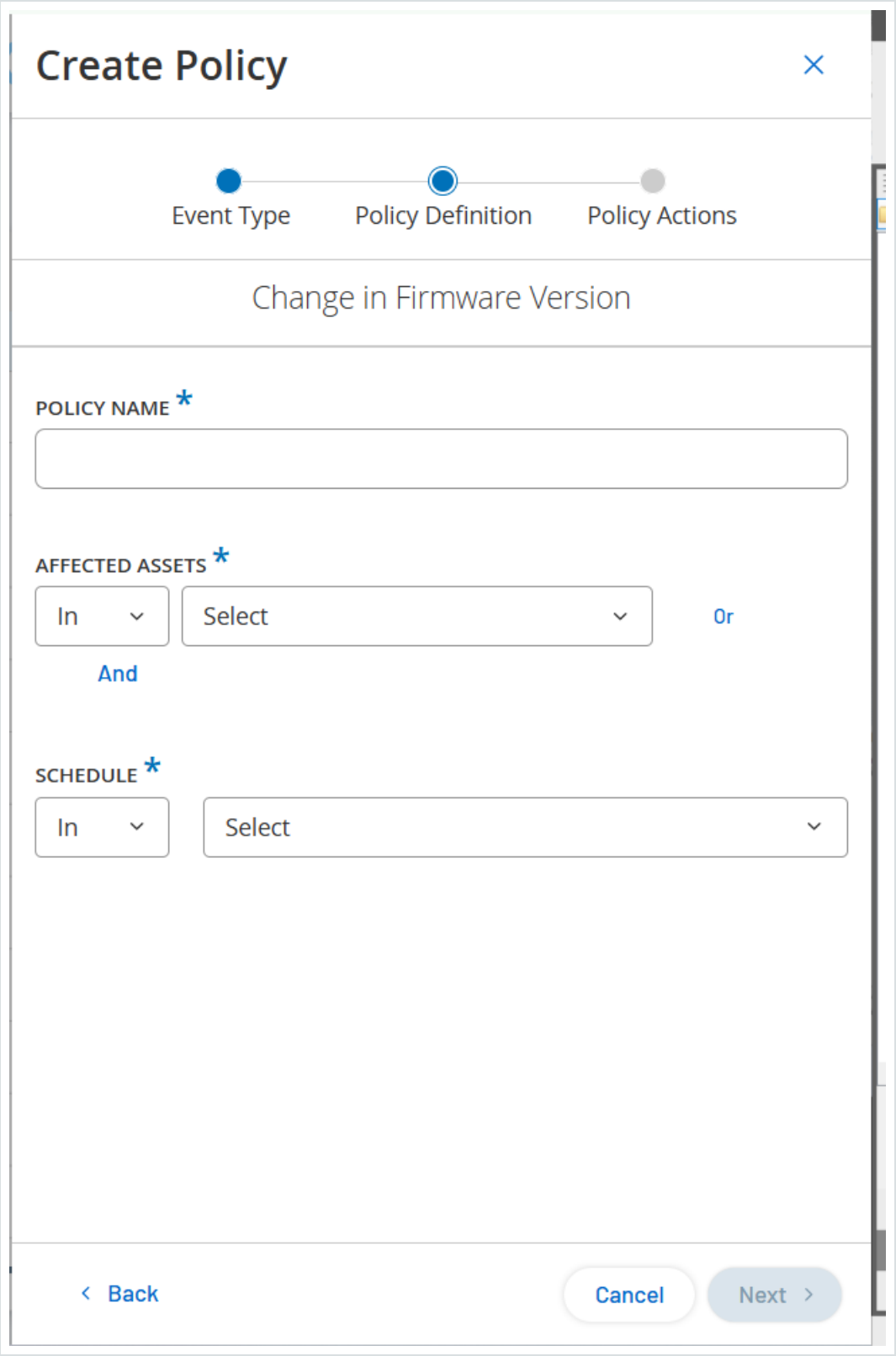

Create Policy
Event Type
Policy Definition
Policy Actions
Search...
Configuration Events (130)
Network Events (17)
Network Threats (3)
SCADA Events (38)
Items: 188
Cancel
Next

2. Click on a Policy Category to show the sub-categories and/or Policy Types.

   A list of all sub-categories and/or Types included in that category are displayed.



3. Select a Policy Type.


Create Policy
Event Type
Policy Definition
Policy Actions
Change in Firmware Version
POLICY NAME *
AFFECTED ASSETS *
In
Select
Or
And
SCHEDULE *
In
Select
Back
Cancel
Next

4. Click Next.

   A series of parameters for defining the Policy are displayed. This includes all relevant Policy conditions for the selected Policy Type.

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

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

6. For each parameter:

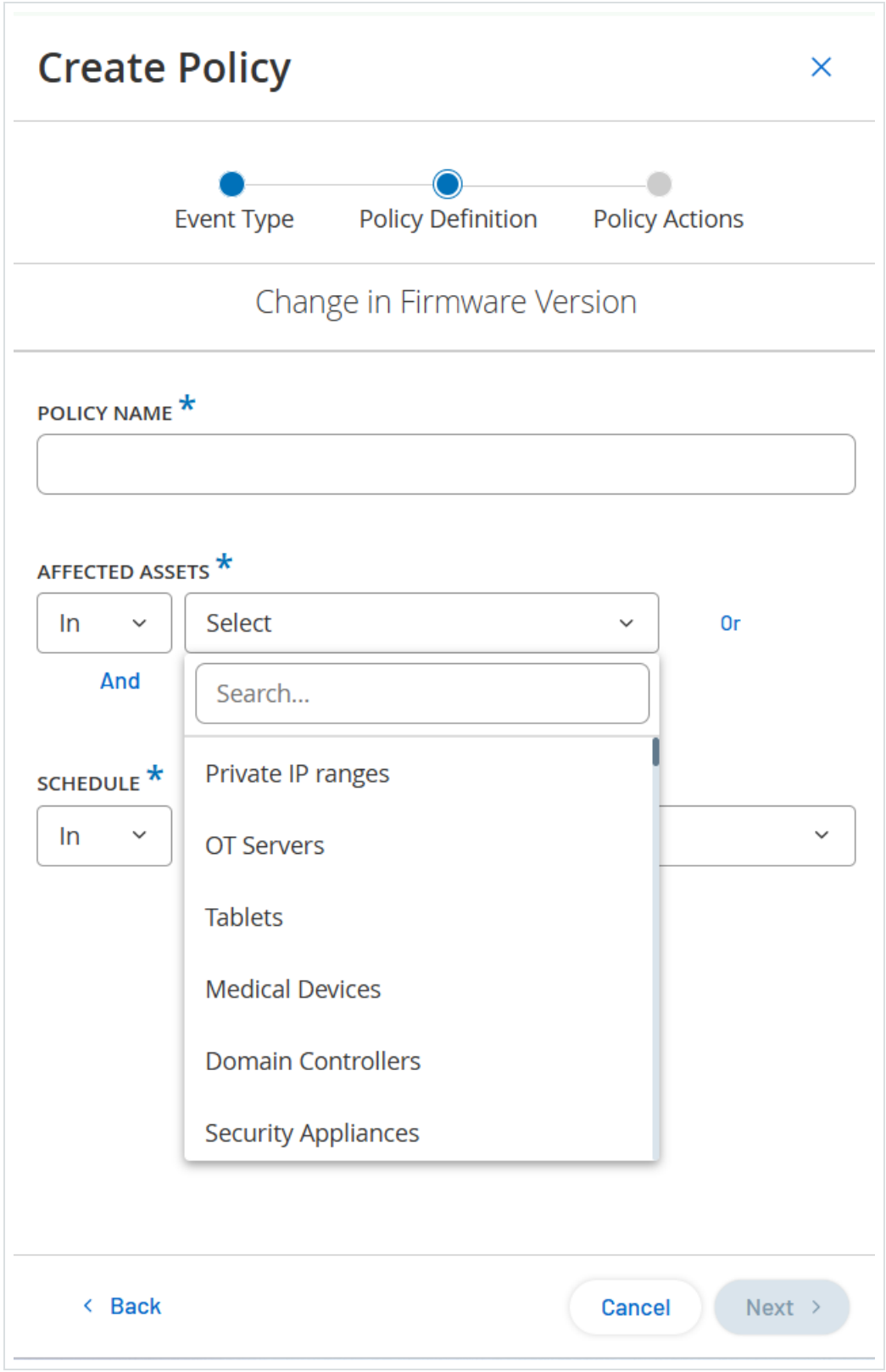
   > Caution: You cannot edit the Source and Destination asset groups for Intrusion Detection System (IDS) events.

   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.) appear.

      > Note: The available selection includes all asset groups except dynamic asset groups that have any of the following asset properties in their rule set:
      > - Risk Score
      > - Backplane Name
      > - Sources
      > - Tags
      > - Hardware State
      > - Lifecycle Status
      > - Replacement Product


Create Policy
Event Type
Policy Definition
Policy Actions
Change in Firmware Version
POLICY NAME *
AFFECTED ASSETS *
In
Select
Or
And
Search...
Private IP ranges
OT Servers
Tablets
Medical Devices
Domain Controllers
Security Appliances
SCHEDULE *
In
Back
Cancel
Next

c. Select the desired element.

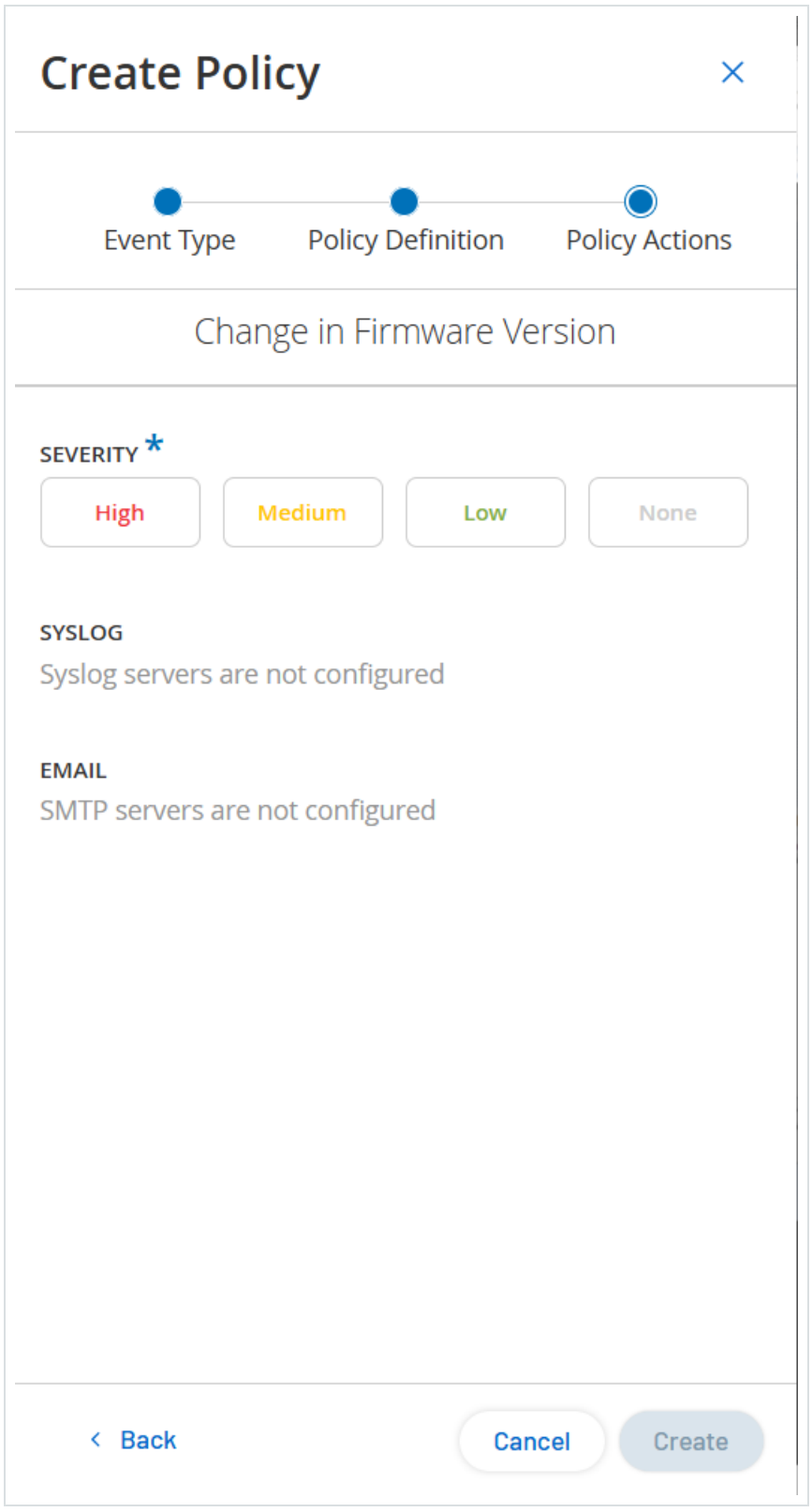
> Note: If the precise grouping to which you would like to apply the Policy does not exist, then you can create a new Group according to your needs, see Groups.

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.


Create Policy
Event Type
Policy Definition
Policy Actions
Change in Firmware Version
SEVERITY *
High
Medium
Low
None
SYSLOG
Syslog servers are not configured
EMAIL
SMTP servers are not configured
Back
Cancel
Create

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

   > Note: To add a Syslog server, see Syslog Servers.

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

    > 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

> Required OT Security User Role: Administrator, Supervisor, Security Manager

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.
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>*".
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.

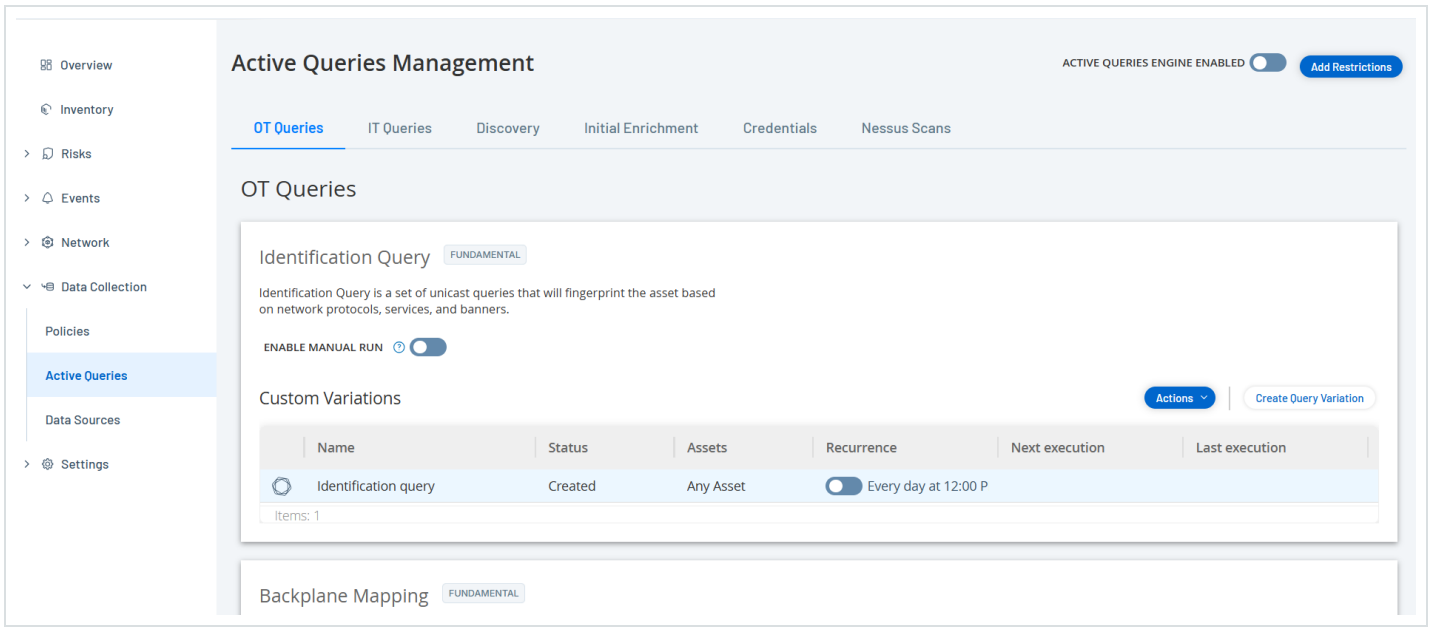
   A confirmation window appears.

6. In the confirmation window, click Delete.

   OT Security deletes the exclusion from the system.

Manage 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.

      Additionally, OT Security provides these options to leverage your SNMP query:

        - SNMP Ports State – Enable the SNMP Ports State toggle to obtain the network port status of the assets and enable the Fetch Neighbors toggle.

        - Fetch Neighbors – When you enable this option, OT Security collects the nearby devices' MAC and IP addresses via SNMP. To add these assets to your inventory, enable the Settings > Environment Settings > Network Definitions > Discover New Assets via SNMP.

    - 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.
  - Subnets Auto-Discovery – Detects subnets by querying network devices using SNMP. On the Inventory page, a Subnets column shows you which subnets the assets' IP addresses belong to. You can also filter assets within a specific subnet.
  - 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.
- OTD Scans – The technical instruction set created through the OT Discovery scan wizard. It defines the how: credentials, schedule, and restrictions.
- 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

> Required OT Security User Role: Administrator, Supervisor

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 Data Collection > Active Queries.

   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. (Only for Duplicated Networks) In the Relevant Sensors box, select the associated sensors.

13. Click Save.

    OT Security adds the query to the Custom Variations table.

    See Run a Query Variation.

Add Restrictions

Required OT Security User Role: Administrator, Supervisor

You can block queries from running on specific asset groups, such as IP ranges, OT servers, Tablets, Medical Devices, and Domain Controllers. You can also apply restrictions on specific protocols (clients).

Note: Restrictions do not apply to the Discovery (ICMP) and Open Ports Check (in Asset Enrichment) queries.

To add restrictions:

1. Go to Data Collection > Active Queries.

   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.

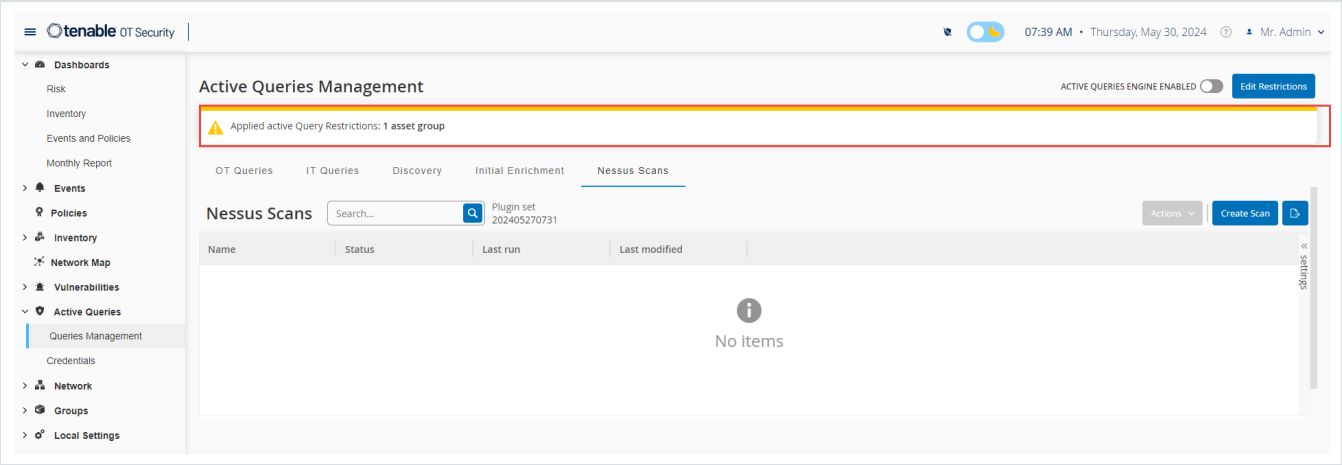
4. In the Restricted Clients drop-down box, select the required clients.

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

> Required OT Security User Role: Administrator, Supervisor

To edit details of a query:

1. Go to Data Collection > Active Queries.

   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

Required OT Security User Role: Administrator, Supervisor

1. Go to Data Collection > Active Queries.

   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

Required OT Security User Role: Administrator, Supervisor

You can run active queries when needed.

To run a query:

1. Go to Data Collection > Active Queries.

   The Queries Management page appears.

2. From the list of queries, select the one you want to run and do one of the following:

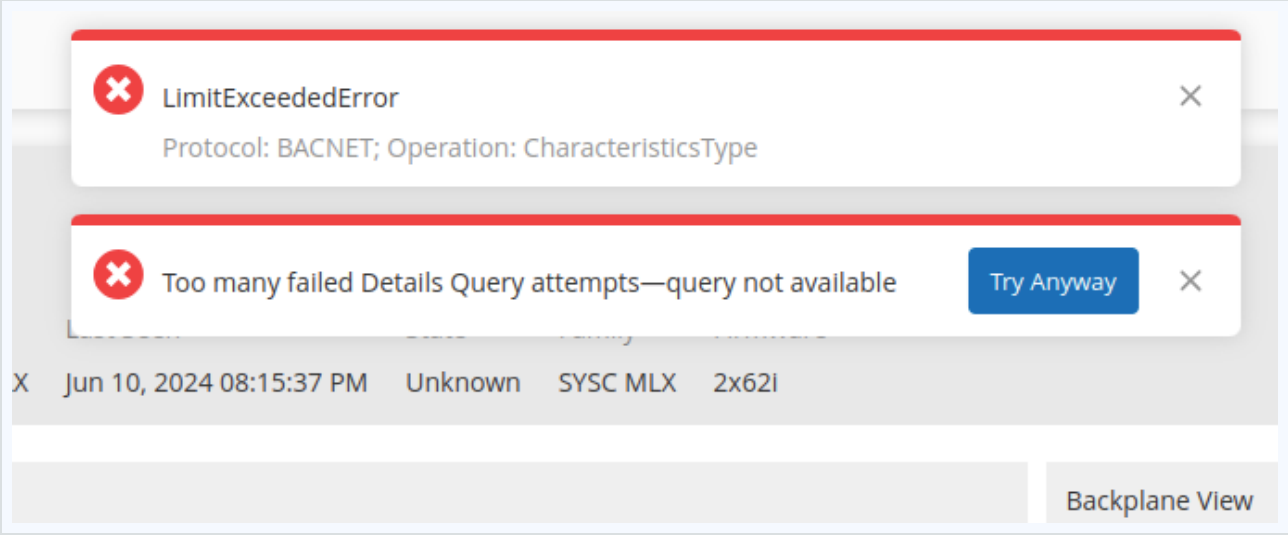
- Right-click the query and select Run now.
- From the Actions menu, click Run now.

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

> Required OT Security User Role: Administrator, Supervisor

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 Data Collection > Active Queries.

   The Active Queries Management window appears.

2. 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.

Discovery Query Types

OT Security uses the following queries for asset discovery for data collection across various network and device types.

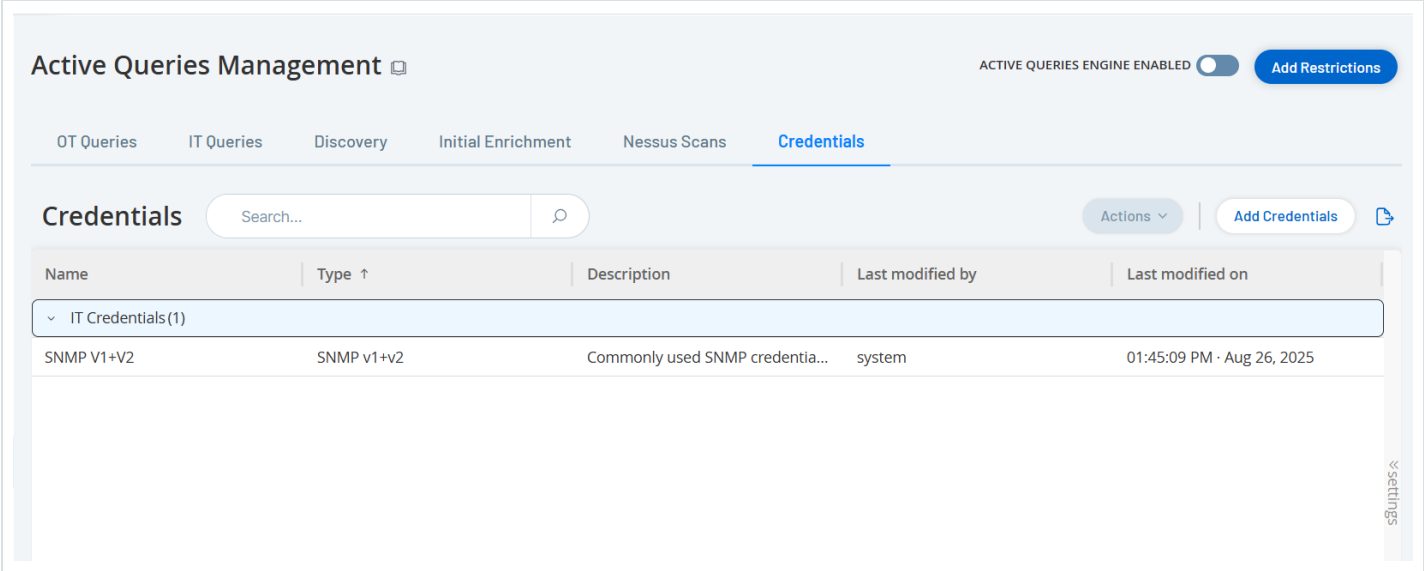
Query Type	Description
SnmpType (SNMP Query)	Standardizes the collection of system data from managed network devices like switches and routers. This query retrieves hardware details, interface statuses, and basic system configurations using the Simple Network Management Protocol (SNMP).
ArpType (Layer 2 ARP Broadcast)	Uses Layer 2 Address Resolution Protocol (ARP) broadcasts to discover active devices on the local network segment. This is essential to identify nearby assets that may not be communicating across gateways.
IdentificationType (Identification Query)	Acts as a primary fingerprinting tool by querying the device for its core identity. This query retrieves the manufacturer, model, and firmware version to establish the baseline asset profile.
CharacteristicsType (Details Query)	Uses proprietary industrial protocols to pull deep-level metadata. This query provides granular hardware and software information that standard identification queries cannot access.

BpScanType (Backplane Scan)	Enumerates all modules, cards, and sub-components residing on a physical chassis for modular hardware. This query provides the complete internal architecture of a Programmable Logic Controller (PLC) or controller.
RunStatusType (Controller State Query)	Monitors the operational mode of PLCs, IEDs, and controllers. For example, modes include RUN, STOP, or FAULT. This query is critical for you to determine if a process is active or if a device shifted into a vulnerable programming state.
NbstatQueryType (NetBIOS Discovery)	Queries the NetBIOS Name Service to identify Windows-based systems and other compatible devices. Use this query to resolve hostnames and workgroup information for assets on the local subnet.
WmiType (WMI Advanced Query)	Uses authenticated Windows Management Instrumentation (WMI) to conduct deep-dive audits of Windows endpoints. Use this query to collect accurate data on installed software, OS patches, active users, and system hotfixes.
WmiUsbType (WMI USB or HID Query)	A specialized WMI request to audit connected physical peripherals. This query detects and logs removable media, for example, thumb drives or Human Interface Device (HID) devices. These devices are common vectors for introducing malware into air-gapped environments.
DnsType (DNS Lookup)	Uses configured DNS servers to resolve an IP address to its Fully Qualified Domain Name (FQDN). This ensures that assets appear by their human-readable network names within the management console.

Credentials

Required OT SecurityUser Role: Administrator, Supervisor

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:

1. Go to Data Collection > Active Queries.

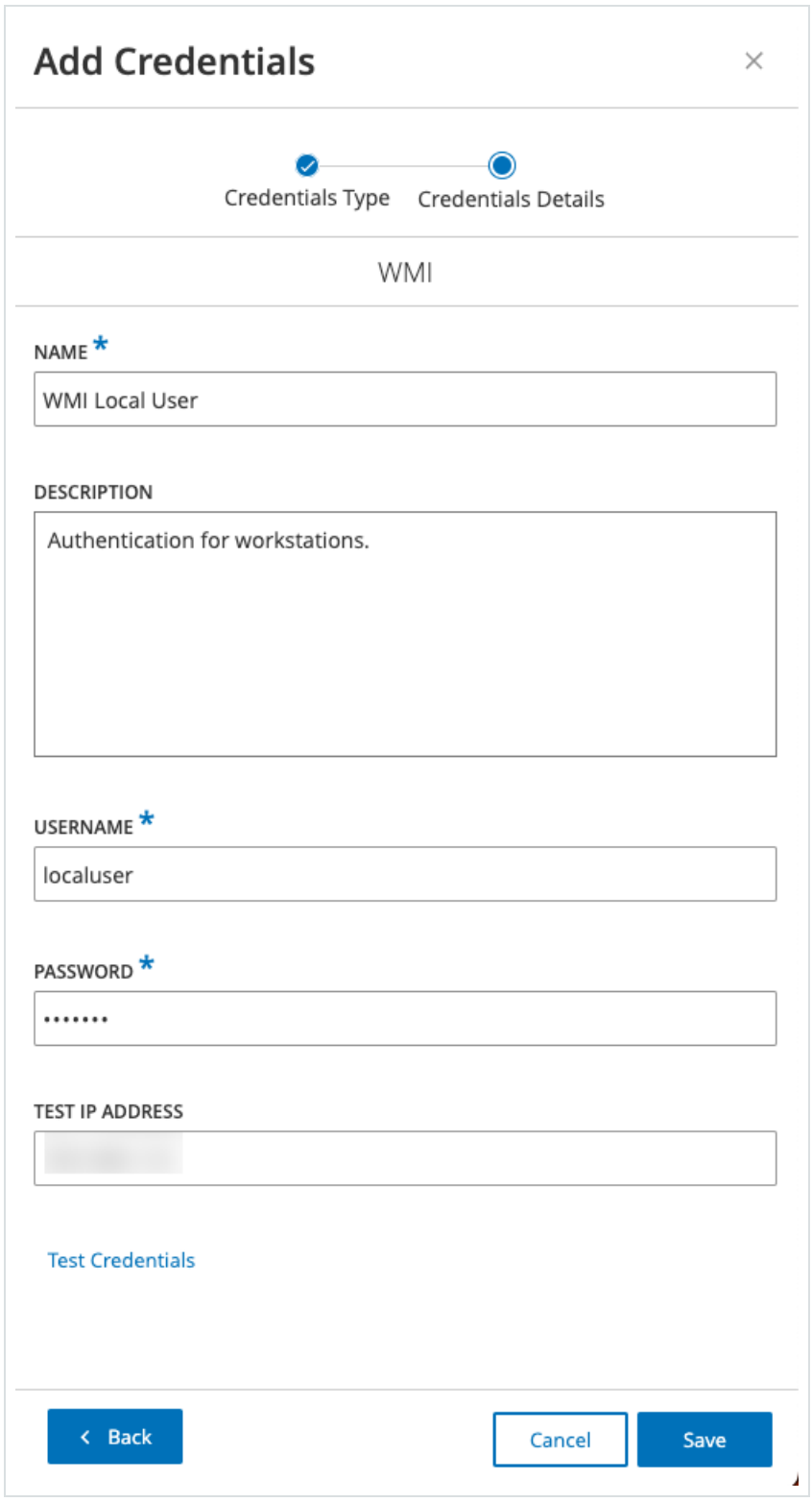
   The Active Queries Management page appears.

2. Click the Credentials tab.

   The Credentials page appears.

3. In the upper-right corner, click Add Credentials.

   The Add Credentials panel appears.



4. 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

5. Click Next.

   The Credentials Details panel appears.

6. 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.
7. Click Test Credentials to confirm if OT Security can reach the device using the credentials.
8. (For duplicated networks) In the Duplicate (Sensor) box, select the associated sensors.
9. 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 Data Collection > Active Queries.

   The Active Queries Management page appears.

2. Click the Credentials tab.

   The Credentials page appears.

3. 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.

4. Modify the details as needed.

5. Click Save.

Delete Credentials

You can delete the credentials that you no longer need.

To delete credentials:

1. Go to Data Collection > Active Queries.

   The Active Queries Management page appears.

2. Click the Credentials tab.

The Credentials page appears.

3. 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

> Required OT Security User Role: Administrator, Supervisor

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.

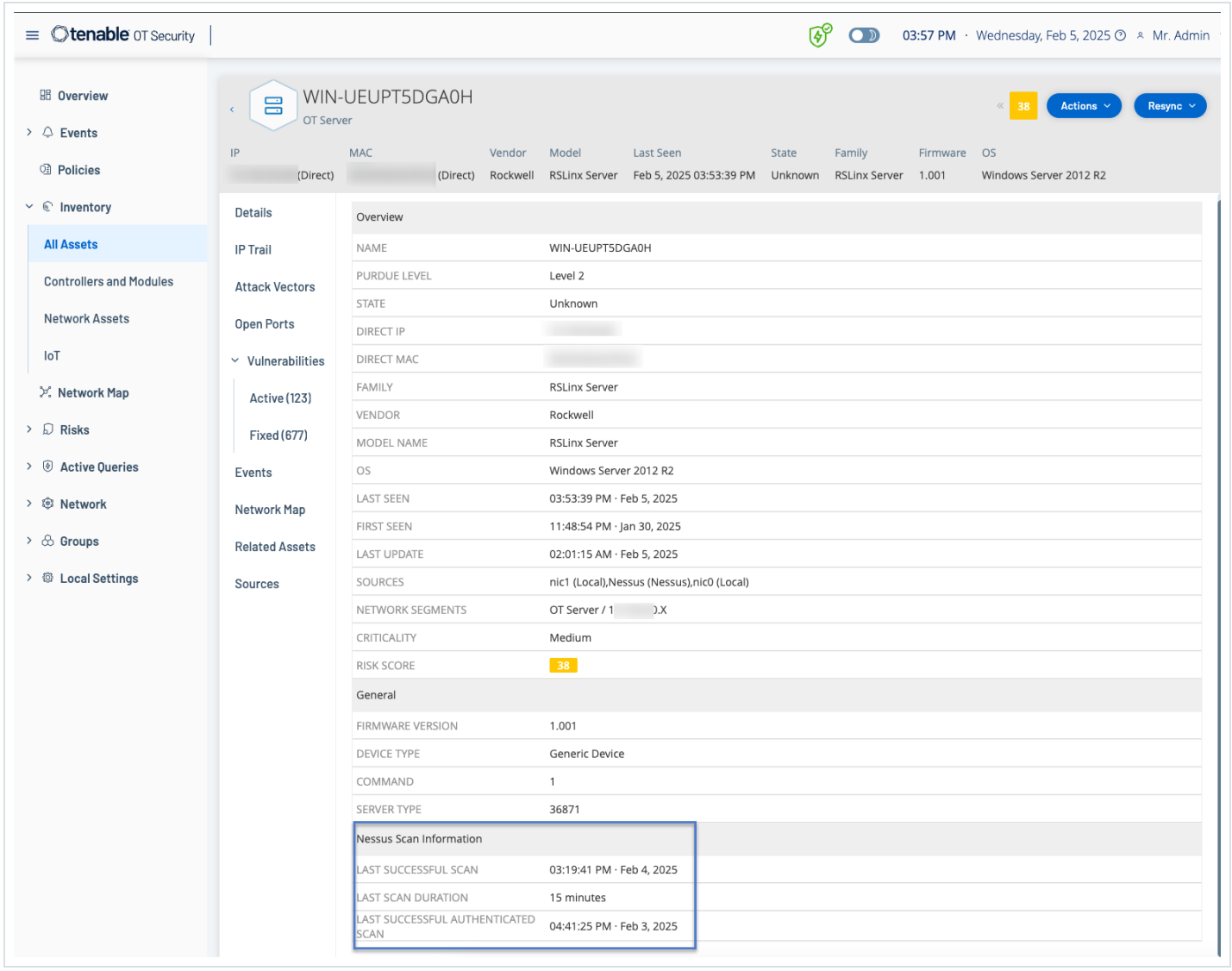
The OT Security executes the scan on responsive assets within the designated CIDRs. However, to protect your OT devices, OT Security scans only confirmed network assets in the given range (non-PLCs). OT Security excludes assets of the type Endpoint from the scan.

Starting from OT Security 4.1, you can create new scans with the following options:

- Perform Thorough Tests – This option allows Nessus to perform a detailed scan that includes plugins that may increase the scan duration, but helps uncover in-depth details such as JAR files or installed Python libraries.
- High Verbosity Processing – This option enables the scan to provide additional details about the vulnerability that you can use to troubleshoot a scan finding. This option also allows Attack Path Analysis to leverage the Nessus scan connections data.
- Network Timeout (In seconds) – The maximum time that Nessus must wait until it gets a response from the host. If you are scanning over a slow host, you can increase the number of seconds. The default is 15 seconds.
- Max Simultaneous Checks Per Host – The maximum number of checks that Nessus must perform against the host. The default number of checks is 2.
- Max Simultaneous Hosts Per Scan – The maximum number of hosts that Nessus can scan simultaneously. The default number of hosts is 10.

The Nessus Scan Information for a credentialed scan includes the following details:

- Last Successful Scan
- Last Scan Duration
- Last Successful Authenticated Scan



The Nessus scan information helps you:

- Understand assessed and unassessed assets.
- Understand if your assets are targeted with credentialed or non-credentialed scans.
- Perform best practices with scanning and vulnerability management. For example, performing vulnerability assessment scans against IT type assets running Windows, Linux. Scanning, whether with or without credentials, helps assess how much of your organization's attack surface is exposed both internally and externally.

The Nessus scan in OT Security uses the same policy settings as a basic network scan in Tenable Nessus, Tenable Security Center, and Tenable Vulnerability Management. The only difference is the performance options in OT Security. The following are the performance options for the Nessus scan in OT Security. These options also apply to the Nessus Basic scan you launch from the Inventory > All Assets page.

- 5 simultaneous hosts (max)
- 2 simultaneous checks per hosts (max)
- 15 second network read timeout

> 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.

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. Go to Data Collection > Active Queries.

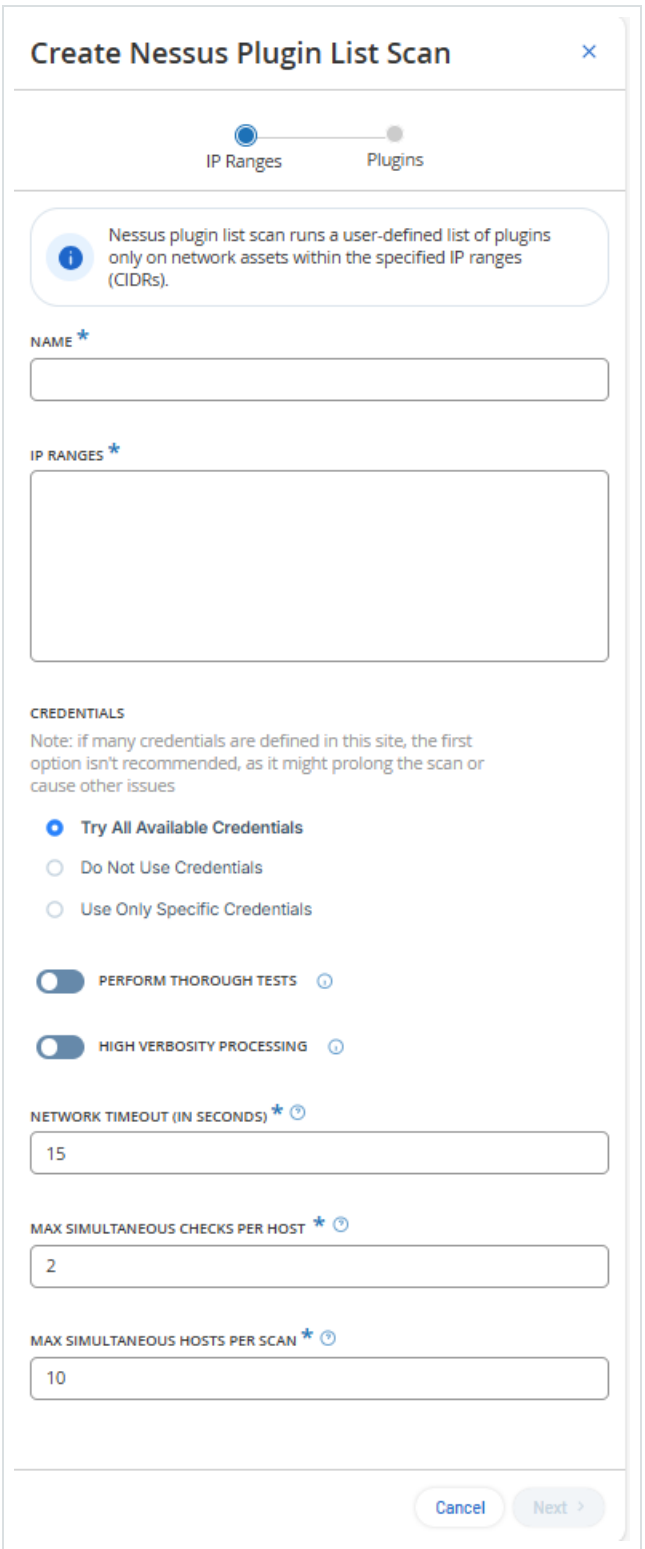
   The Active Queries Management page appears.

3. Click the Nessus Scans tab.

   The Nessus Scans page appears.

4. 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 *
CREDENTIALS
Note: if many credentials are defined in this site, the first option isn't recommended, as it might prolong the scan or cause other issues
Try All Available Credentials
Do Not Use Credentials
Use Only Specific Credentials
PERFORM THOROUGH TESTS
HIGH VERBOSITY PROCESSING
NETWORK TIMEOUT (IN SECONDS) *
15
MAX SIMULTANEOUS CHECKS PER HOST *
2
MAX SIMULTANEOUS HOSTS PER SCAN *
10
Cancel
Next

> Note: The image shows the default values for creating a new Nessus scan. If you opt to run the scan with the default values, the scans run with the same configuration as the earlier scans.

5. In the Name box, type a name for the Nessus scan.
6. In the IP Ranges box, type a range of IPs or CIDRs.
7. Select one of the options to assign credentials for the Nessus scan:
    - Do not use credentials – Select this option if you want to run an unauthenticated scan.

      > Tip: Skip this option if you have several configured credentials, as selecting it may prolong the scan.

    - Try All Available Credentials – Select this option if you want the scan to try all available credentials.
    - Use Only Specific Credentials
        a. If you select Use Only Specific Credentials, select the required credentials from a list of all credentials that are defined in the ICP.
8. (Optional) Click the Thorough Tests toggle to enable a detailed scan.

> Note: The Thorough Tests options include plugins that may increase the scan duration, but enabling the option helps the Nessus scan uncover in-depth details such as JAR files or installed Python libraries.

9. (Optional) Click the Higher Verbosity toggle to enable the scan to provide additional details about the vulnerability.

> Note: Enabling Higher Verbosity allows the scan to provide additional details about the vulnerability or help troubleshoot a scan finding. This option also allows Attack Path Analysis to leverage the Nessus scan connections data.

10. In the Network Timeout (In Seconds) box, type the maximum time that Nessus must wait until it gets a response from the host. If you are scanning over a slow host, you can increase the number of seconds. The default timeout is 15 seconds.
11. In the Max Simultaneous Checks Per Host, type the maximum number of checks that Nessus must perform against the host. The default number of checks is 2.
12. In the Max Simultaneous Hosts Per Scan box, type the maximum number of hosts that Nessus can scan simultaneously. The default number of hosts is 10.
13. 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.

14. 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.

15. 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.

Create OTD Scans

> Required OT Security User Role: Administrator

You can use the OT Discovery (OTD) scan wizard to define a set of scan instructions for offline scanning. The OTD scan configuration defines the how the scan executes, including credentials, schedules, and restrictions.

For information on how to use the OTD scan configuration in Portable state agent scanning, see Scan Using Portable OT Agentsdocumentation.

To create an OTD scan using the configuration wizard:

1. Go to Data Collection > Active Queries.

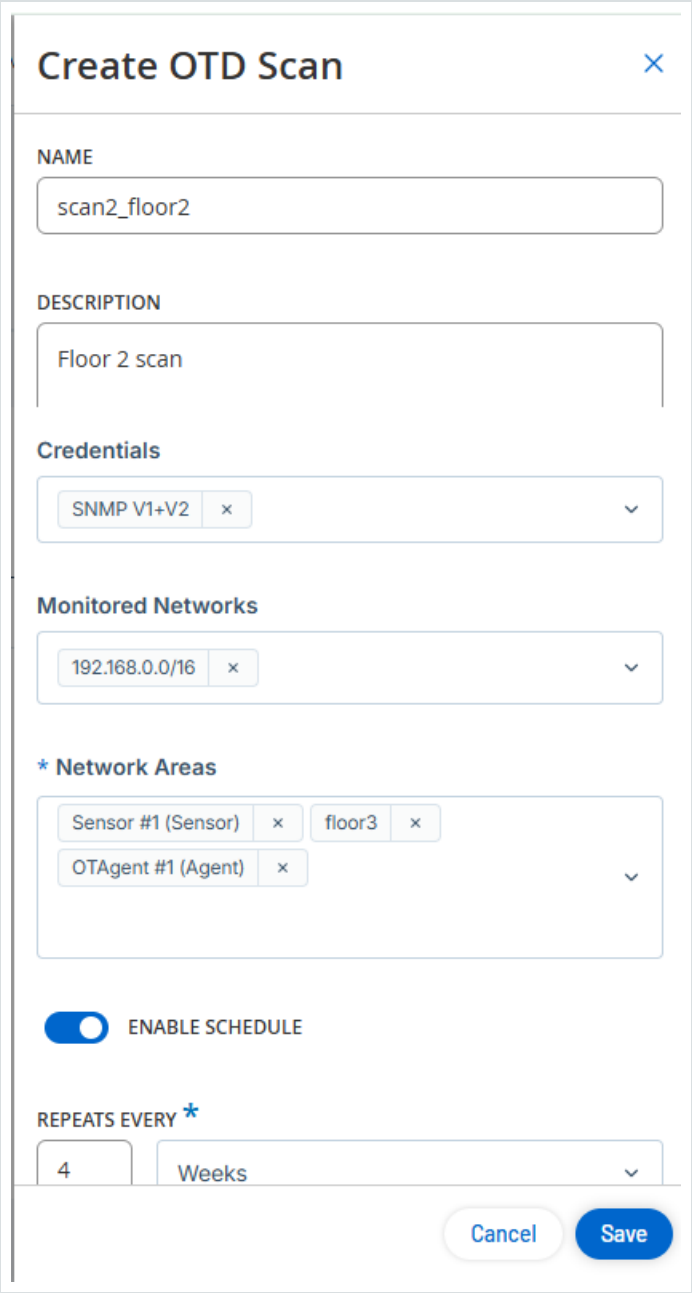
   The Active Queries Management page appears.

2. Click the OTD Scans tab.

   The OTD Scans page appears.

3. Click Create OTD Scan.

   The Create OTD Scan panel appears.



4. In the Name box, type a unique name for the scan.
5. In the Description box, type context or details for the scan.
6. In the Credentials drop-down box, select the required credentials from the list.

7. (Optional) In the upper-right corner, click Add Restrictions to apply restrictions to the scan. For more information, see Add Restrictions.

8. In the Monitored Networks drop-down box, select one or more subnets for the scan, or type a CIDR range.

   > Note: You can pre-populate subnets on the Monitored Networks page, or you can create them directly within this field by typing the CIDR range.

9. In the Network Areas drop-down box, select one or more network areas.

   > Note: You can pre-populate network areas on the Network Areas page, or you can create them directly within this field by typing a new name for the network area.

10. For Static agents, define a schedule.

    a. Click the Enable Schedule toggle.

    b. In the Repeats Every drop-down box, specify the frequency interval in minutes, hours, days, or weeks.

    c. In the On section, select the days of the week you want to run the scan.

    d. In the At drop-down box, select the time of the day you want to run the scan.

11. Click Save.

    OT Security saves the OTD scan configuration.

    ### What to do next

    Scan Using Portable OT Agents

Data Sources

The Data Sources section in OT Security includes the following configuration pages:

- Sensors – View and manage sensors, approve or delete incoming Sensor pairing requests, and configure Active Queries performed by Sensors. See Sensors.
- Agents – Create OT Agents to scan remote Windows machines where installing sensors is not feasible. See OT Agents .
- IoT Connectors – Maps all managed Internet of Things (IoT) devices to their respective application server. See Manage IoT Connectors.
- 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.
- Manual Uploads:
    - Update Asset Details Using CSV – Update the details of your assets using a CSV template. See Update Asset Details Using CSV.
    - Add Assets Manually – Add new assets to your assets list using a CSV template. See Add Assets Manually.
    - SCD Files – Upload Substation Configuration Description (SCD) file OT Security and gain visibility into your assets, IEC 61850 configuration and security insights about your environment. See SCD Files.
    - Rockwell Project Files – Upload `Rockwell .L5X` files to create assets, enrich asset details, and build relationship between assets in air-gapped or limited visibility environments. See Rockwell Project Files.

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.

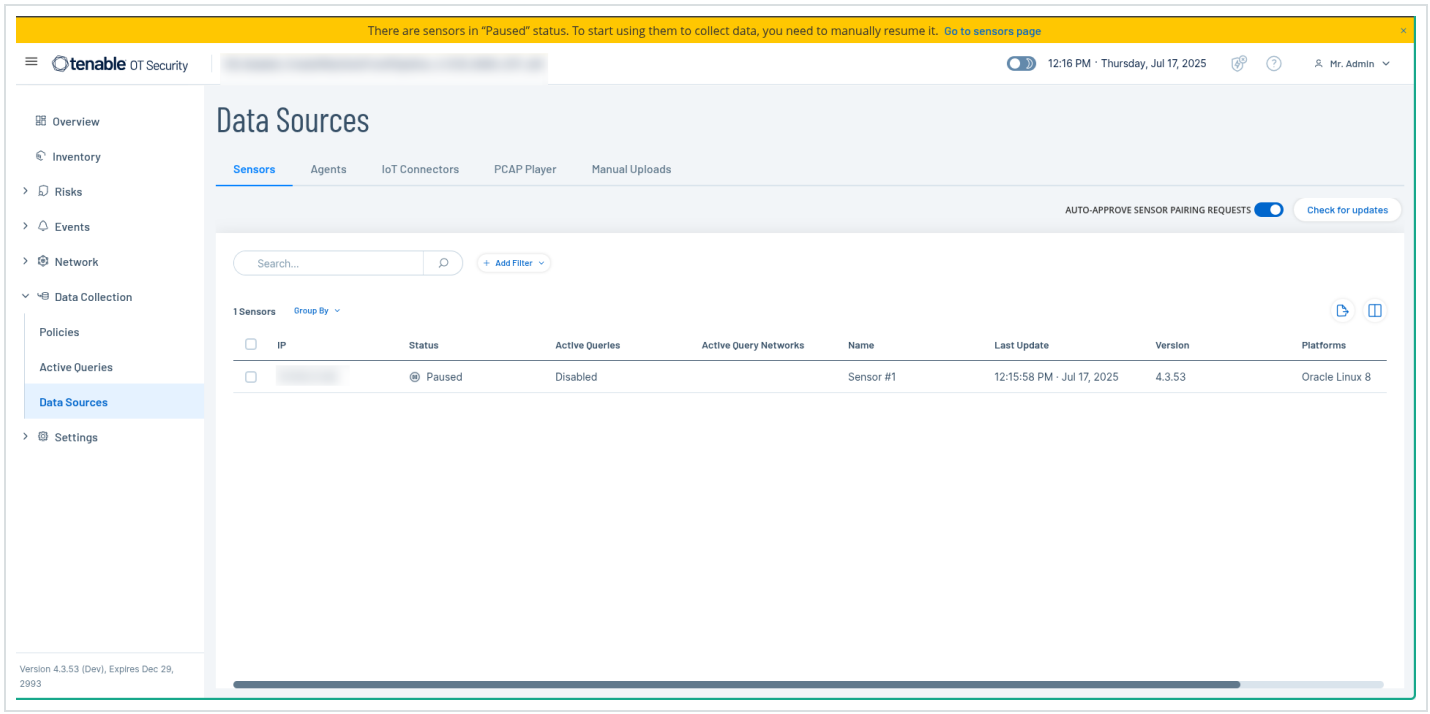
Note: Sensors models preceding version 2.214 do not appear in the ICP Sensors page. However, they can still be used in unauthenticated mode.

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

Required OT Security User Role: Administrator, Supervisor, Security Manager, Security Analyst, Site Operator, Read Only

The Sensors table shows a list of all Sensors version 2.214 and later in the system. For information about how to customize tables, see Management Console User Interface Elements.



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. Important: Once paired, all sensors show the status as Paused. • To change the status for authenticated sensors: In OT Security, right-click the sensors and activate them by changing the status from Paused to Connected. • To change the status for unauthenticated sensors: In Tenable Core + OT Security Sensor, navigate to the OT Security Sensor > Pairing Info section, then click Resume Data Transfer to change the Connection Status.
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

Required OT Security User Role: Administrator

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.

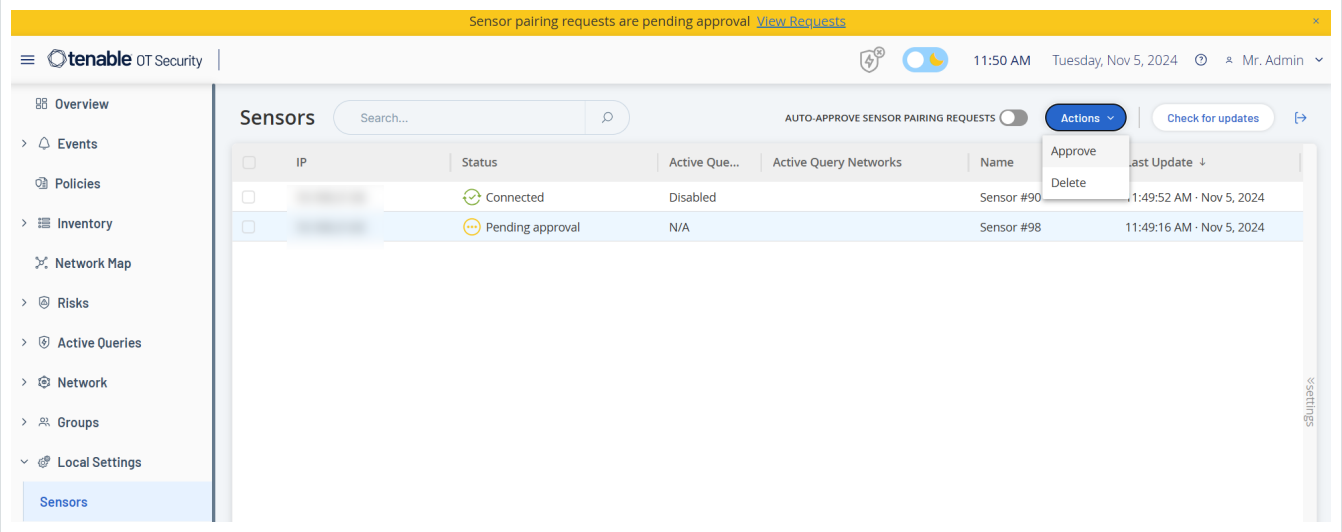
To manually approve a sensor pairing request:

1. In the Data Collection > Data Sources page, click the Sensors tab.

   The Sensors page appears.

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

Required OT Security User Role: Administrator

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:

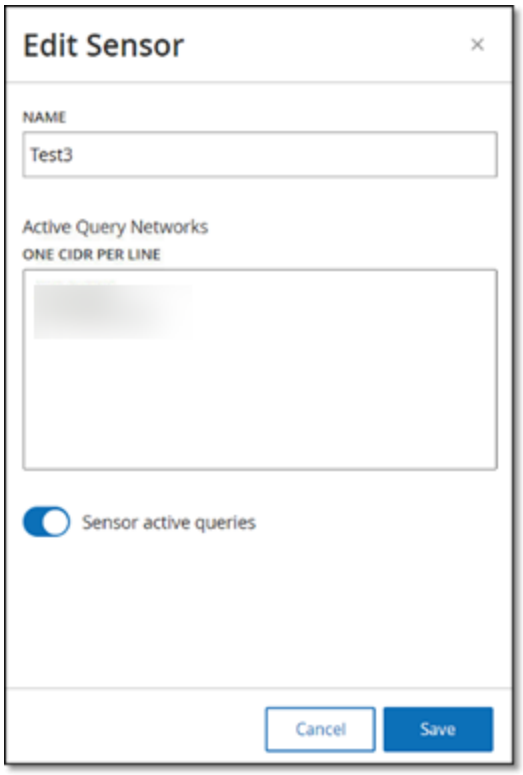
1. In the Data Collection > Data Sources page, click the Sensors tab.

   The Sensors page appears.

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.



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.

   > Note: If the sensor is part of a duplicated network, the duplicated network IP address appears in the Active Query Networks box and is disabled for editing.

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

> Required OT Security User Role: Administrator

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.

> Note: OT Security uses the offline ISO for the centralized updates. To centrally update all authenticated sensors attached to an ICP, place the ICP / Sensor offline ISO under `/srv/tenablecore/offlineiso/tenable-offline-updates.iso` on the ICP.

> Note: (For OT Security EM users only). OT Security uses the offline ISO for the centralized updates. To centrally update all authenticated sensors attached to an ICP through an EM, place the EM offline iso under `/srv/tenablecore/offlineiso/tenable-offline-updates.iso` on the EM.

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 Pair the Sensor.

To update authenticated sensor version 3.16 or later with the ICP:

1. In the Data Collection > Data Sources page, click the Sensors tab.

   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.

OT Agents

OT Agents are software components you can install on remote Windows machines to actively query and discover OT Security assets in environments where sensor installation is not possible or practical. OT Agents leverage active queries to scan duplicated and active query networks listed under Monitored Networks. This allows the agent, running on a Windows-based gateway, an engineering workstation, or Human-Machine Interface (HMI) to identify critical OT / IoT, and embedded devices on the network.

Every OT asset the OT Agent discovers is associated with that specific agent as its discovery source. This provides traceability for asset identification within your network.

To scan networks, first install and configure the OT Agent. The following sections describe how to install, configure, and run scans using the OT Agent.

1. Download the OT Agent
2. Install the OT Agent
3. Configure the OT Agent
4. Run scans

View OT Agents

The OT Agents page acts as the central hub for monitoring and configuring the agents that you deploy to monitor your network.

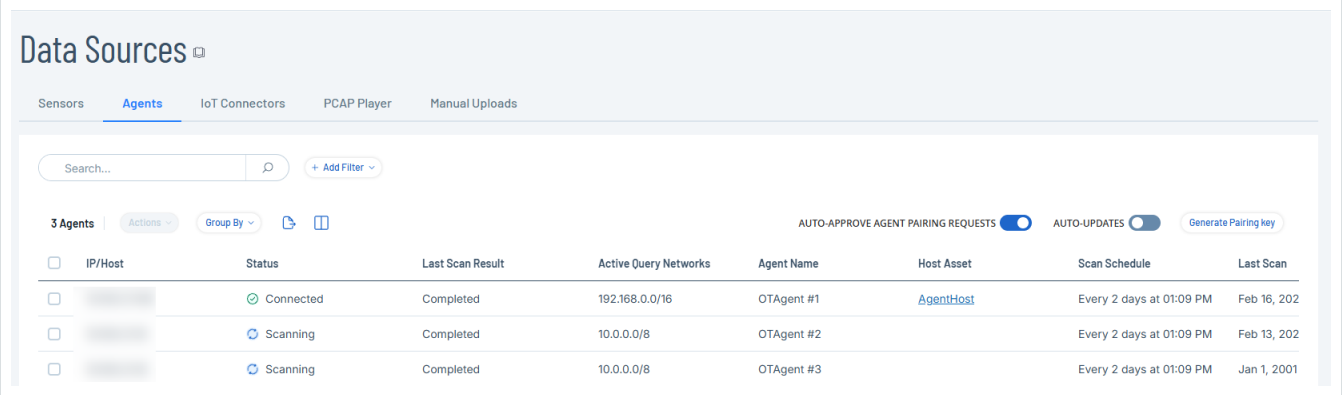
To access the OT Agents page:

1. In the left navigation menu, click Data Collections > Data Sources.

   The Data Sources page appears.

2. Click the Agents tab.

   The Agents page appears displaying a list of your deployed OT Agents.



The Agents page includes the following details:

Parameter	Description
IP/Host	The IPv4 address of the machine where the OT Agent is installed.
Status	The status of the agent: • Connected • Paused • Disconnected • Pending Configuration • Pending Approval • Preparing Connection • Waiting for Connection • Updating • Scanning
Last Scan	The status of the last scan: Completed or Failed.

Result	
Active Query Networks	The specific network segments that OT agents are targeting in the current scan.
Agent Name	The unique name assigned to the OT agent.
Host Asset	A direct link to host asset's details page.
Scan Schedule	The configured frequency for the scan. The column displays Disabled if there are no schedules.
Last Scan	The date and time the most recent scan was initiated.
Last Scan Duration	The time taken to complete the last scan.
Credentials	The credentials the agents use to scan the devices.
Reported Assets	The number of assets detected in the scan.
Agent Version	The version of the OT Agent.
OTD Version	The version of the OT Discovery engine.
Host OS	The operating system on the host machine.

Install OT Agent

> Required OT Security User Role: Administrator

Install the OT Agent on a Windows machine to scan OT environments.

Before you Begin

- Download the OT Agent from the Tenable downloads portal.
- Make sure you have administrator permissions on the Windows machine.

Note: The default ports for pairing and connection are 443 and 28306 respectively. For information about ports, see Firewall Considerations

To install the OT Agent:

1. Transfer the install file (`Tenable-OT-Agent-version.msi`) to the Windows machine.
2. Click the `.msi` install file to open the installation wizard.
3. In the OT-Agent Setup Wizard window, click Next.

   The Enter ICP Details window appears.
4. Select one of the following:

   - Use Pairing Key

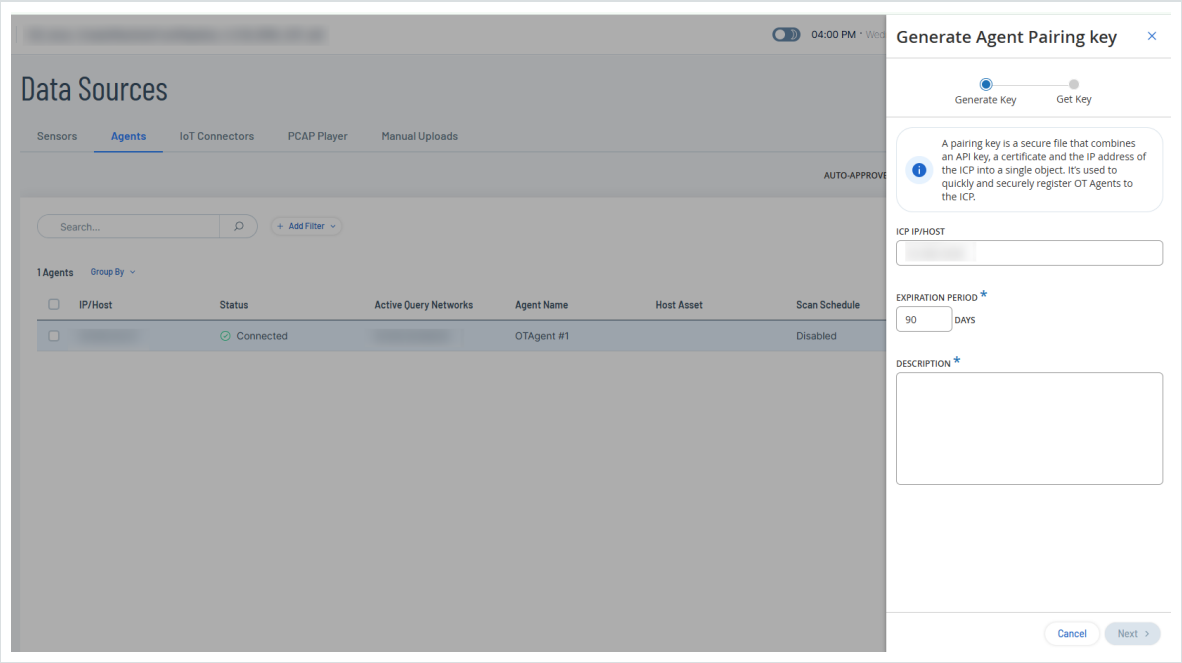
     This is the default option. If you selected this option, perform the following steps:

     1. In OT Security, navigate to Data Collection > Data Sources.

        The Data Sources page appears.
     2. Click the Agents tab.

        The Agents page appears.
     3. In the upper-right corner, click Generate Pairing Key.

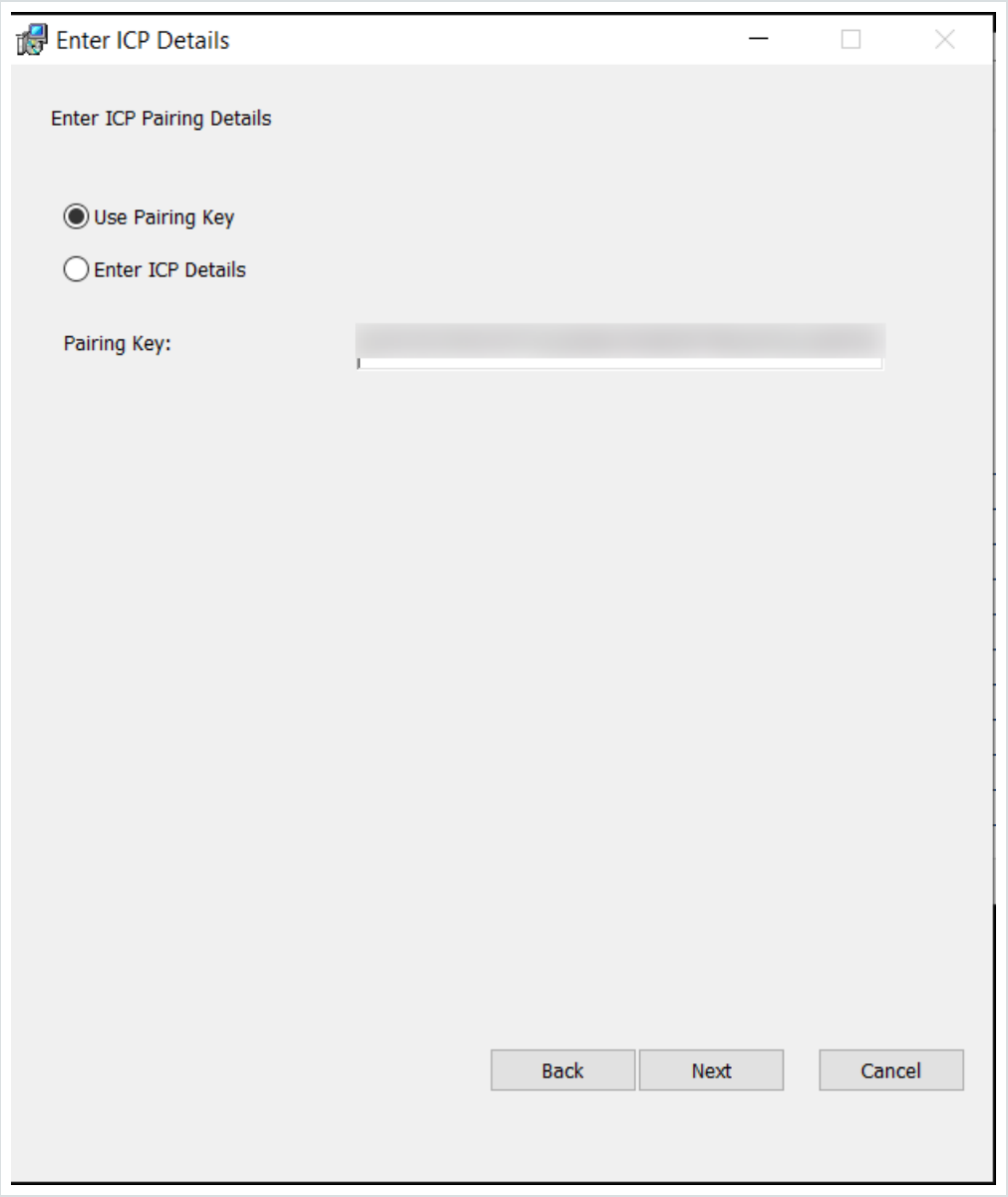
        The Generate Agent Pairing Key panel appears.



4. In the ICP IP/Host box, provide the IP address or the hostname of the ICP.
5. In the Expiration Period drop-down box, retain the default 90 days or specify the number of days after which the key expires.
6. In the Description box, provide a description for the key.
7. Click Next.

   OT Security generates the pairing key.
8. Click the button to copy the pairing key.
9. Click Done.

   OT Security closes the panel.
10. Navigate back to the Windows host machine.
11. In the Pairing Key box, paste the pairing key you copied from the ICP.



- Enter ICP Details

  If you select this option, the relevant fields appear where you can provide the required details for the ICP.

  1. In the ICP Address box, type the IP address of the ICP.
  2. In the ICP Username box, type the name of the ICP machine.

3. In the ICP Password box, type the password of the ICP machine.
4. In the API Key box, provide the API key generated from the ICP. See Generate API Keys.
5. In the Certificate Fingerprint box, provide the fingerprint generated from the ICP. See Certificates.

> Note: The pairing key and certificates are only required for the pairing process. Once pairing is complete, you can delete the pairing key and certificate, if needed.

5. Click Next.

   The Destination Folder window appears.

6. In the Install OT-Agent to: box, retain the default destination or provide the path to install the OT Agent and click Next.
7. Click Install.

   The installer installs the OT Agent and lists it on the Agents tab in OT Security with the status Pending Configuration.

8. Click Finish to close the installer.

> Note: If there are issues with the pairing, you can use the Repair option in the OT Agent installation wizard to provide the pairing details again.

9. To automatically approve the pairing request, click to enable the Auto-Approve Agent Pairing Requests toggle.

   If this option is not enabled, do the following:

   - Right-click the newly added OT Agent.

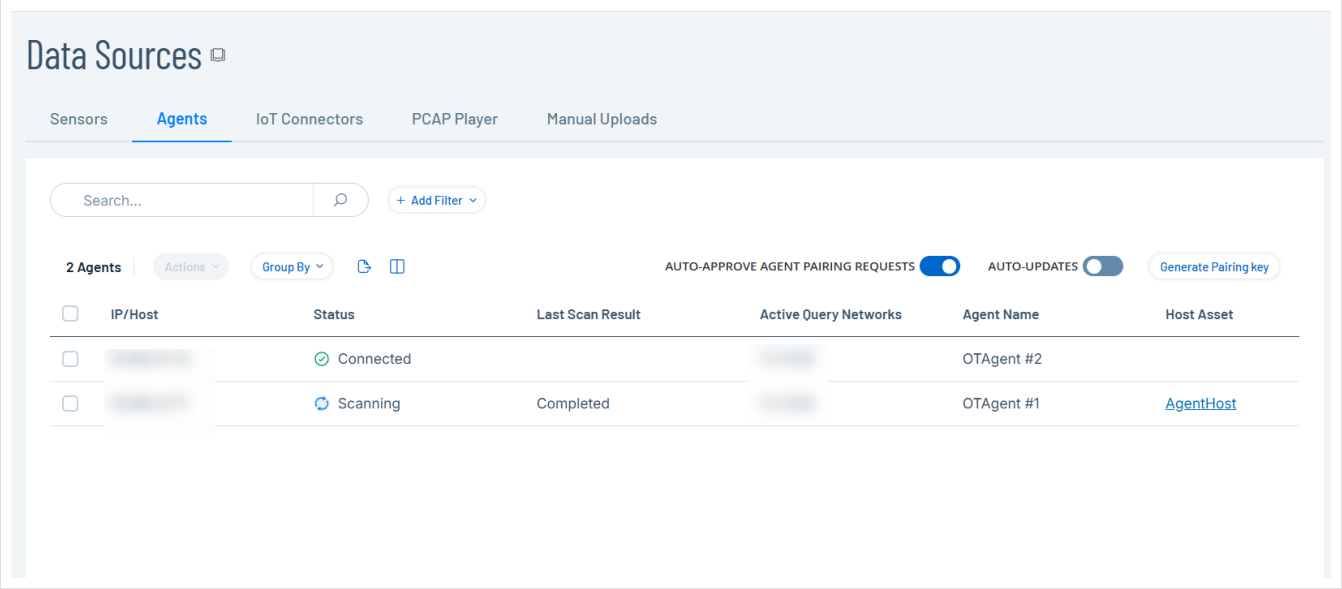
     A menu appears.

- Select the checkbox next to the OT Agent.

  OT Security enables the Actions > Approve menu.

10. Click Approve.

    OT Security approves the agent pairing and changes the status to Pending Configuration.



> Note: Before you run the OT Agent, ensure that its configuration is complete, even if the Auto-Approve Agent Pairing Requests option is enabled.

What to do next

Configure the OT Agent

Configure OT Agent

> Required OT Security User Role: Administrator

After installing the OT Agent, configure it to define its name, specify the networks it scans, and set a schedule for active queries.

Before you Begin

- Install the OT Agent.

To configure the OT Agent:

1. In the Agents tab, do one of the following:

   - Right-click the newly added OT Agent.

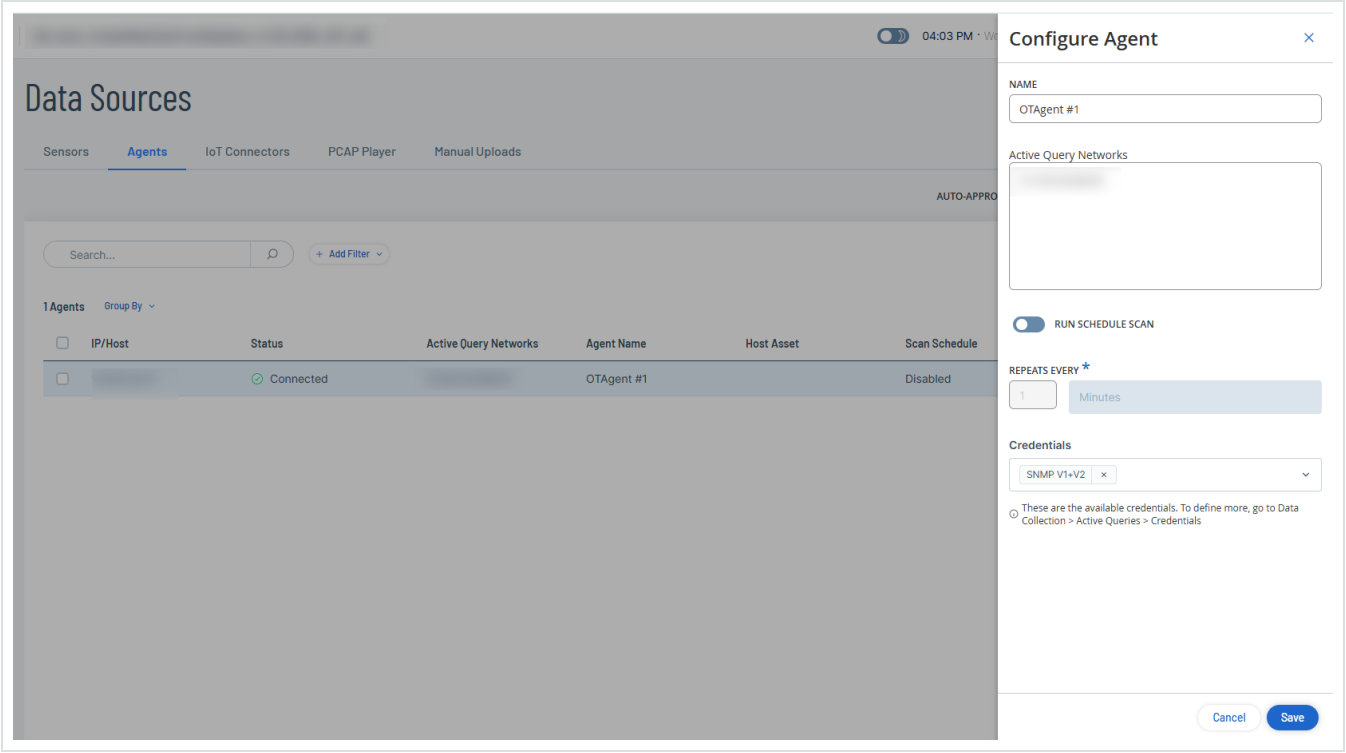
     A menu appears.

   - Select the checkbox next to the OT Agent.

     OT Security enables the Actions > Configure menu.

2. Click Configure.

   The Configure Agent panel appears.



3. In the Name box, type a name for the agent.

4. In the Active Query box, provide the IP addresses of the networks to scan.

> Note: The OT Agent scans only those active query network IP addresses that are part of the Monitored Networks (Environment Settings > Network Definitions > Monitored Networks).

5. (Optional) To enable scheduled scans, click the Run Schedule Scan toggle.

   OT Security enables the Repeats Every drop-down box.

6. (Optional) Specify the minutes, hours, days, or weeks as required.

7. In the Credentials drop-down box, select the required credentials.

   > Note: Only credentials you create in Active Queries > Credentials appear in this list. For more information, see Credentials.

8. Click Save.

   OT Security updates OT Agent's status to Connected.

What to do next

Run Scans

Run Scans using OT Agent

> Required OT Security User Role: Administrator

When you initiate an Agent scan, it triggers the following active queries:

- Discovery: Detects live assets in the monitored network.
- Open ports check: Scans the most frequently used ports of the active query clients.
- Initial Enrichment: Identifies newly discovered assets with Dynamic Fingerprinting Engine (DFE).

- OT Queries:Gathers device information, such as PLC running state and other modules connected to the backplane.
- IT Queries: Obtains data from IT devices monitored by OT Security.

For more information, see Manage Active Queries.

To run an agent scan:

1. In the Data Sources > Agents tab, do one of the following:
   - Right-click the newly added OT Agent.

     A menu appears.
   - Select the checkbox next to the OT Agent.

     OT Security enables the Actions button in the header.

   > Note: To initiate scans for multiple agents, select more than one OT Agent, then click Bulk Actions > Scan Now.

2. Click Actions > Scan Now.

   The status of the agent changes to Scanning and scan begins on the specified networks. After the scan completes, click the link in the Reported Assets column in the Agents table to view the filtered results on the Inventory page.

Abort a scan

> Required OT Security User Role: Administrator

If you need to stop a scan in progress:

1. In the Data Sources > Agents tab, do one of the following:

    - Right-click the agent and select Abort Scan.
    - Select the checkbox next to the agent, and then click Actions > Abort Scan.

    OT Security stops the scan and the Last Scan Result column shows Failed.

Update OT Agent

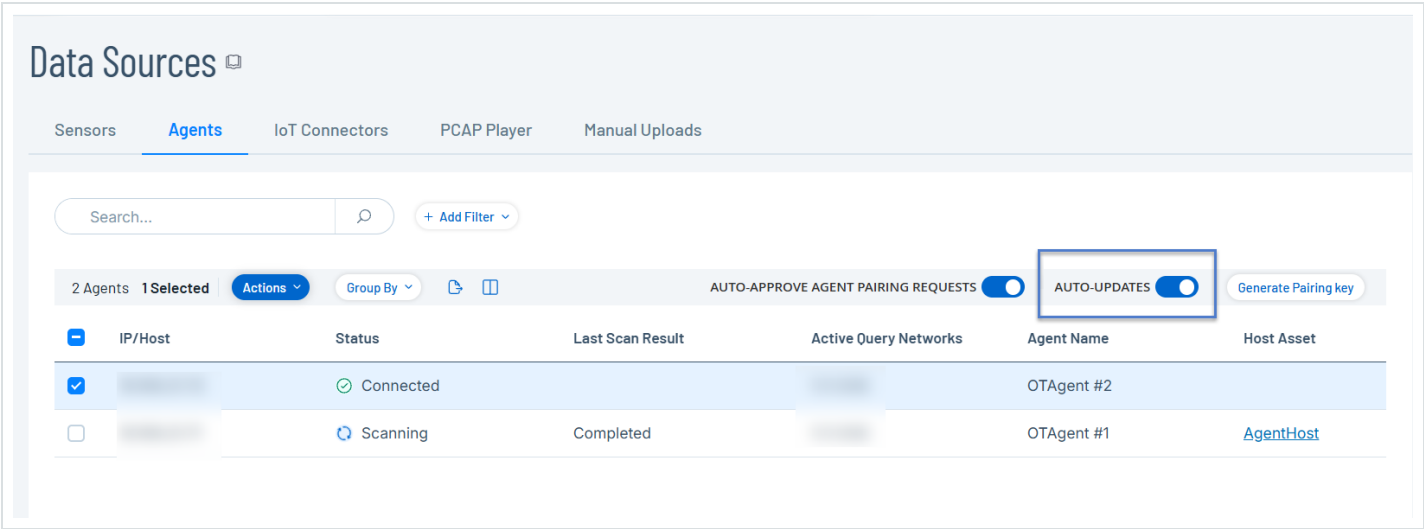
> Required OT Security User Role: Administrator

> Required **OT Security** User Role to upload the file: Administrator, Supervisor, and Security Analyst.

OT Agents use the OT Discovery (OTD) engine for actively scanning your environment. You can update the OT Discovery engine versions either manually or automatically from the Agents page.

Automatic Updates

To automatically update the OTD versions when an ICP update is available, enable the Auto-Updates toggle. The toggle is disabled by default. When you enable Auto-Updates, OT Security automatically pushes the latest OTD engine version to connected agents whenever a new release is available.



Manual Updates

Use manual updates when you need to update the OTD engines between official releases or bulk-update multiple agents simultaneously.

Before you Begin

- Upload the OTD file in the System Configuration > Updates > OT Discovery Engine (OTD) Update section as mentioned in OT Discovery Engine (OTD) Updates.
- Ensure that the OT Agent is online and the status is Connected.

To manually update the OTD engine:

1. In the left navigation bar, click Data Sources > Agents.

   The Agents tab appears.

2. To update agents, do one of the following:

   - Right-click the agent you want to update.

     A menu appears.

   - Select the checkbox next to the agent you want to update.

     OT Security enables the Actions menu.

     > Note: To bulk-update OTD engines, select multiple agents, and then click Bulk Actions > Update.

3. Click Actions > Update.

   The Update OTD Version dialog box appears.

4. Click Update to confirm.

   OT Security updates the OT Discovery engines to the latest version.

Delete an OT Agent

Required OT Security User Role: Administrator

Uninstalling the OT Agent from the Windows machine changes the status of the agent to Disconnected in OT Security.

To delete an OT Agent:

1. In the Windows machine, open the installer and click Remove.
2. Follow the steps in the wizard to uninstall the agent.

   OT Agent gets uninstalled from the Windows machine.
3. Navigate to the Data Sources > Agents tab in OT Security.

   OT Security updates the status of the agent to Disconnected.
4. Do one of the following:

   - Right-click the newly added OT Agent.

     A menu appears.
   - Select the checkbox next to the OT Agent.

     OT Security activates the Actions > Delete menu.

     Note: To delete OT agents in bulk, select more than one OT Agent, then click Bulk Actions > Delete.
5. Click Delete.

   OT Security deletes the OT Agent.

   Note: If there are associated duplicated networks, you must first delete them before deleting the agent.

Install OT Agents Using CLI

> Required OT Security User Role: Administrator

Use CLI commands to install OT Agent with pairing key, ICP credentials, or API key. You can also uninstall OT Agent via CLI.

Before you begin

- Download the OT Agent installer from the Tenable Downloads portal.

To install OT Agent with a pairing key, run the following command:

```
msiexec.exe /i "<OtAgentInstaller.msi>" /qn PAIRING_KEY="<PairingKey>"
```

Where:

- `OtAgentInstaller.msi` is the installation file.
- `PairingKey` is the key that you generate from the Data Collection > Data Sources > Agents tab in OT Security.

Example:

```
msiexec.exe /i "OtAgentInstaller.msi" /qn PAIRING_
KEY="xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxoxxxxxxxxxxxx"
```

To install OT Agent with username and password, run the following command:

```
msiexec.exe /i "<OtAgentInstaller.msi>" /qn ICP_ADDRESS="<IpAddress>" ICP_USERNAME="<Username>" ICP_
PASSWORD="<Password>" ICP_FINGERPRINT="<CertFingerprint>"
```

Where:

- `OtAgentInstaller.msi` is the installation file.
- `IpAddress` is the IP address of the ICP.

- `Username` is the username to log in to the ICP.
- `Password` is the ICP password.
- `CertFingerprint` is the certificate that you generate in OT Security.

Example:

```
msiexec.exe /i "OtAgentInstaller.msi" /qn ICP_ADDRESS="XX.XXX.XX.XX" ICP_USERNAME="admin" ICP_
PASSWORD="xxxxxxx" ICP_FINGERPRINT="XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX"
```

To install with an API Key, run the following command:

```
msiexec.exe /i "<OtAgentInstaller.msi>" /qn ICP_ADDRESS="<IpAddress>" ICP_APIKEY="<APIKey>" ICP_
FINGERPRINT="<CertFingerprint>"
```

(Optional parameter) `INSTALLBASE='"<FullDirPath>"'`

Where:

- `OtAgentInstaller.msi` is the installation file.
- `IpAddress` is the IP address of the ICP.
- `APIKey` is the API Key generated from the ICP.
- `CertFingerprint` is the certificate generated from the ICP.
- `FullDirPath` is the path of the installation directory.

Example 1:

```
msiexec.exe /i "OtAgentInstaller.msi" /qn ICP_ADDRESS="XX.XXX.XX.XX" ICP_APIKEY="kxxxxxxxxxxxxxxxxx_
xxxxxxxx=" ICP_FINGERPRINT="XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX"
```

Example 2: Using the `INSTALLBASE` parameter:

```
msiexec.exe /i "OtAgentInstaller.msi" /qn ICP_ADDRESS="xx.xxx.xx.xx" ICP_APIKEY="xxxxxxxxxxxxxxx_
```

```
xxxxxxxxxxx=" ICP_FINGERPRINT="XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX"
INSTALLBASE='"C:\Program Files\AAA"'
```

To uninstall OT Agent, run the following command:

```
msiexec.exe /x "<OtAgentInstaller.msi>" /qn
```

Where:

- `OtAgentInstaller.msi` is the installation file.

Enable, Disable, or Set Scheduled Scans for OT Agents

Enable or disable scheduled scans for multiple OT Agents simultaneously using the Bulk Actions option.

Before you Begin

- Make sure that the OT Agents are online and that their Status column shows Connected.

To perform bulk actions on scheduled agent scans:

1. In the Agents table, select more than one OT Agent for your scan.

   OT Security enables Bulk Actions in the header.

2. Select one of the following options:

Bulk Actions Option	Description
Enable Scheduled	Select this option to enable scheduled agent scans. The scheduled scan runs every minute by default.

Scan	
Disable Scheduled Scan	Select this option to disable scheduled agent scans.
Set Schedule Scan	a. To configure a scheduled scan, click Bulk Actions > Set Schedule Scan. The Set Schedule panel appears. b. In the Repeats Every box, select the number of times you want the scan to repeat. c. Specify the minutes, hours, days, or weeks as required. Note: The schedule that you specify here overrides any existing schedules for the agents. d. Click Save.

Comparing OT Agent and Sensor

Capability	OT Agent	Sensor
Target Use Case	For assessments, PoVs, and flexible Windows-based OT environments.	For full deployments where traffic inspection and control are required.
Deployment Type	Installed on Windows machines (HMI, workstation, jump box)	Installed on hardware or VM, based on Tenable Core operating system.
ICP Dependency	Requires pairing with ICP, but can	Fully dependent on ICP

	operate independently to collect data (requires support + scripts)	
Installation Complexity	Lightweight, flexible; can be deployed in bulk	Requires physical or virtual deployment + configuration
Data Flow to ICP	Results pushed after scan completion	Continuous data stream (active +passive)
Execution Type	Active scanning only	Active and passive scanning
Scan Management UI	Managed from the Agents page only	Queries triggered from the Active Query and Inventory pages.
Nessus Integration	Not supported	Nessus queries can route through Sensors.
Vulnerability Matching	Uses embedded Nessus in ICP for matching.	Uses embedded Nessus in ICP for both matching and active scanning.
Scan Scheduling	Supported (one-time or recurring).	Supported (one-time or recurring).
Asset Visibility	Assets shown in inventory but not queryable from inventory.	Assets fully queryable from inventory.
Credential Scope	Uses dedicated credentials configured per Agent.	Uses global credentials from ICP.
Duplicated Network Support	Supported	Supported

Respects Global Restrictions	Not supported in version 4.3	Supported
Pairing Method	Pairing Key (API key +certificate + ICP IP in one blob).	Requires API key, Certificate, or IP configured manually.
Hardware	None - runs on existing Windows machines.	Dedicated hardware or VM required.
Passive Traffic Capture	Not supported	Fully supported

Manage IoT Connectors

> Required OT Security User Role: Administrator, Supervisor

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.

> 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 Settings > Environment Configuration > Assets Settings and disable the Fetch IP Address for IoT Assets option.

Requirements for IoT Connector Agent

Requirement Category	Minimum Requirement
Operating System	• Windows XP, 7, 10, or 11; Windows Server 2003, 2008, 2012, 2016, 2019, or 2022 • Ubuntu 20.x or 22.x
Memory	1 GB
Disk Space	1 GB
CPU	Any hardware with a minimum of 10% dedicated CPU capacity.

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.

You can perform the following tasks for IoT connectors:

Add IoT Connectors

1. In the Data Collection > Data Sources page, click the IoT Connectors tab.

   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 Address of the Server box, type the IP address of the connector to add.
3. To connect to the VMS hosted in the database, click to enable the VMS Credentials toggle.

   OT Security enables the relevant fields required for VMS credentials.
4. In the IP Address of the Database box, add the IP address of the database hosting the VMS.
5. In the Database port box, add the port number to connect to the server.
6. In the Username box, type the username for the database.
7. In the Password box, type the password for the database.
8. 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.

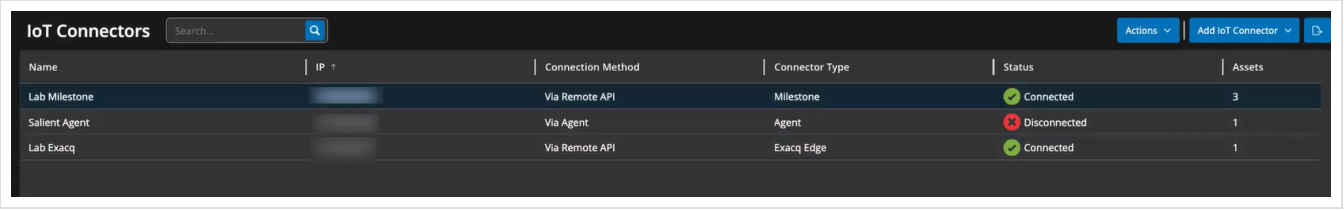
- Via Remote API

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.



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.

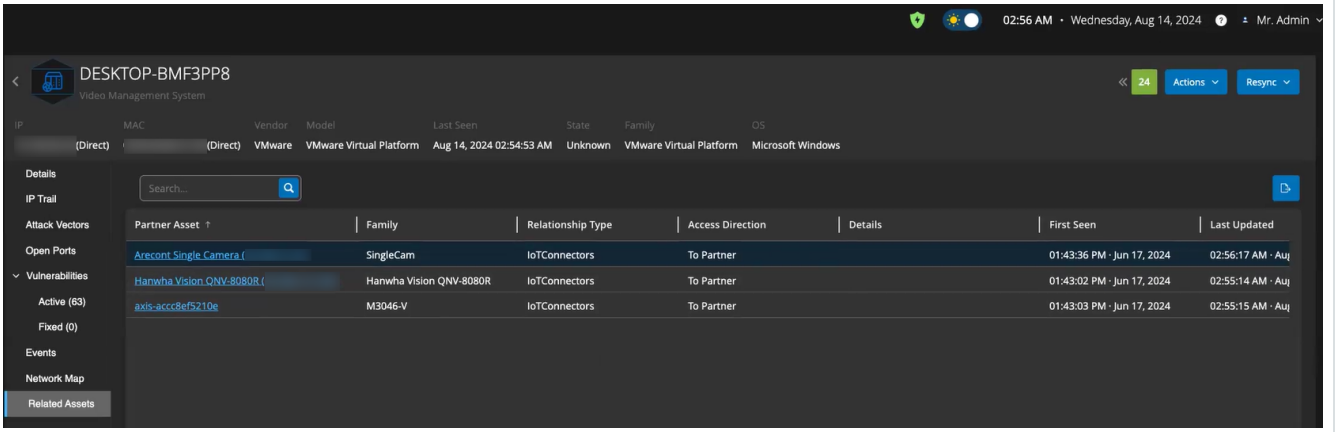
To view all devices managed by the server:

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.



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 an 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.

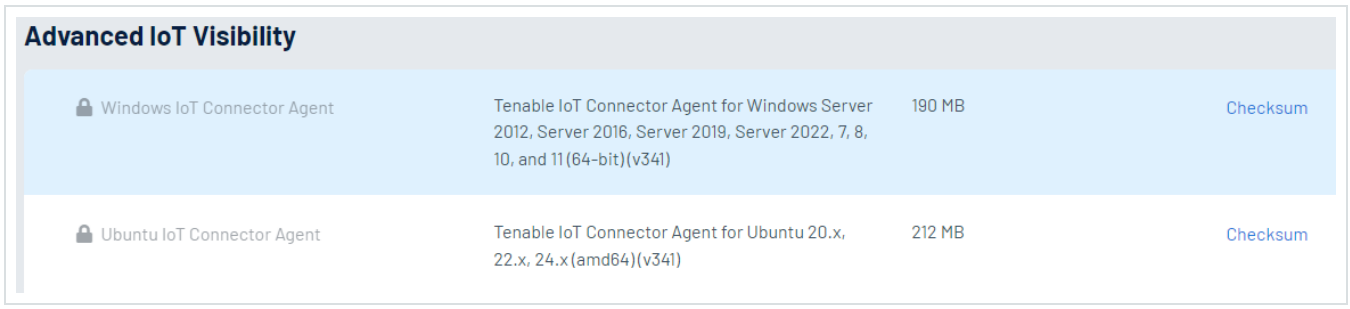
Install IoT Connector Agent on Windows

> 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.



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.

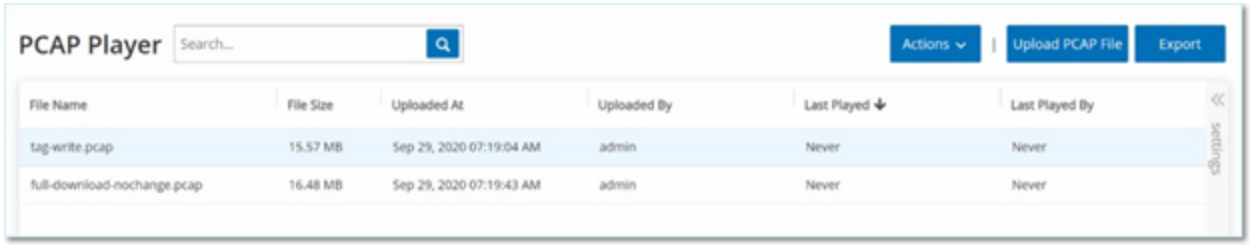
b. Confirm that the **OT Security** IoT Connector Agent appears in the list of services currently running.

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.

PCAP Player

> Required OT Security User Role: Administrator, Supervisor

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. In the Data Collection > Data Sources page, click the PCAP Player tab.

   The PCAP Player page appears.

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. In the Data Collection > Data Sources page, click the PCAP Player tab.

   The PCAP Player page appears.

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.

Manual Uploads

Required OT Security User Role: Administrator, Supervisor, Site Operator

The Manual Uploads tab includes the following:

- Update Assets Details Using CSV
- Add Assets Manually
- SCD Files
- Rockwell Project Files

Update Assets Details Using CSV

You can export a CSV file of the All Assets table, make edits, and then upload it. The editable fields include: Type, Name, Criticality, Purdue Level, Location, Description, and all custom fields.

You can update asset details using a CSV file only when the language is set to English. Non-English users can temporarily switch to English while exporting and uploading the CSV file, then revert to their preferred language.

To upload the asset details CSV file:

1. In the Data Collections > Data Sources page, click the Manual Uploads tab.
2. In the Update Asset Details Using CSV section, click Upload.
3. Browse to the location where you have the CSV file and upload it.

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 Data Collection > Data Sources.

   The Data Sources page appears.

2. In the Manual Uploads tab, navigate to the Add Assets Manually section.

3. From the Actions menu, select Download CSV template.

   OT Security downloads the tot_Assets template document.

4. Open the `tot_Assets` template document.

5. Edit the `tot_Assets` template precisely in accordance with the instructions found in the file, leaving only the column headers such as Name and Type) and the values you provide.

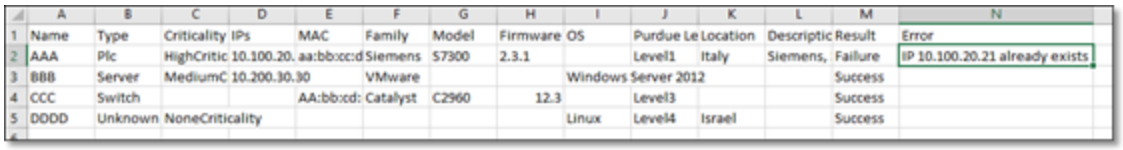
6. Save the edited file.

7. Return to the Assets Settings page.

8. From the Actions menu, select Upload CSV and navigate to and open the desired CSV file to upload it.

9. In Add Assets Manually, click Download Report.

A CSV file with report 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	Descriptic	Result	Error
2	AAA	Plc	HighCritic	10.100.20.	aa:bb:cc:d	Siemens	S7300	2.3.1		Level1	Italy	Siemens,	Failure	IP 10.100.20.21 already exists
3	BBB	Server	MediumC	10.200.30.	30	VMware			Windows	Server 2012			Success	
4	CCC	Switch			AA:bb:cd:	Catalyst	C2960	12.3		Level3			Success	
5	DDDD	Unknown	NoneCriticality						Linux	Level4	Israel		Success	

SCD Files

The Substation Configuration Description (SCD) file includes the complete communication-related details for a substation. You can now upload an SCD file to OT Security and gain visibility into your assets, IEC 61850 configuration and security insights about your environment.

Based on the SCD file information, OT Security reports findings related to substation misconfiguration such as:

- Access to Manufacturing Message Specification (MMS) reports from unauthorized clients.
- Unauthorized clients not mentioned in the SCD file trying to subscribe to MMS reports.

> Note: OT Security supports only the following formats for SCD files:
>
> - Substation Configuration Language (SCL) versions 1.0 and 2.0.
> - SCD files with only one substation.

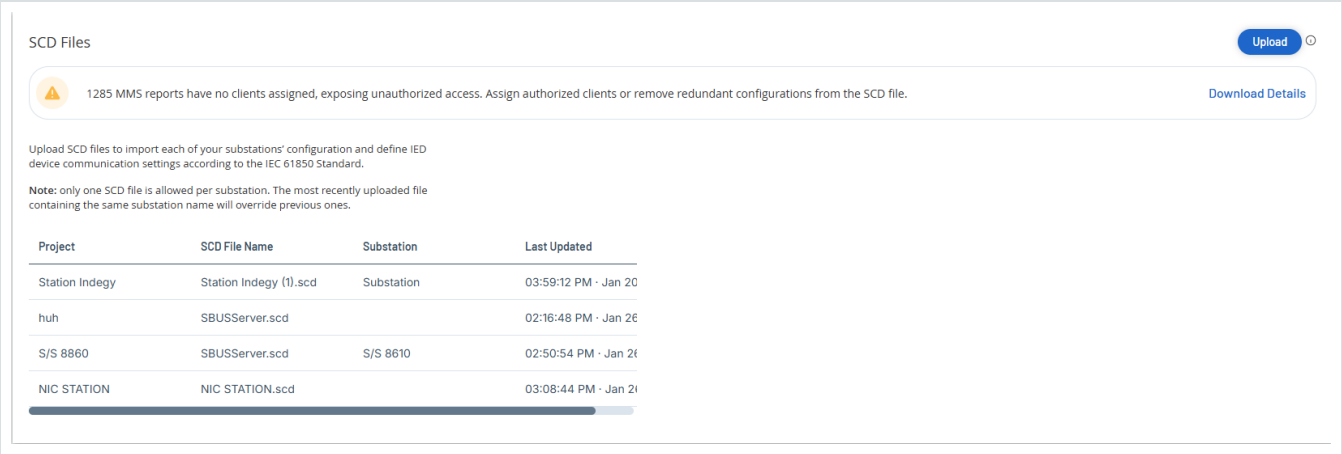
To upload an SCD file:

1. Go to Data Collection > Data Sources.

   The Data Sources page appears.

2. In the Manual Uploads tab, navigate to the SCD Files section.

3. In the SCD Files section, click Upload.



> Note: You can upload only one SCD file per substation. The most recently uploaded file containing the same substation name overrides previous one.

4. Browse and select the file to upload.

   OT Security uploads the SCD file and you can view the asset details in the Inventory > Details and IEC 61850 tabs. Any misconfiguration in the SCD file triggers an event and an unauthorized access error message appears at the top of the Details and IEC 61850 pages.

5. (Optional) To download the findings details, in the error message, click Download Details.

   OT Security downloads the details in the CSV format.

Rockwell Project Files

You can upload Rockwell `.L5X` files to create assets, enrich asset details, and build relationship between assets in air-gapped or limited visibility environments. The maximum project file size is 50 MiB.

> Important: By default, the `ProjectFilePopulatePrimaryLayerAssetIPs` is set to `True` and `ProjectFilePopulateNonPrimaryLayerAssetIPs` is set to `False`. When uploading multiple project files containing assets with identical IP addresses, setting the `ProjectFilePopulateNonPrimaryLayerAssetIPs` configuration parameter to `True` resolves duplicate assets. This allows the system to display the IP addresses of assets in the non-primary

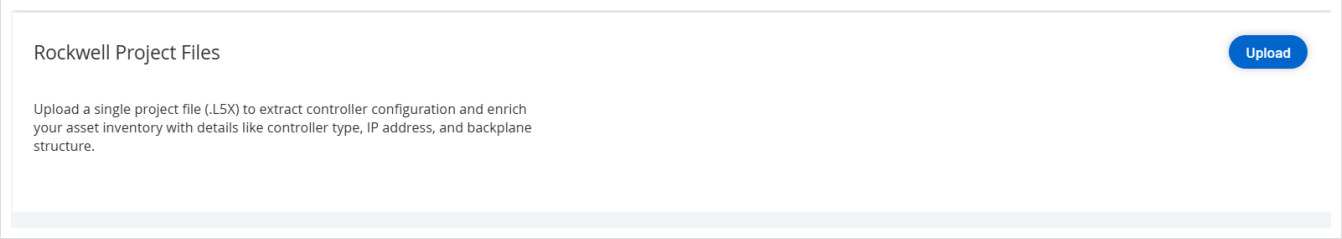
ayer, enabling you to resolve assets with the same IP address as a single asset and place them orrectly on the same backplane. For changing the configuration, contact Tenable Support.

To upload a Rockwell file:

1. Go to Data Collection > Data Sources.

   The Data Sources page appears.

2. In the Manual Uploads tab, navigate to the Rockwell Project Files section.



3. Click Upload.

4. Browse and select the file to upload.

   OT Security uploads the Rockwell project file and you can view the asset details in the Inventory > Details tab.

Settings

The Settings section in OT Security includes most of the configuration pages for OT Security:

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. See Generate API Keys.
- License – View, update, and renew your license. See License.

Environment Settings

- **Network Definitions**
    - Passive Monitoring – Enable passive monitoring to allow OT Security to discover assets. See Passive Monitoring.
    - Update Asset Details Using CSV – Update the details of your assets using a CSV template. See Update Asset Details Using CSV.
    - 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 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.

- Monitored Network – View and edit the aggregation of IP ranges in which the system classifies assets. See Monitored Networks.
- 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:
  - Factory Reset – Returns all settings to the factory defaults. Only an Administrator or Security Manager can perform a factory reset.

    > Caution: This operation cannot be undone and all data in the system will be lost.

    The following options are now available from Tenable Core:

- 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.

- System Log – Shows a log of all system events that occurred in the system. For example, Policy turned on, Policy edited, and Event Resolved. You can export the log as a CSV file or send it to a Syslog server. See System Log.

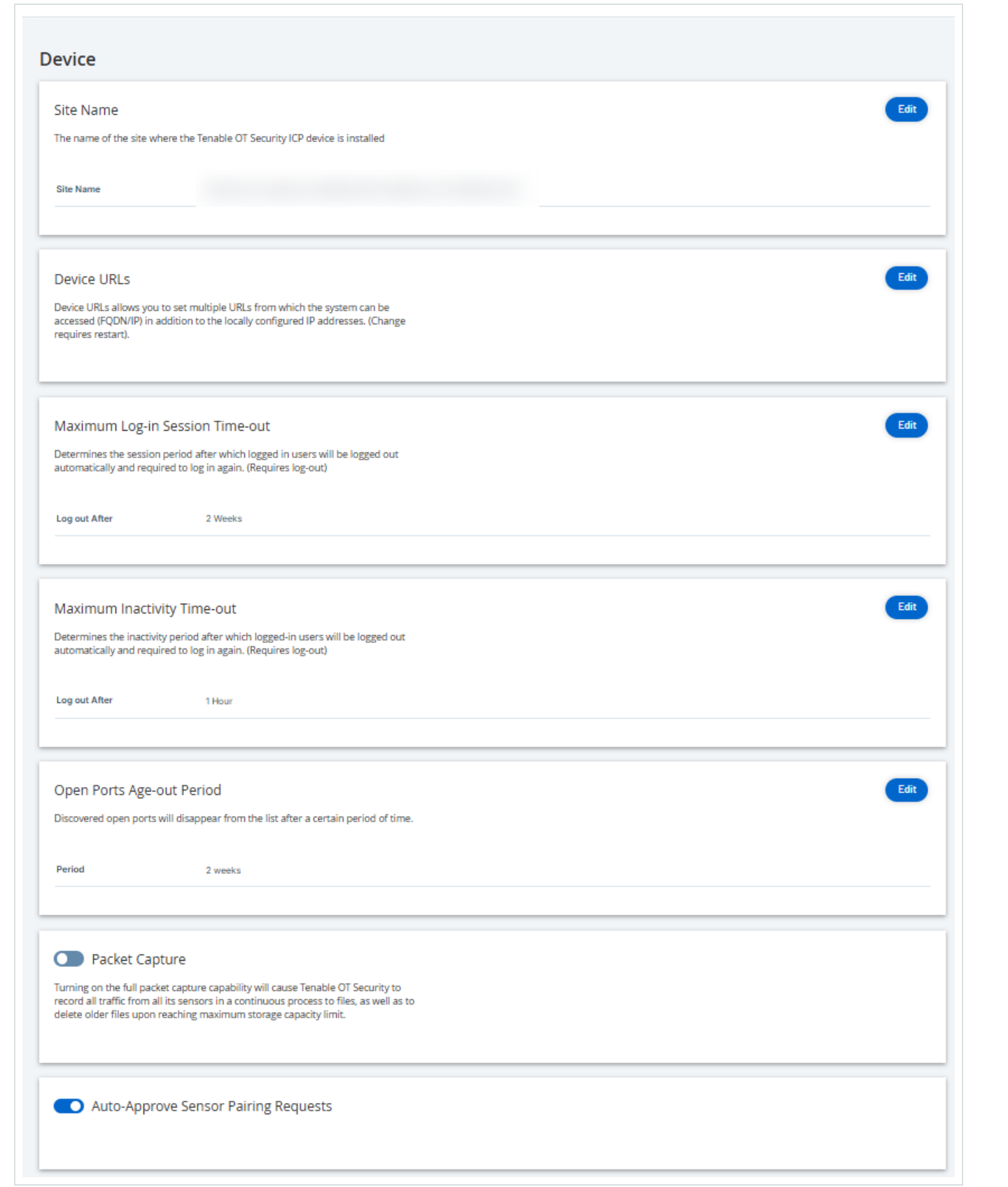
System Configuration

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

> Required OT Security User Role: Administrator, Supervisor

The Device page shows detailed information about your OT Security configuration. You can view and edit the configuration in this page.


Device
Site Name
Edit
The name of the site where the Tenable OT Security ICP device is installed
Site Name
Device URLs
Edit
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).
Maximum Log-in Session Time-out
Edit
Determines the session period after which logged in users will be logged out automatically and required to log in again. (Requires log-out)
Log out After
2 Weeks
Maximum Inactivity Time-out
Edit
Determines the inactivity period after which logged-in users will be logged out automatically and required to log in again. (Requires log-out)
Log out After
1 Hour
Open Ports Age-out Period
Edit
Discovered open ports will disappear from the list after a certain period of time.
Period
2 weeks
Packet Capture
Turning on the full packet capture capability will cause Tenable OT Security to record all traffic from all its sensors in a continuous process to files, as well as to delete older files upon reaching maximum storage capacity limit.
Auto-Approve Sensor Pairing Requests

Site 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.

Maximum Log-in Session Time-out

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 Time-out

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.

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

Starting from version 4.1, you can review and configure the split ports Tenable Core interface on port 8000.

Set Compliance Dashboard Preferences

> Required OT Security User Role: Administrator, Supervisor

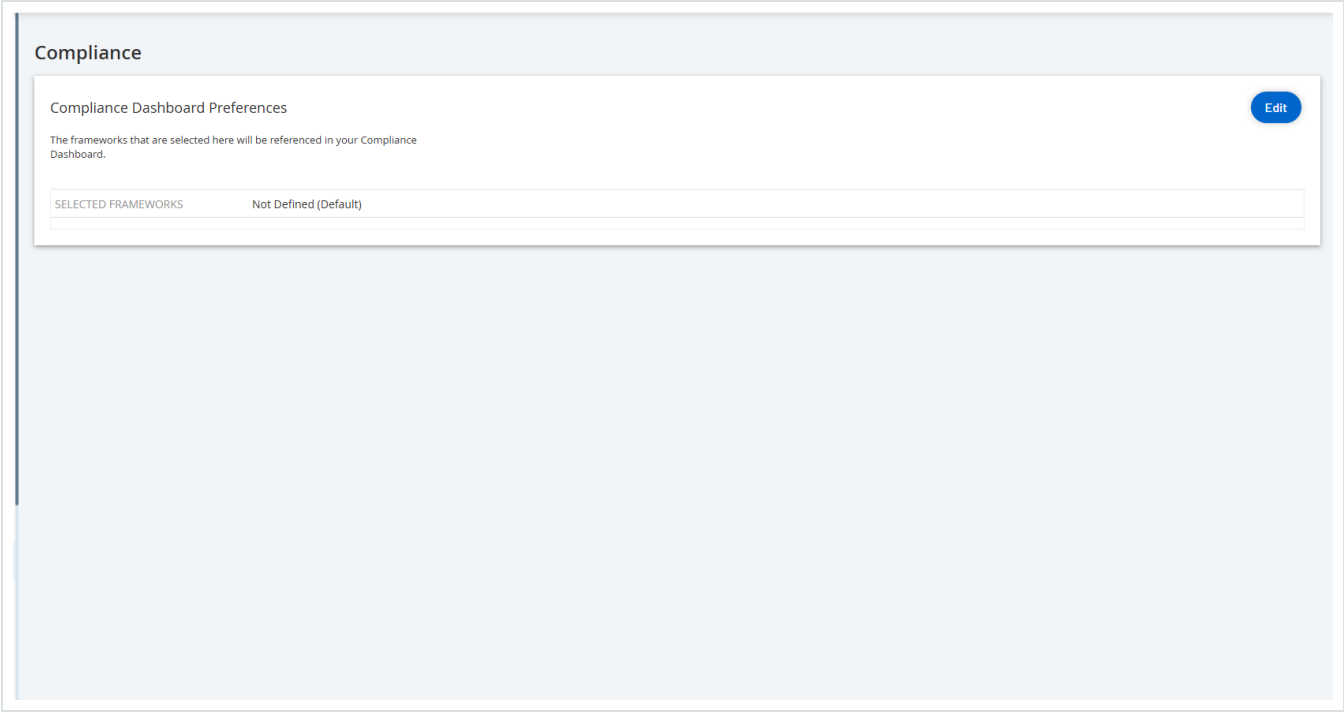
You can specify the security frameworks that the Compliance dashboard refers to when generating the data.

To set the compliance dashboard preferences:

1. Do one of the following:

    - Go to 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)
   - NERC-CIP Requirements
   - IEC-62443-3-3 Requirements

4. Click Save.

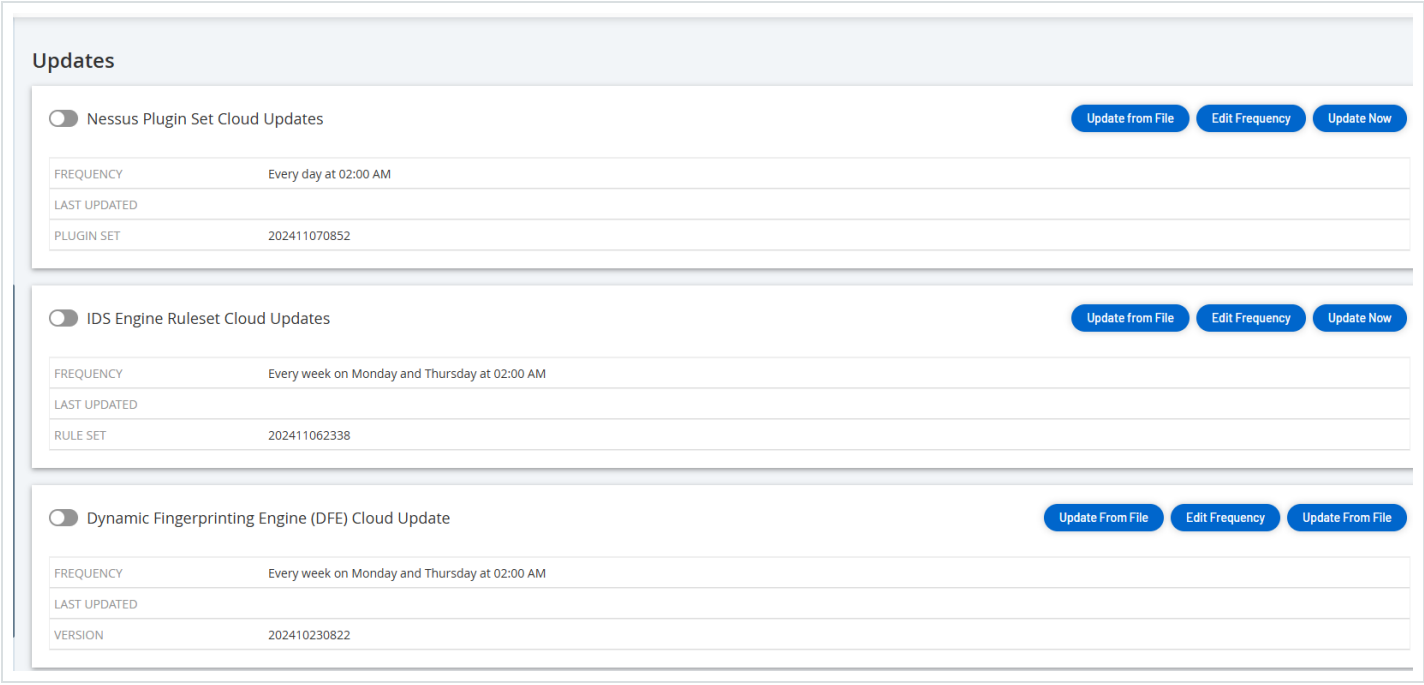
OT Security saves the compliance framework preferences and checks your organization's compliance against the specified preferences. OT Security displays the results from the compliance checks on the Compliance dashboard.

Updates

Required OT Security User Role: Administrator, Supervisor, Security Manager

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, and coverage 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.



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

To enable automatic updates of plugins:

1. Go to 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

1. Go to 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.

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 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 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

To enable automatic updates of the IDS Engine Ruleset:

1. Go to 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

1. Go to 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 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.

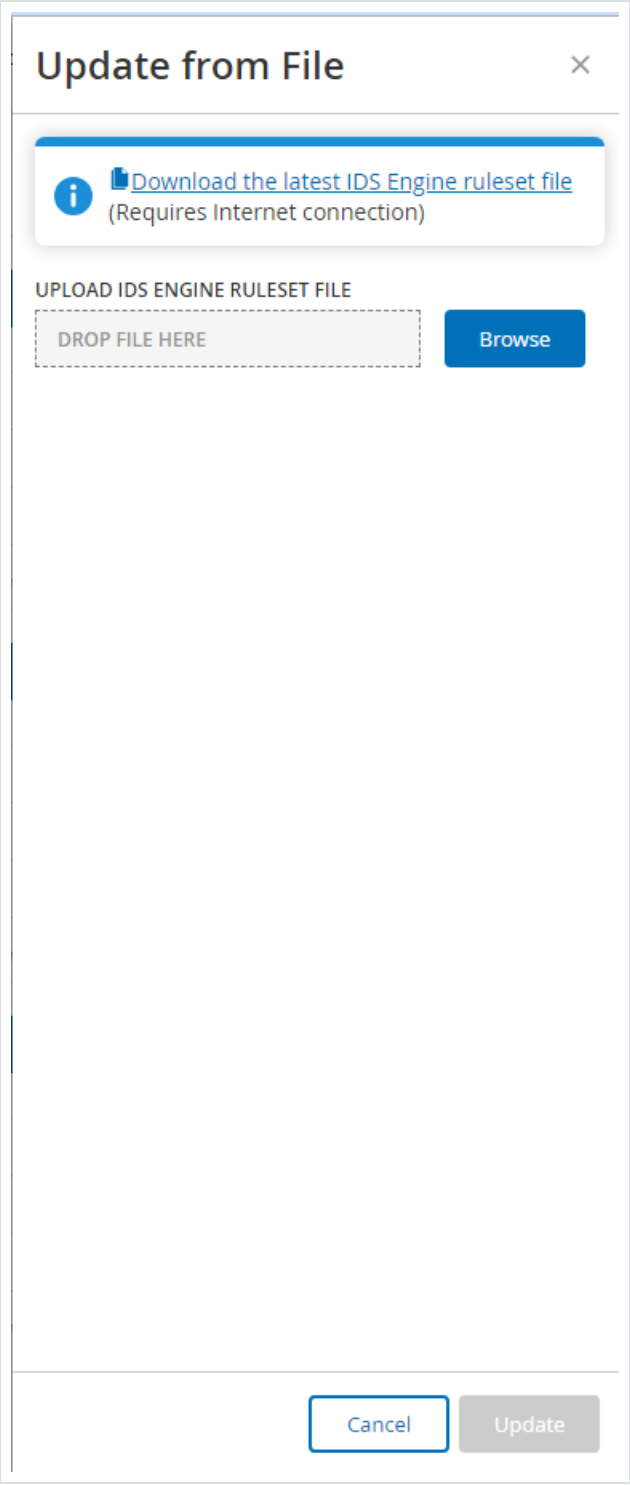
To update the IDS Engine Ruleset offline:

1. Go to 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

To enable automatic DFE updates:

1. Go to 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

1. Go to 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 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.

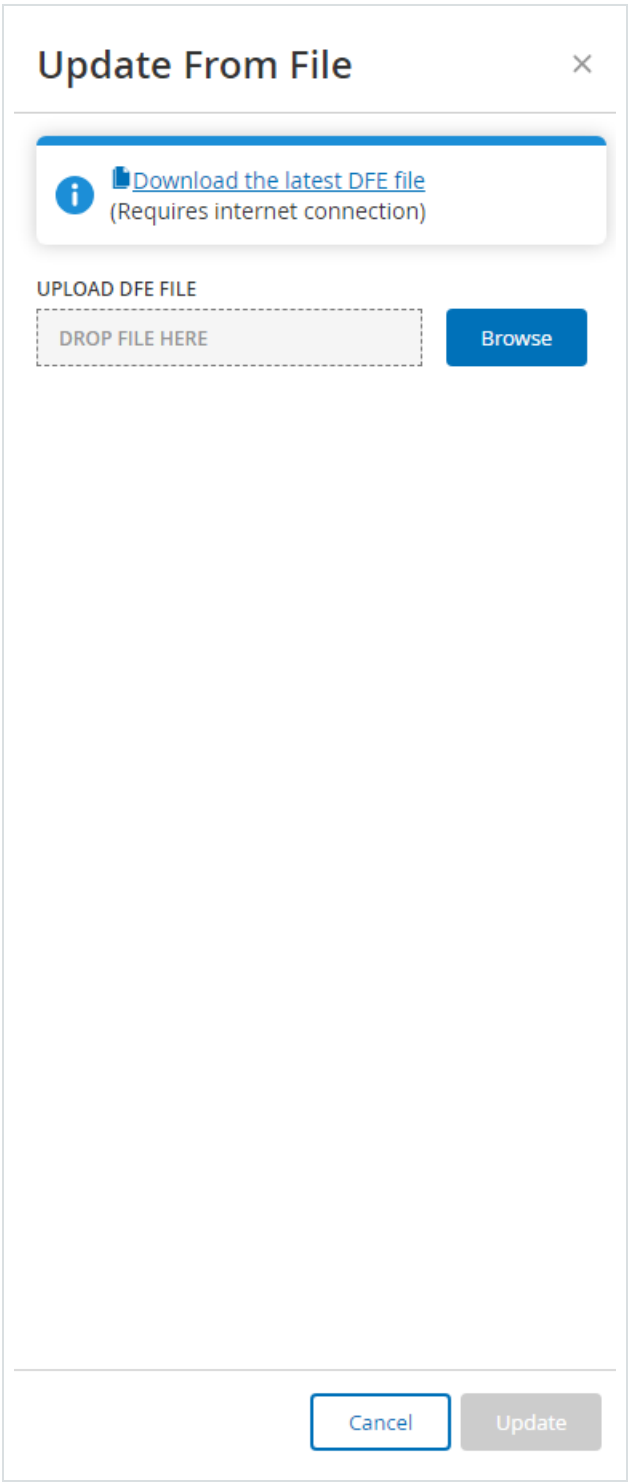
To perform an offline DFE update:

1. Go to 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.

OT Discovery Engine (OTD) Updates

> Required OT Security User Role: Administrator, Supervisor, and Security Analyst

OT Agents use the OT Discovery (OTD) engine for scanning your environment. You can update the OTD engines either manually or automatically from the Data Sources > Agents page. Before updating the OTD engine, you must first upload the latest OTD file to OT Security.

Before you Begin

- Download the OT Discovery (OTD) engine file from the downloads portal.

To upload the OTD engine file:

1. Go to Settings > System Configuration > Updates.

   The Updates page appears.

2. In the OT Discovery Engine (OTD) Update section, click Upload.

   The Upload File panel appears.

3. Click Browse and navigate to the OTD engine file you downloaded from the Tenable downloads portal.

4. Click Upload.

5. To update the OTD engine, follow the steps in Update the OT Agent.

Certificates

> Required OT Security User Role: Administrator

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.

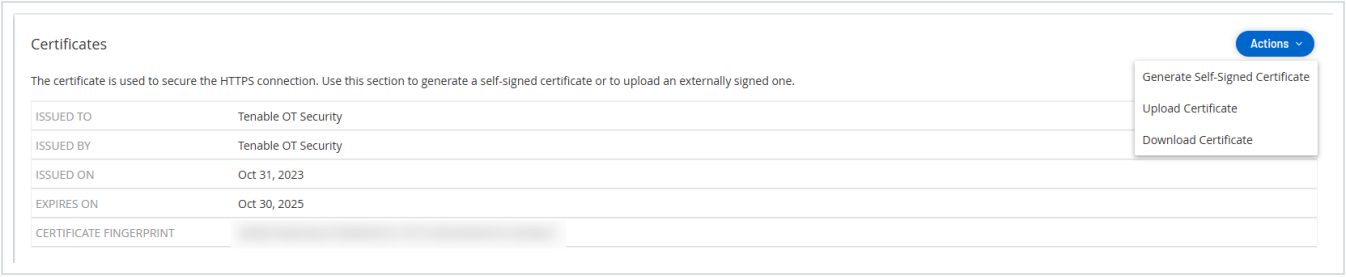
> Note: Generating a new certificate overrides the current certificate.

To generate a self-signed certificate:

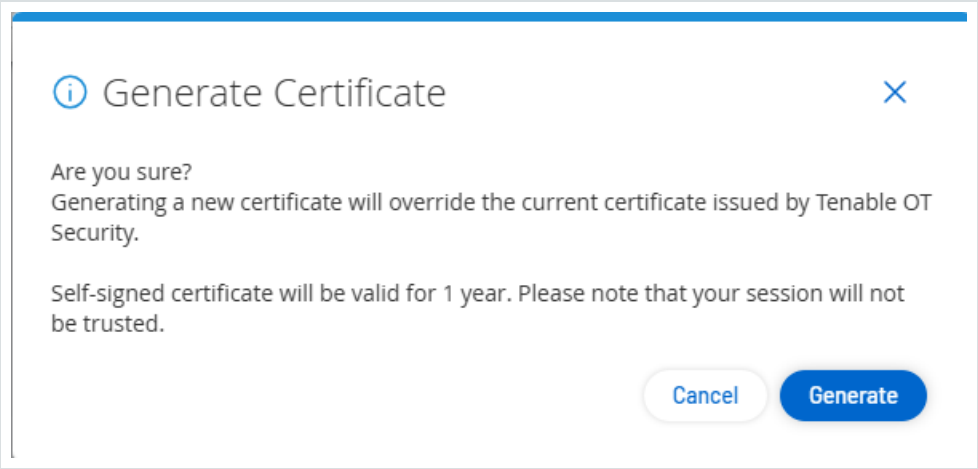
1. Go to Settings > System Configuration > Certificates.

   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 Certificates page.

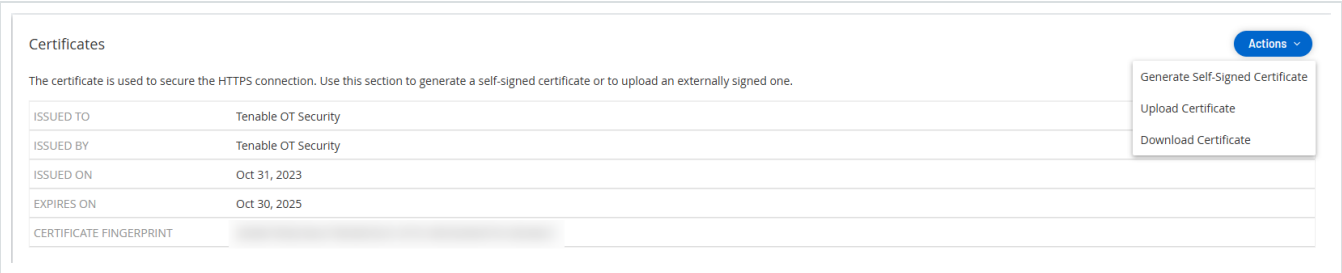
Upload an HTTPS Certificate

To upload an HTTPS Certificate:

1. Go to Settings >System Configuration > Certificates.

   The Certificates window appears.

2. From the Actions menu, select Upload Certificate.



   The Upload Certificate side panel appears.

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.

Generate API Keys

> Required OT Security User Role: Administrator, Supervisor, Security Manager, Security Analyst, Site Operator, Read Only

Generating an API key can help integrate OT Security with other security tools and systems within your organization.

To generate API keys in OT Security:

1. Go to Settings > System Configuration > API Keys.

   The API Keys page appears.
2. In the upper-right corner, click Generate Key.

   The Generate Key panel appears.
3. In the Expiration Period box, select the number of days after which the API key can age out.
4. In the Description box, type a description for the API key.

5. Click Generate.

   The Generate Key panel appears with the ID and API Key.

6. Click the button to copy the API key.

7. Click Done.

   The API Keys page appears with the newly added API key ID.

Pair ICP with Enterprise Manager

Required OT Security User Role: Administrator, Supervisor

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.

Note:Once paired with EM, all updates must be done at the EM level so that the sites and their sensors receive the latest version updates.

Before you Begin

Make sure that:

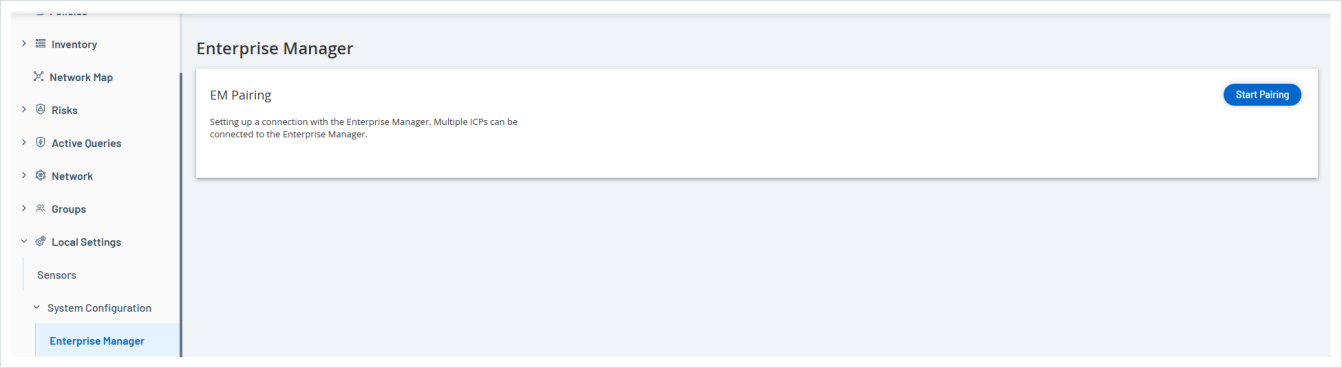
- OT Security EM can connect via API to the ICP.
- Make sure TCP 443 and TCP 28305 are open for communication from ICP to OT Security EM.
- HTTPS connections exist between ICP and OT Security EM.
- (Optional) Generate an API Key in OT Security EM.

  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 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	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.

	Tip: You can skip this step and manually approve the certificate from the EM Pairing page. Note: You can access the Certificates page from Local Settings > System Configuration in OT Security EM.
Pair using API Key	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. Tip: You can skip this step and manually approve the certificate from the EM Pairing page. Note: You can access the Certificates page from Local Settings > System Configuration in OT Security EM.

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

Required OT Security User Role: Administrator, Supervisor

You can disconnect the ICP pairing from the EM or the ICP when the pairing is no longer needed.

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.

Disconnect an ICP pairing from OT Security

1. In OT Security, go to 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 Settings

Network Definitions

> Required OT Security User Role: Administrator, Supervisor, Site Operator

The Network Definitions page includes the following sections:

- Passive Monitoring
- Duplicated Internal Networks
- Discover New Assets via SNMP
- Fetch IP Address for IoT Assets

Passive Monitoring

Passive monitoring is disabled during the initial configuration of OT Security. Tenable recommends that you finish setting up your monitored networks before you enable passive monitoring. This helps you reduce an alert overload with too many initial alerts and security events.

Duplicated Internal Networks

> Required OT Security User Role: Administrator, Supervisor

Overlapping IP ranges occur when an IP address is assigned to multiple devices. Overlapping IP ranges are common across manufacturing environments, leading to challenges in accurately

identifying and tracking assets, resulting in visibility gaps and incorrect asset associations. You can define your overlapping networks for OT Security to track assets accurately even when IP addresses are reused across different segments.

> Note: If an asset in a duplicated network is detected by both a sensor and another source (such as another sensor or the ICP locally), the OT Security interface merges it into a single asset. However, licensing counts it as two assets. To prevent this, Tenable recommends adjusting the duplicated network range to exclude such assets.

Add a Duplicated Network

Before you Begin

- Make sure you have paired authenticated sensors.

  > Note: OT Security does not support duplicated networks on unauthenticated sensors.

To define the duplicate networks in your environment:

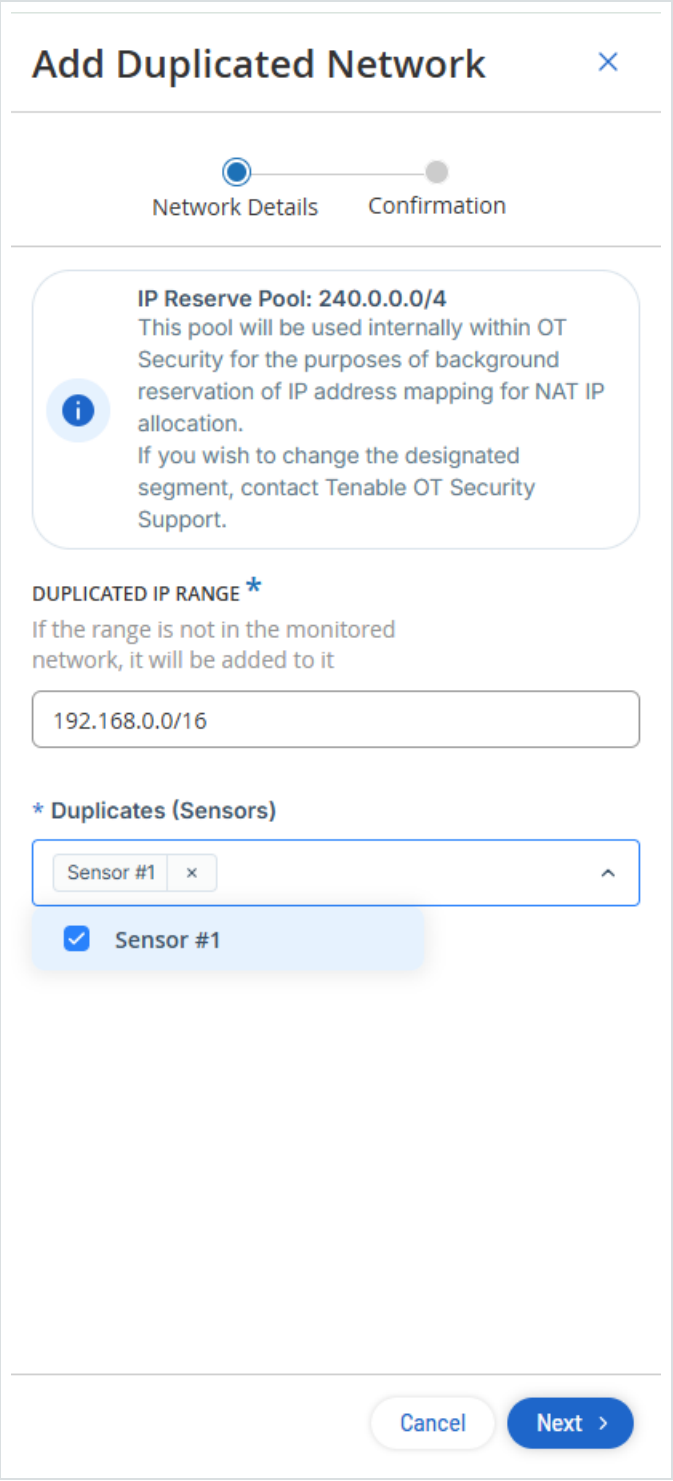
1. Go to Settings > Environment Settings > Network Definitions.

   The Network Definitions page appears.

2. In the Duplicated Internal Networks section, click Add Network.

   The Add Duplicated Network panel appears with the Network Details.

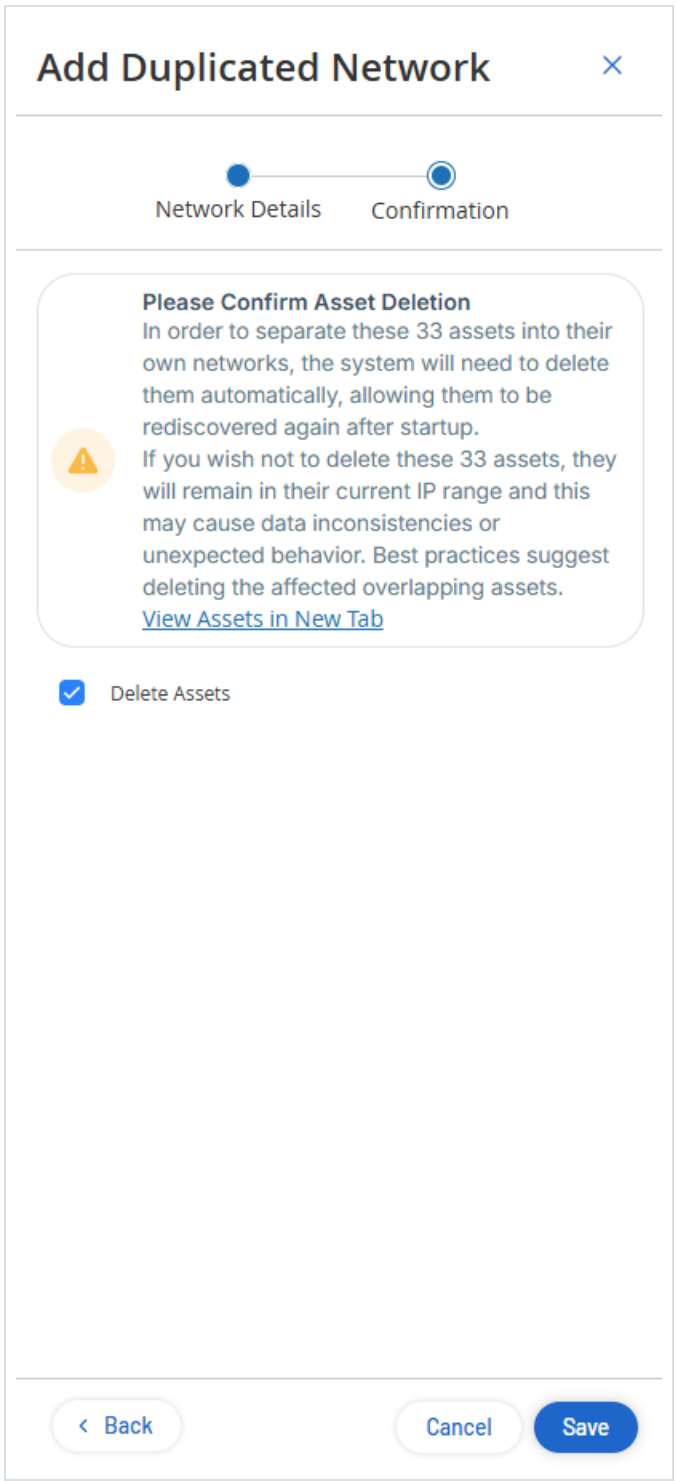
   > Note: OT Security uses the 240.0.0.0/4 IP range as the internal reserve pool for mapping IP addresses to NAT IP allocation. To change this reserve pool range, contact Tenable Support.



3. In the Duplicated IP Range box, type the IP range in the CIDR format, for example, 192.168.0.0/24.

4. From the Duplicates (Sensors) drop-down box, select the sensors associated with the duplicated IP range.
5. Click Next.

   The Confirmation panel appears.

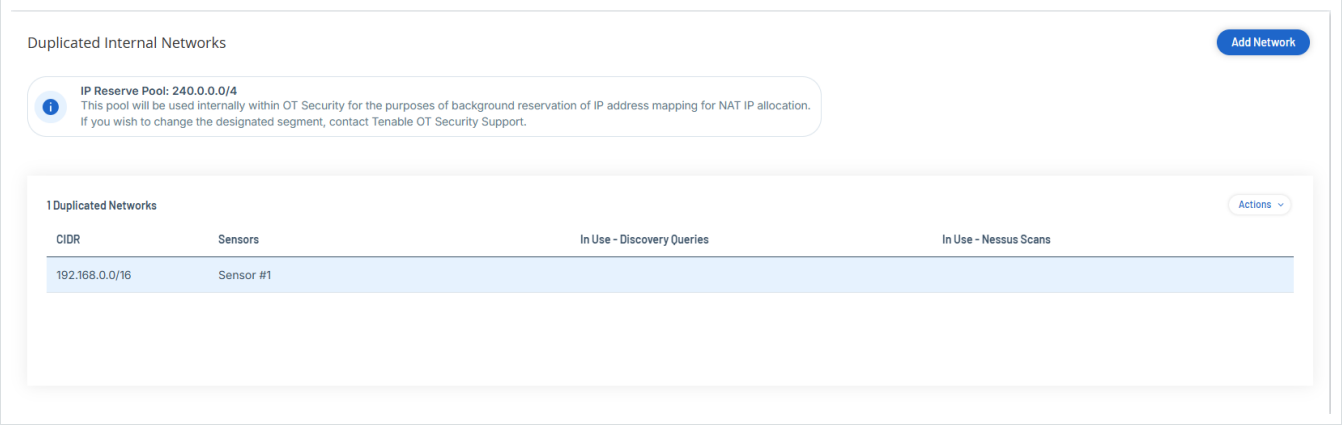


6. (Optional) Select the Delete Assets checkbox.

Tip: To separate all the selected assets into their own networks, Tenable recommends that you allow OT Security to delete the assets and rediscover them after startup. If you do not select the Delete Assets checkbox, the assets remain in the current IP range and may cause inconsistencies or unexpected behavior.

7. Click Save.

   OT Security saves the duplicate IP range and it appears in the Duplicated Internal Networks table.



Important: Once you complete configuring duplicated networks, Tenable recommends that you restart OT Security before enabling the sensors.

8. Restart OT Security.

9. To enable sensors, go to Settings > Sensors:

Note: The IP ranges (CIDRs) for the active query are the ones that you configured in the Duplicated Internal Network settings.

   1. Do one of the following:

      - Single sensor: Right-click the sensor and click Edit. In the Edit Sensor panel, click the Sensor active queries toggle to enable active queries.

- Multiple sensors: Select all the required sensors. In the header, select Bulk Actions > Enable Active Queries.

2. Right-click the sensors and activate them by changing the status from Paused to Connected.

Next Steps

After configuring the duplicated networks and restarting OT Security, the assets appear with their actual IPs in the All Assets table. Additionally, when entering an IP assigned to a duplicated network, you must select the corresponding Sensor. For example: in Active query > Discovery / Nessus Scan > Create Scan, or in Credentials > Test Credentials:

- In Inventory > All Assets, view the real IP addresses and the Source of assets in the All Assets table. For instance, two assets that share the same IP address but are associated with different sensors.
- In Active Queries > Queries Management > Discovery or Nessus Scans > Create Scan, when configuring an active query involving duplicated networks, select the Relevant Sensors for that IP range. This allows you to run the query for assets associated with a specific sensor while excluding the other sensors.

  > Note: OT Security enables the Relevant Sensors box only for IP ranges in duplicated networks. It remains disabled for all other IP ranges.

- In Active Queries > Credentials > Test Credentials when configuring credentials, if you input an IP range in duplicated network, you must also select the associated sensors in the Duplicate (Sensor) box.
- To create Asset Groups for assets part of duplicated networks, use the Asset Selection option and identify the specific IP based on the Source column in the Assets table.

Duplicated Internal Networks table

The Duplicated Internal Networks table shows the following details:

Column	Description
CIDR	The duplicated network IP range.
Sensors	The sensors associated with the duplicated network IP range.
In Use - Discovery Queries	Indicates if the CIDRs are in-use in at least one Asset Discovery (active query). If yes, remove the CIDR Active Discovery before deleting the duplicated network that contains that CIDR.
In Use - Nessus Scans	Indicates if the CIDRs are in-use in at least one Nessus Scan. If yes, remove the CIDR from the Nessus Scan before deleting the duplicated network that contains that CIDR.

Actions on Duplicated Internal Networks

Edit a Duplicated Network

You can modify the duplicated network configuration as needed.

To edit a duplicated network:

1. In the Duplicated Internal Networks section, select the duplicated network to modify.
2. Do one of the following:
   - Right-click the duplicated network and select Edit.
   - In the upper-right corner of the section, select Actions > Edit.

   The Edit Duplicated Network panel appears with the details of the selected duplicated network.
3. Modify the values as needed.
4. Click Next.

5. In the Confirmation panel, click Save.

   OT Security saves the changes to the duplicated network.

Delete a Duplicated Network

You can delete duplicated networks that you no longer need.

To delete a duplicated network:

1. In the Duplicated Internal Networks section, select the duplicated network to delete.
2. Do one of the following:
   - Right-click the duplicated network and select Delete.
   - In the upper-right corner of the section, select Actions > Delete.

OT Security deletes the duplicated network.

Delete a Sensor in-use in a duplicated network

To delete a sensor that is used in a duplicated network:

1. Remove the CIDRs from Nessus Scan / Active Discovery.
2. Delete the sensor from the duplicated network settings configuration.
3. In case of replacement, use API to set the new sensor ID and replace the old sensor.
4. In the Sensors page, delete the old sensor.

Discover New Assets via SNMP

When you enable the Discover New Assets via SNMP option, OT Security adds the assets discovered by SNMP queries to the assets inventory.

Fetch IP Address for IoT Assets

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, disable the Fetch IP Address for IoT Assets option. For more information, see Manage IoT Connectors.

Event Clusters

Required OT Security User Role: Administrator, Supervisor

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.

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 be part of the cluster.

To enable clustering:

1. Go to Settings > Environment Settings > Event Clusters.

   The Event Clusters page appears.

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.

Monitored Networks

Required OT Security User Role: Administrator, Supervisor

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.

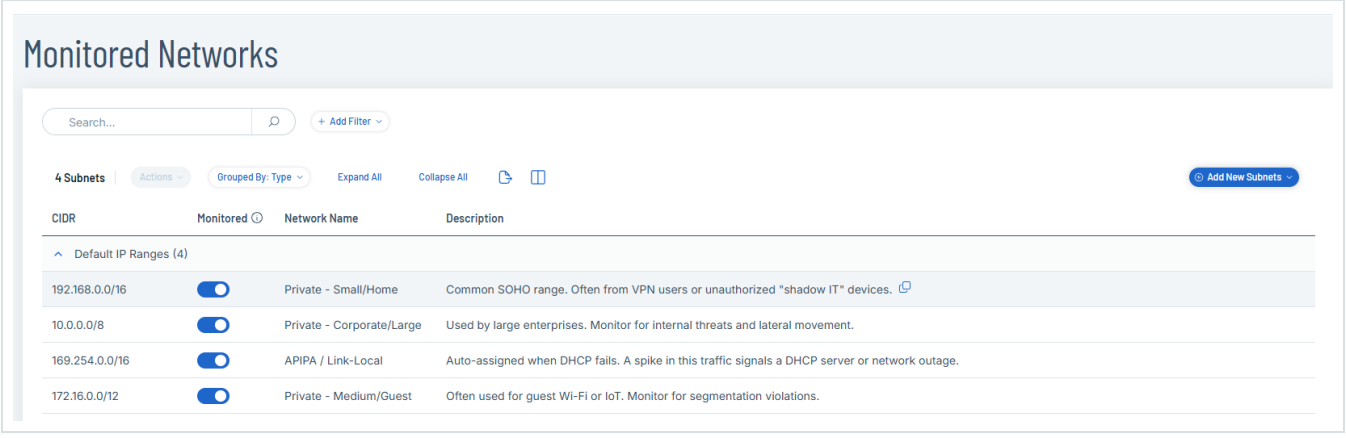
By default, OT Security configures three default public ranges: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16, as well as the link-local range of 169.254.0.0/16 (APIPA).

Caution: If you configure more than 5,000 unique monitored subnets, OT Security truncates the list to the first 5,000 entries. The system does not provide a notification when this truncation occurs.
For Nessus Network Monitor (NNM) components, OT Security processes only the first 128 entries.

To disable any of the default ranges or add ranges appropriate for your network:

1. Go to Settings > Environment Settings > Monitored Networks.

   The Monitored Networks page appears.



2. Go to Settings > Environment Settings > Network Management.

   The Network Management page appears with Monitored Networks as the default tab.

3. Customize tables as required. See Customize Tables.

4. The Monitored Networks table includes the following details:

Column	Description
Default IP Ranges and Custom IP Ranges	The Default IP Ranges section displays the default IP ranges configured in OT Security. The Custom IP Ranges section displays any IP range that you create.
CIDR	The CIDR column displays the IP addresses to monitor.
Monitored	Click to enable or disable the monitoring of the configured IP addresses.
Network Name	The name of the network.
Description	The description about the IP ranges.
	Hover over a value to display the Copy button. You can use this to copy the parameter value.

Add Subnets

You can add a subnet or a list of subnets for monitoring.

To add a new subnet:

1. In the left navigation menu, click Settings > Environment Settings > Monitored Networks.

   The Monitored Networks page appears.

2. In the upper-right corner, click Add New Subnets.

   A menu appears.

3. Select one of the following:

   - Add One Subnet – Select this option to add a single subnet.
   - Add Subnets List – Select this option to add a list of subnets.

   The Add Subnet panel appears.

4. If you selected Add One Subnet:

   a. In the CIDR box, type the IP address range. For example, `192.168.1.0/24`.

   b. Click the Monitored toggle to enable OT Security to capture traffic and execute active queries within the IP range.

   > Note: The Monitored toggle is enabled by default. To turn off monitoring, click to disable the Monitored toggle.

   c. (Optional) In the Network Name box, type a name for the network.

   d. (Optional) In the Description box, type a description for subnets.

   e. Click Save.

5. If you selected Add Subnets List, in the Add Subnets panel, do the following:

   a. In the CIDR box, provide the list of CIDRs, one CIDR per line.

   b. Click the Monitored (All Added Subnets) toggle to allow OT Security to capture traffic and execute active queries for all the listed subnets.

> Note: The Monitored toggle is enabled by default. To turn off monitoring, click to disable the Monitored (All Added Subnets) toggle.

c. Click Save.

OT Security saves the subnets and they appear on the Monitored Networks page.

Edit a Subnet

You can edit a subnet to make changes to it.

1. To edit a subnet, do one of the following:

   - In the Monitored Networks table, hover over the IP range row you want to edit.

     OT Security enables the Actions menu.

   - In the Monitored Networks table, right-click the row of the IP range you want to edit.

     A menu appears.

2. Select Edit Subnet.

   The Edit Subnet panel appears.

3. Make the changes needed.

4. Click Save.

   OT Security saves the changes to the subnets.

Scan Using Portable OT Agents

> Required OT Security User Role: Administrator

An OT agent in a portable state can discover assets in air-gapped, isolated, and complex OT environments, and then return results to OT Security for analysis.

The following interconnected capabilities allow agent scanning in complex air-gapped environments:

- Network Areas to anchor assets to logical or physical sites. For more information, see Network Areas.
- Agent in a disconnected portable state collects and packages discovery data and transfers it securely to the ICP without requiring a live connection.
- A native interface for field technicians to load scan profiles, track progress, run scans offline, and download results. The interface is also for pairing, and system log.

Key Concepts

The following entities work together to deliver portable OT discovery.

- Network Areas – A logical or physical container (for example, Building B) that anchors assets to a location. OT Security treats identical IP addresses in different network areas (duplicated networks) as separate, unique assets.
- OT Discovery Scan (OTD Scan) – The technical instruction set that you create through the OT Discovery scan wizard. The instruction set defines the scan credentials, and schedules.
- Subnet (Monitored Network) – A network range in CIDR notation (for example, 192.168.0.0/24) that defines the scope of discovery. OT Security does not create assets that fall outside the configured subnets.
- Source – Any entity that reports asset data, such as sensors, agents, local ICP, CSV uploads, or Packet Capture (PCAP) Player.

Agent States

The last connection to OT Security determines the state of an agent:

- Static – The agent has an active live connection to OT Security and receives scan configurations in real time.
- Portable – The agent last connected via a result upload without establishing a live connection. The agent operates independently in air-gapped environments and performs OT discovery without a network path to OT Security.

Portable State Agent Scan Workflow

Prerequisites

- Verify that you have Administrator permissions.
- Define your network area and subnets on the Network Areas page.

  > Note: Both the network area and the subnet must exist in OT Security before the agent returns results. If a result upload references a network area or subnet that does not exist, OT Security notifies you and holds the results. OT Security releases the results after you link them to an existing network area or create a new one.

- Install OT Agent.

Step 1: Define the OT Discovery Scan

You must first create an OTD scan using the OTD configuration wizard.

1. Go to Data Collection > Active Queries.

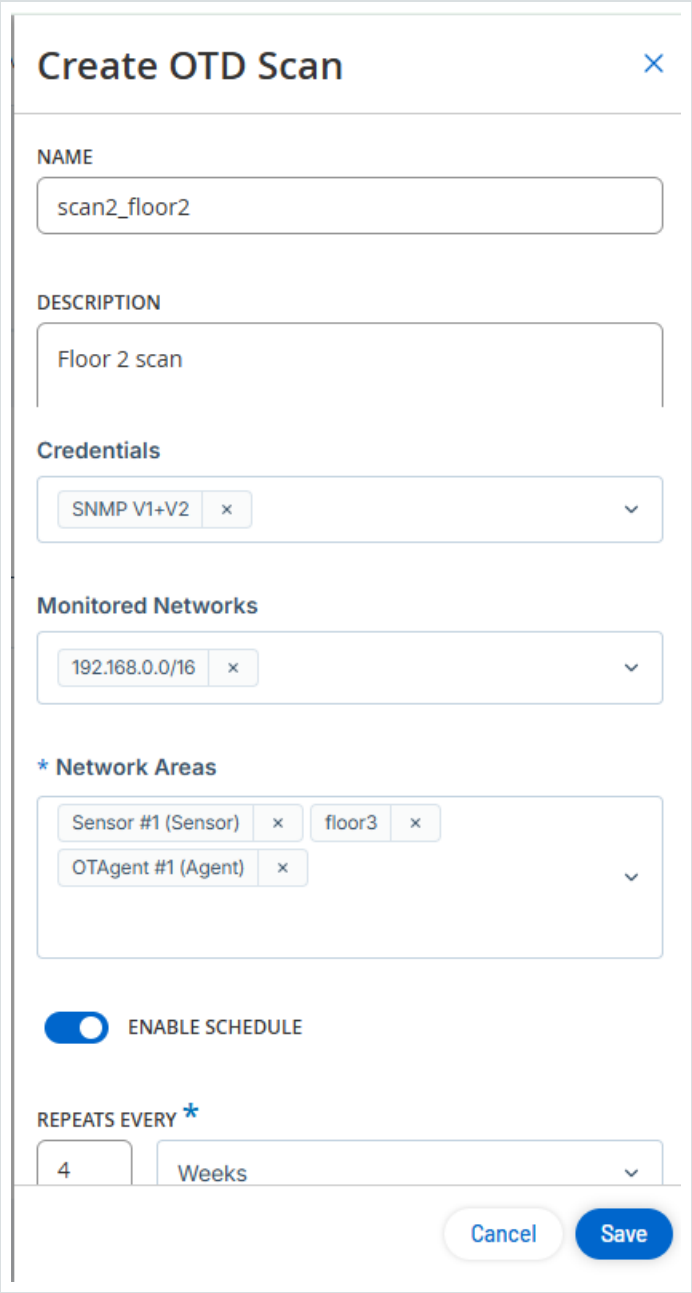
   The Active Queries Management page appears.

2. Click the OTD Scans tab.

   The OTD Scans page appears.

3. Click Create OTD Scan.

   The Create OTD Scan panel appears.



4. In the Name box, type a name for the scan.
5. In the Description box, type the context or details for the scan.
6. In the Credentials drop-down box, select the required credentials from the list.

Step 2 Link the Subnet and Network Area

Within the OTD scan wizard, you must link the subnet and network area.

1. In the Monitored Networks drop-down box, select one or more subnets for the scan or type a CIDR range.

   > Note: You can pre-populate subnets on the Monitored Networks page, or you can create them directly in this field by typing the CIDR range.

2. In the Network Areas drop-down box, select one or more network areas.

   > Note:You can pre-populate network areas on the Network Areas page, or you can create them directly in this field by typing a new name.

3. Define a schedule.

   a. Click the Enable Schedule toggle.

      The Repeats Every drop-down box becomes active.

   b. (Optional) Specify the interval minutes, hours, days, or weeks as required.

   c. In the On section, select the days you want to run the scan.

   d. In the At drop-down box, select the time at which you want to run the scan.

4. Click Save.

   OT Security saves the OTD Scan.

Step 3 Sync the Configuration to the Agent

1. Access your local OT Agent interface on Windows.

   > Note: The agent automatically syncs available scan configurations whenever it establishes a connection to OT Security.

2. Select the upload file that you want to run or pair with the ICP (static or online).

3. Select the network area where you want to run the scan.

Step 4 Run the Scan

1. Run the scan from the local agent interface. In the portable state, the agent performs OT discovery on the selected network without a live connection to Tenable OT Security.
2. View the progress of the scan in the execution log and download the results.

Step 5 Upload Results

Upload results through Manual Uploads in OT Security.

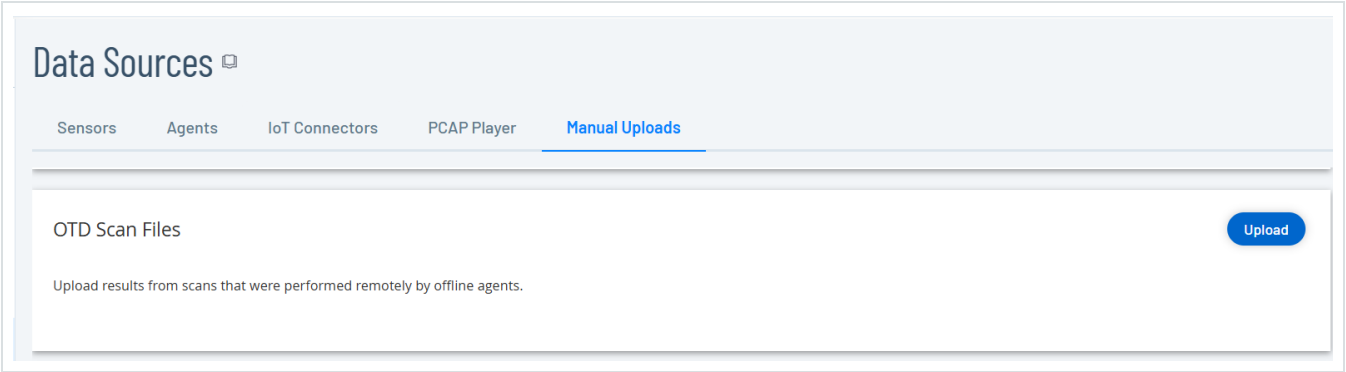
1. Go to Data Collection > Data Sources.

   The Data Sources page appears.

2. Click the Manual Uploads tab.

   The Manual Uploads page appears.

3. Navigate to the OTD Scan Files section and click Upload.



4. Browse to your local OTD scan results file and select it to upload.

   > Note: If you do not define the network area or subnet before this upload, OT Security notifies you. You must link the results to an existing network area or create a new one with a name that matches the same name as the results before the system populates your asset inventory.

5. View the imported asset data results in the Inventory page.

Monitored Networks

Required OT Security User Role: Administrator, Supervisor

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.

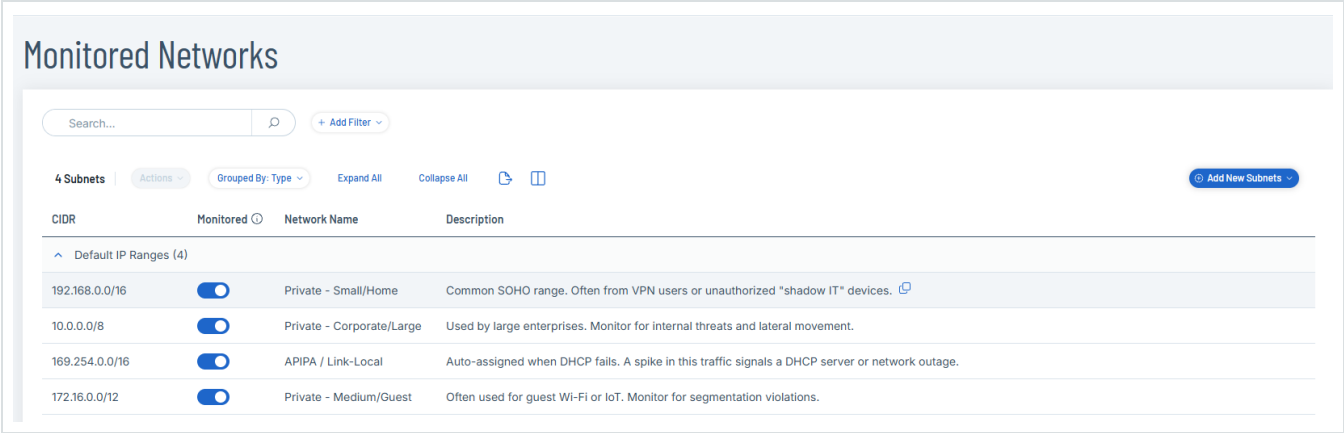
By default, OT Security configures three default public ranges: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16, as well as the link-local range of 169.254.0.0/16 (APIPA).

Caution: If you configure more than 5,000 unique monitored subnets, OT Security truncates the list to the first 5,000 entries. The system does not provide a notification when this truncation occurs.
For Nessus Network Monitor (NNM) components, OT Security processes only the first 128 entries.

To disable any of the default ranges or add ranges appropriate for your network:

1. Go to Settings > Environment Settings > Monitored Networks.

   The Monitored Networks page appears.



2. Go to Settings > Environment Settings > Network Management.

   The Network Management page appears with Monitored Networks as the default tab.

3. Customize tables as required. See Customize Tables.

4. The Monitored Networks table includes the following details:

Column	Description
Default IP Ranges and Custom IP Ranges	The Default IP Ranges section displays the default IP ranges configured in OT Security. The Custom IP Ranges section displays any IP range that you create.
CIDR	The CIDR column displays the IP addresses to monitor.
Monitored	Click to enable or disable the monitoring of the configured IP addresses.
Network Name	The name of the network.
Description	The description about the IP ranges.
	Hover over a value to display the Copy button. You can use this to copy the parameter value.

Add Subnets

You can add a subnet or a list of subnets for monitoring.

To add a new subnet:

1. In the left navigation menu, click Settings > Environment Settings > Monitored Networks.

   The Monitored Networks page appears.

2. In the upper-right corner, click Add New Subnets.

   A menu appears.

3. Select one of the following:

- Add One Subnet – Select this option to add a single subnet.
- Add Subnets List – Select this option to add a list of subnets.

The Add Subnet panel appears.

4. If you selected Add One Subnet:
   a. In the CIDR box, type the IP address range. For example, `192.168.1.0/24`.
   b. Click the Monitored toggle to enable OT Security to capture traffic and execute active queries within the IP range.

      > Note: The Monitored toggle is enabled by default. To turn off monitoring, click to disable the Monitored toggle.

   c. (Optional) In the Network Name box, type a name for the network.
   d. (Optional) In the Description box, type a description for subnets.
   e. Click Save.
5. If you selected Add Subnets List, in the Add Subnets panel, do the following:
   a. In the CIDR box, provide the list of CIDRs, one CIDR per line.
   b. Click the Monitored (All Added Subnets) toggle to allow OT Security to capture traffic and execute active queries for all the listed subnets.

      > Note: The Monitored toggle is enabled by default. To turn off monitoring, click to disable the Monitored (All Added Subnets) toggle.

   c. Click Save.

OT Security saves the subnets and they appear on the Monitored Networks page.

Edit a Subnet

You can edit a subnet to make changes to it.

1. To edit a subnet, do one of the following:

    - In the Monitored Networks table, hover over the IP range row you want to edit.

      OT Security enables the Actions menu.

    - In the Monitored Networks table, right-click the row of the IP range you want to edit.

      A menu appears.

2. Select Edit Subnet.

   The Edit Subnet panel appears.

3. Make the changes needed.

4. Click Save.

   OT Security saves the changes to the subnets.

Network Areas

> Required OT Security User Role: Administrator

Network Areas map your subnets to their physical location. This mapping helps differentiate between scan data from overlapping IP ranges across different physical locations.

The Network Areas page displays all network areas configured in your system. Network areas fall into two distinct categories:

- Automatic: Created by the system when you register a sensor or static agent.
- Manual: Created by an administrator as a placeholder for a portable agent scan.

Use the Network Areas page to create categories for grouping your subnets.

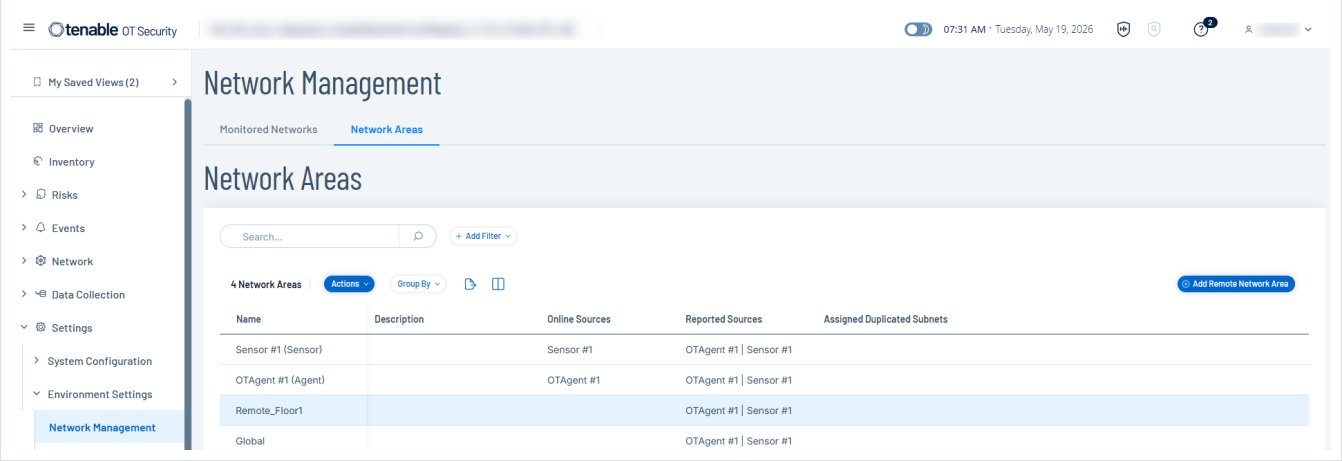
View Network Areas

1. Go to Settings> Environment Settings > Network Management.

   The Network Management page appears. The default tab is Monitored Networks.

2. Click the Network Areas tab.

   The Network Areas page appears and lists all the sensors and agents configured in your ICP.



The Network Areas table includes the following details:

Column	Description
Name	A unique identifier for the network area.
Description	A brief description of the network area.
Online Sources	All online entities associated with this network area.
Reported Sources	All reporting entities associated with this network area.
Assigned Duplicated Subnets	Displays the CIDR range and a counter showing the network area's position among all network areas that share that subnet. For example, if five network areas share one subnet, the column displays 1/5, 2/5, 3/5, 4/5, 5/5

	respectively for each subnet.
In-Use	Indicates whether this network area is actively used in any Nessus scans or OT Discovery (OTD) scans. A network area marked In-Use cannot be deleted until it is removed from all associated scans.

Add Remote Network Areas

1. Go to Settings > Environment Settings > Network Management.

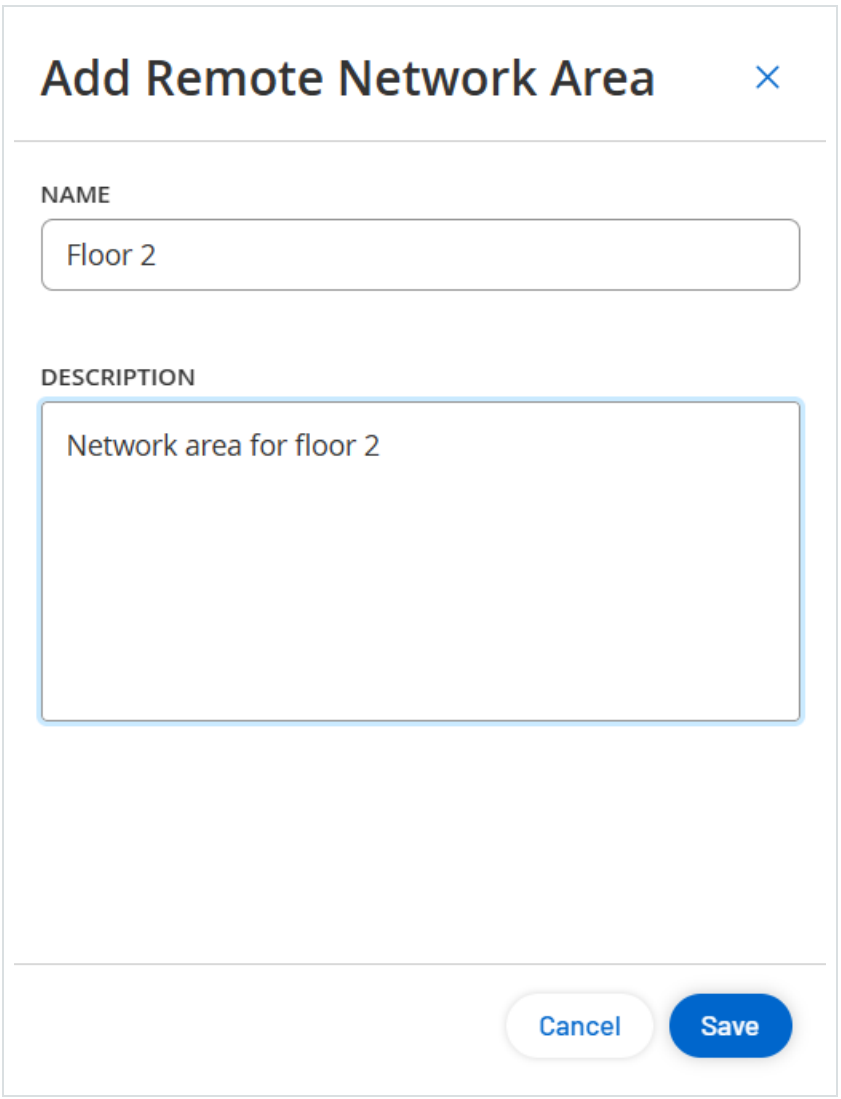
   The Network Management page appears.

2. Click the Network Areas tab.

   The Network Areas page appears.

3. In the upper-right corner, click Add Remote Network Area.

   The Add Remote Network Area panel appears.



4. In the Name box, type a name for the remote area.
5. In the Description box, type a description for the remote area you are defining.
6. Click Save.

   OT Security saves the remote network area.

Move Sources to a Network Area

You can group multiple sources under a single network area. For example, if a specific floor or building is monitored by three different sensors, you can group them under one network area. If you

have two buildings where each building contains four sensors, you only need to configure two network areas (one per building) instead of eight separate areas.

To combine multiple reporting sources into a single network area:

1. In the Network Areas table, do one of the following:

    - Select the network area from which you want to move sources.

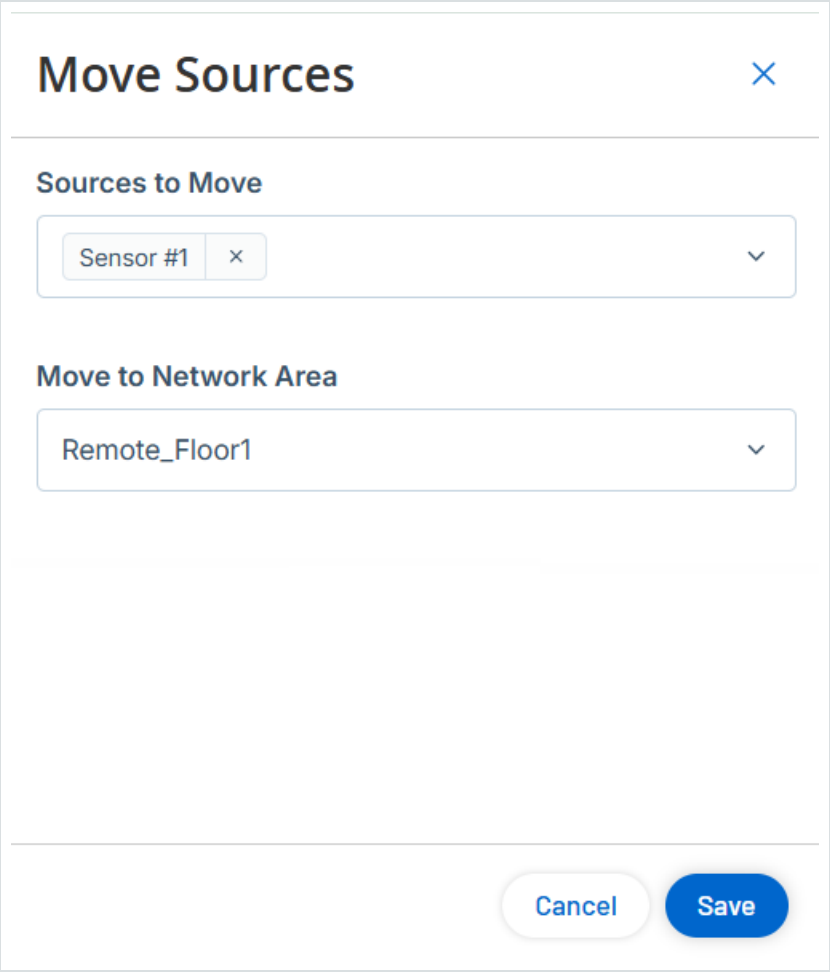
      OT Security enables the Actions menu in the header.

    - Right-click the network area from which you want to move sources.

      A menu appears.

2. Select Move Sources.

    The Move Sources panel appears.



3. In the Sources to Move drop-down box, select one or more sources to move.
4. In the Move to Network Area drop-down box, select the target network area from the list.
5. Click Save.

   OT Security moves the selected sources to the specified network area.

Edit Remote Network Area

You can edit the name and description of an existing remote network area.

1. In the Network Areas table, do one of the following:

    - Select the network area you want to edit.

      OT Security enables the Actions menu in the header.

    - Right-click the network area you want to edit.

      A menu appears.

2. Select Edit Details.

   The Edit Details panel appears.

3. Modify the details as needed.

4. Click Save.

   OT Security saves your modifications, and the updated details appear in the Network Areas table.

Delete Remote Network Area

You can delete remote network areas that you no longer need.

> Note: You cannot delete a network area that is currently marked as In-Use. To delete a network area, you must remove all sources associated with it and ensure it is removed from all active Nessus and OT Discovery scans.

To delete a network area:

1. In the Network Areas table, do one of the following:

    - Select the network area you want to delete.

      OT Security enables the Actions menu in the header.

- Right-click the network area you want to delete.

  A menu appears.

2. Select Delete.

   OT Security deletes the selected network area.

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 and Site Operators User Group > Site Operator role. 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

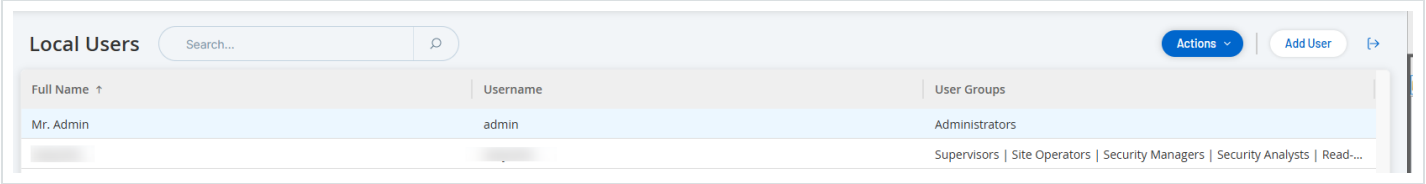
> Required OT Security User Role: Administrator

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.



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 Settings > User Management > Local Users.
2. Click Add User.

   The Add User pane appears.
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, such as Administrators User Group > Administrator role, Site Operators User Group > Site Operator role. 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 Settings >User Management > Local User.

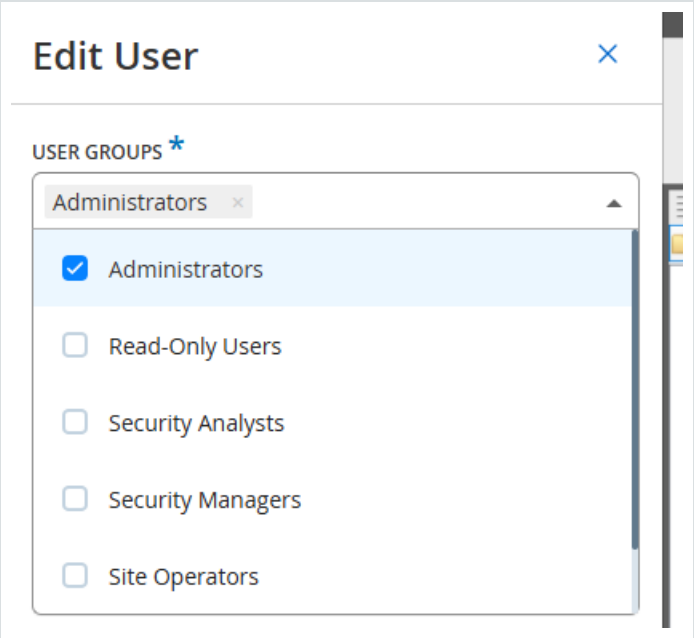
   The Local Users page appears.

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 Settings > User Management > Local User.

   The Local Users page 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.

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 Settings > User Management > Local User.

   The Local Users page 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

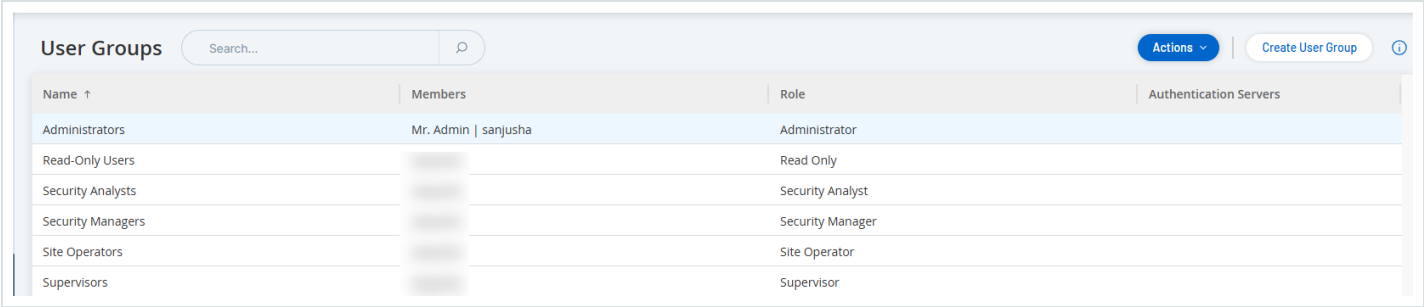
> Required OT Security User Role: Administrator

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 and Site Operators User Group > Site Operator role. 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.



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.

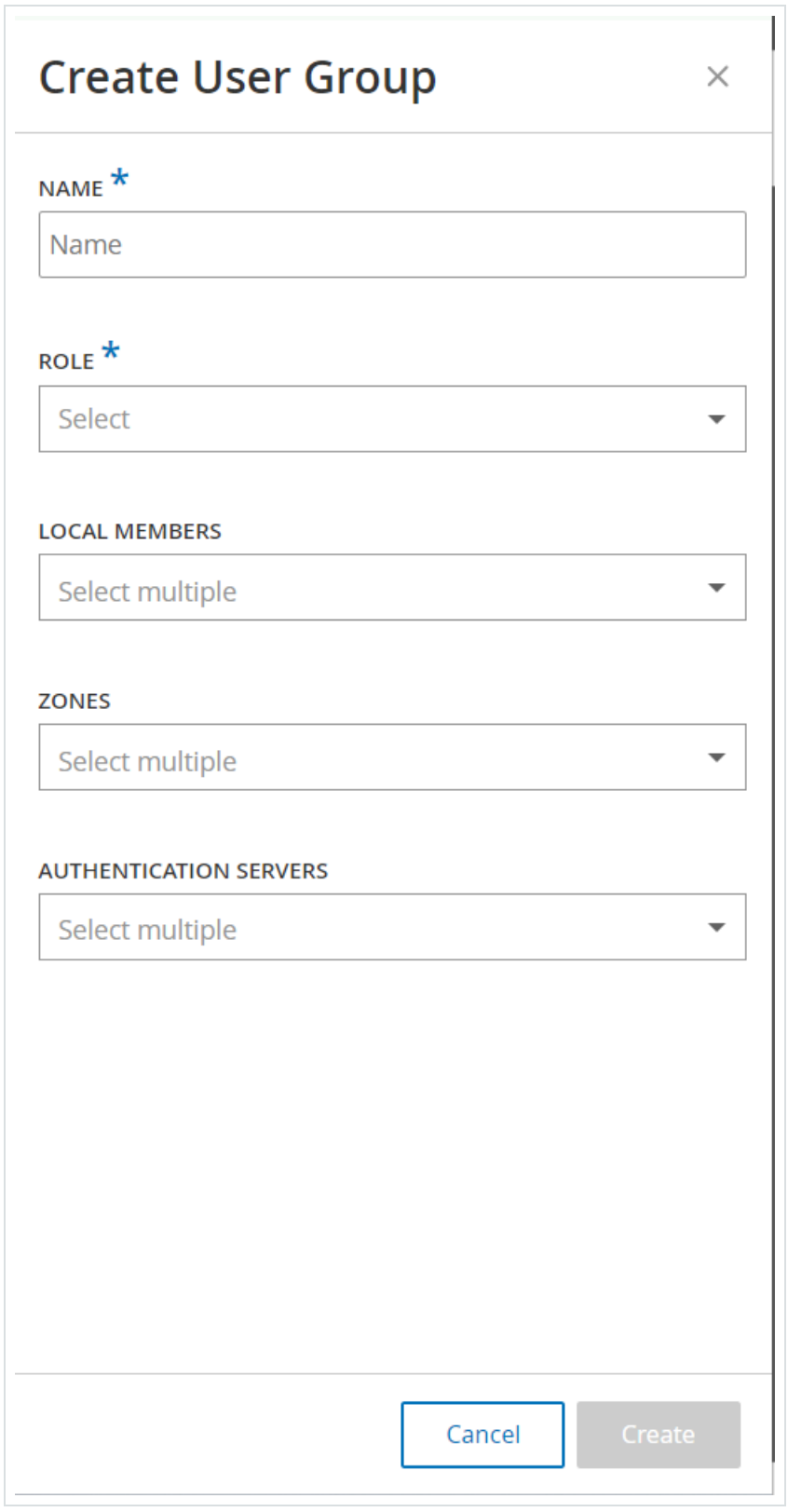
To create a user group:

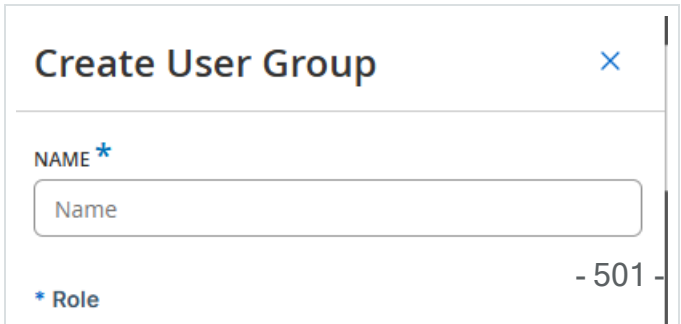
1. Go to Settings >User Management > User Groups.

   The User Groups screen appears.

2. Click Create User Group.

   The Create User Group pane appears.


Create User Group
NAME *
Name
ROLE *
Select
LOCAL MEMBERS
Select multiple
ZONES
Select multiple
AUTHENTICATION SERVERS
Select multiple
Cancel
Create


Create User Group
NAME *
Name
* Role

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 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.

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 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)	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	✓	✓	✓	✓	✓	✓	✓

Permission	Admin (Local)	Admin (External/ AD)	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
Enable/Disable	✓	✓	✓	✓	✗	✗	✗
View action	✓	✓	✓	✓	✓	✓	✓
Edit	✓	✓	✓	✓	✗	✗	✗
Duplicate	✓	✓	✓	✓	✗	✗	✗
Delete	✓	✓	✓	✓	✗	✗	✗
Create policy	✓	✓	✓	✓	✗	✗	✗
Export	✓	✓	✓	✓	✓	✓	✓
Assets							
View assets	✓	✓	✓	✓	✓	✓	✓
View action	✓	✓	✓	✓	✓	✓	✓
Edit	✓	✓	✓	✗	✗	✓	✗
Delete	✓	✓	✓	✗	✗	✓	✗
Import (upload new	✓	✓	✓	✗	✗	✓	✗

Permission	Admin (Local)	Admin (External/ AD)	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
assets by csv)							
Hide	✓	✓	✓	✗	✗	✓	✗
Export	✓	✓	✓	✓	✓	✓	✓
Resync	✓	✓	✓	✓	✓	✓	✗
Nessus scan	✓	✓	✓	✓	✓	✓	✗
Take snapshot (single asset)	✓	✓	✓	✓	✓	✓	✗
Update open ports (single asset)	✓	✓	✓	✓	✓	✗	✗
Update port state (single asset)	✓	✓	✓	✓	✓	✗	✗
View in	✓	✓	✓	✓	✓	✓	✓

Permission	Admin (Local)	Admin (External/ AD)	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
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	✓	✓	✓	✓	✗	✗	✗

Permission	Admin (Local)	Admin (External/ AD)	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
Export	✓	✓	✓	✓	✓	✓	✓
Network							
Turn on packet capture	✓	✓	✓	✗	✗	✗	✗
Close ongoing captures	✓	✓	✓	✓	✓	✓	✗
Download PCAP file	✓	✓	✓	✓	✓	✓	✓
Export conversations table	✓	✓	✓	✓	✓	✓	✓
Set as baseline	✓	✓	✓	✓	✗	✗	✗
Generate map	✓	✓	✓	✓	✓	✓	✓
Refresh map	✓	✓	✓	✓	✓	✓	✓

Permission	Admin (Local)	Admin (External/ AD)	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
Groups							
View groups	✓	✓	✓	✓	✓	✓	✓
View action	✓	✓	✓	✓	✓	✓	✓
Edit	✓	✓	✓	✓	✗	✗	✗
Duplicate	✓	✓	✓	✓	✗	✗	✗
Delete	✓	✓	✓	✓	✗	✗	✗
Create group	✓	✓	✓	✓	✗	✗	✗
Export	✓	✓	✓	✓	✓	✓	✓
Report							
View reports	✓	✓	✓	✓	✓	✓	✓
Generate	✓	✓	✓	✓	✓	✓	✓
Download	✓	✓	✓	✓	✓	✓	✓
Export	✓	✓	✓	✓	✓	✓	✓

Permission	Admin (Local)	Admin (External/ AD)	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
Network Segments							
View Network Segments	✓	✓	✓	✓	✓	✓	✓
Edit	✓	✓	✓	✓	✗	✗	✗
Delete	✓	✓	✓	✓	✗	✗	✗
Create	✓	✓	✓	✓	✗	✗	✗
Export	✓	✓	✓	✓	✓	✓	✓
Learn More	✓	✓	✓	✓	✓	✓	✓
Local Settings							
Queries	✓	✓	✓	✗	✗	✗	✗
System Configuration - Device Details	✓	✓	✓	✗	✗	✗	✗
System Configurati	✓	✓	✓	✓ (No Actions)	✓ (No	✓ (No Action	✓ (No

Permission	Admin (Local)	Admin (External/ AD)	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
on - Sensors					Actions)	s)	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	✓	✓	✗	✗	✗	✗	✗

Permission	Admin (Local)	Admin (External/ AD)	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
Configuration - License							
Environment Configuration - Asset Settings	✓	✓	✓	✗	✗	✗	✗
Environment Configuration - Hidden Assets	✓	✓	✓	✓ - no restore	✓ - no restore	✓	✓ - no restore
Environment Configuration - Custom Fields	✓	✓	✓	✗	✗	✗	✗
Environment Configuration -Event Clusters	✓	✓	✓	✗	✗	✗	✗

Permission	Admin (Local)	Admin (External/ AD)	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
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	✓	✓ (No	✓

Permission	Admin (Local)	Admin (External/AD)	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
				Actions)	(No Actions)	Actions)	(No Actions)
System Actions	✓	✓ without factory reset	✓ only backup and diagnostics	✓ only diagnostics	✗	✗	✗
System log	✓	✓	✓	✓	✓	✓	✓ no syslog
Enable (on setup and after disable)	✓	✓	✗	✗	✗	✗	✗
Delete Assets	✓	✓	✓	✗	✗	✗	✗

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

> Required OT Security User Role: Administrator

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 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 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 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 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 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

> Required OT Security User Role: Administrator

The Authentication Servers page shows your existing integrations with authentication servers. You can add a server by clicking the Add server button.

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, such as Administrators User Group > Administrator role and Site Operators User Group > Site Operator role. 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 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.
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.

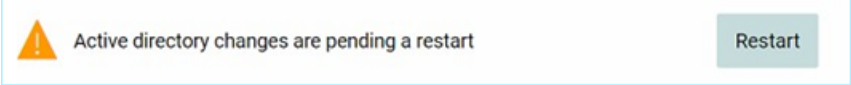
   > Note: If you are not aware of the DN of the group that you would like to assign OT Security privileges, you can view a list of all groups configured in your Active Directory which contain users by entering the command `dsquery group -name Users*` in the Windows CMD or Command Line. Type the name of 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.



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 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

Required OT Security User Role: Administrator

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 Azure

To configure SAML:

1. Go to Settings >Users Management > SAML.
2. Click Configure.

   The Configure SAML panel appears.
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.

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

Required OT Security User Role: Administrator, Supervisor, Security Manager, Security Analyst, Site Operator, Read Only

To view groups:

1. Go to Settings > Groups.

   The Groups section expands to display the group types.

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 & Tags – Assets are hardware entities in the network. Asset Groups are used as a Policy condition for a wide range of Policy types.
- 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.
- Controller 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.

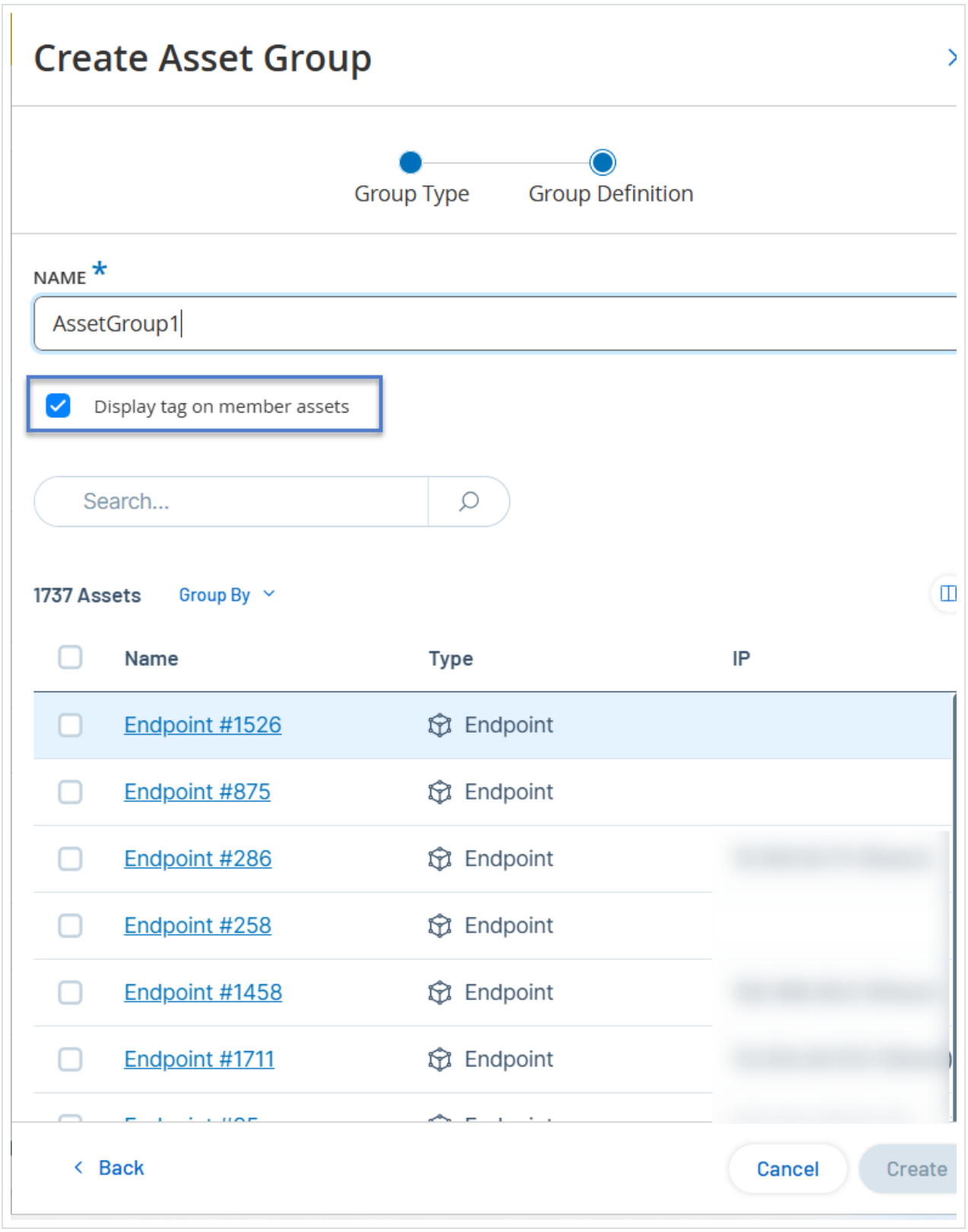
Asset Groups and Tags

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.

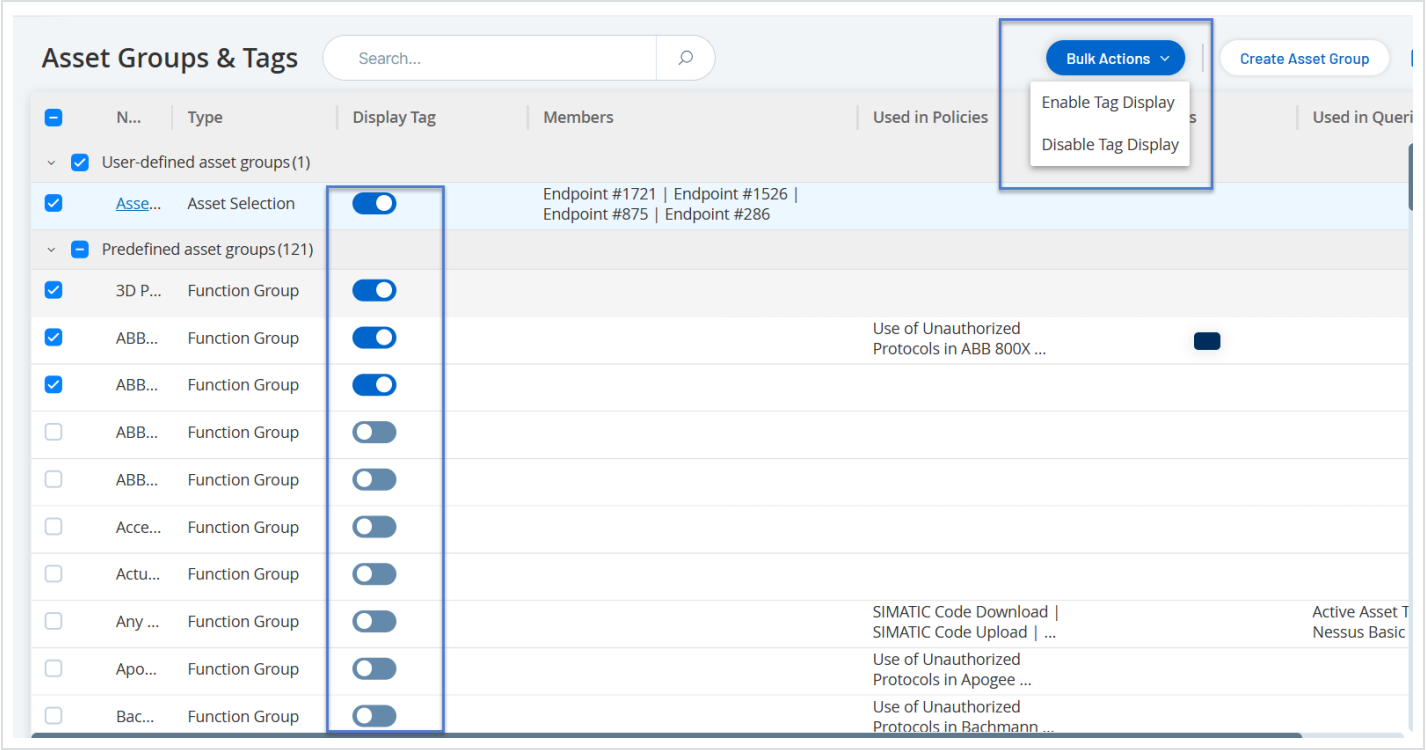
Tags

Tags help group assets based on a specific criteria allowing you to streamline and prioritize various workflows. When you create groups, OT Security converts these as tags on your assets.

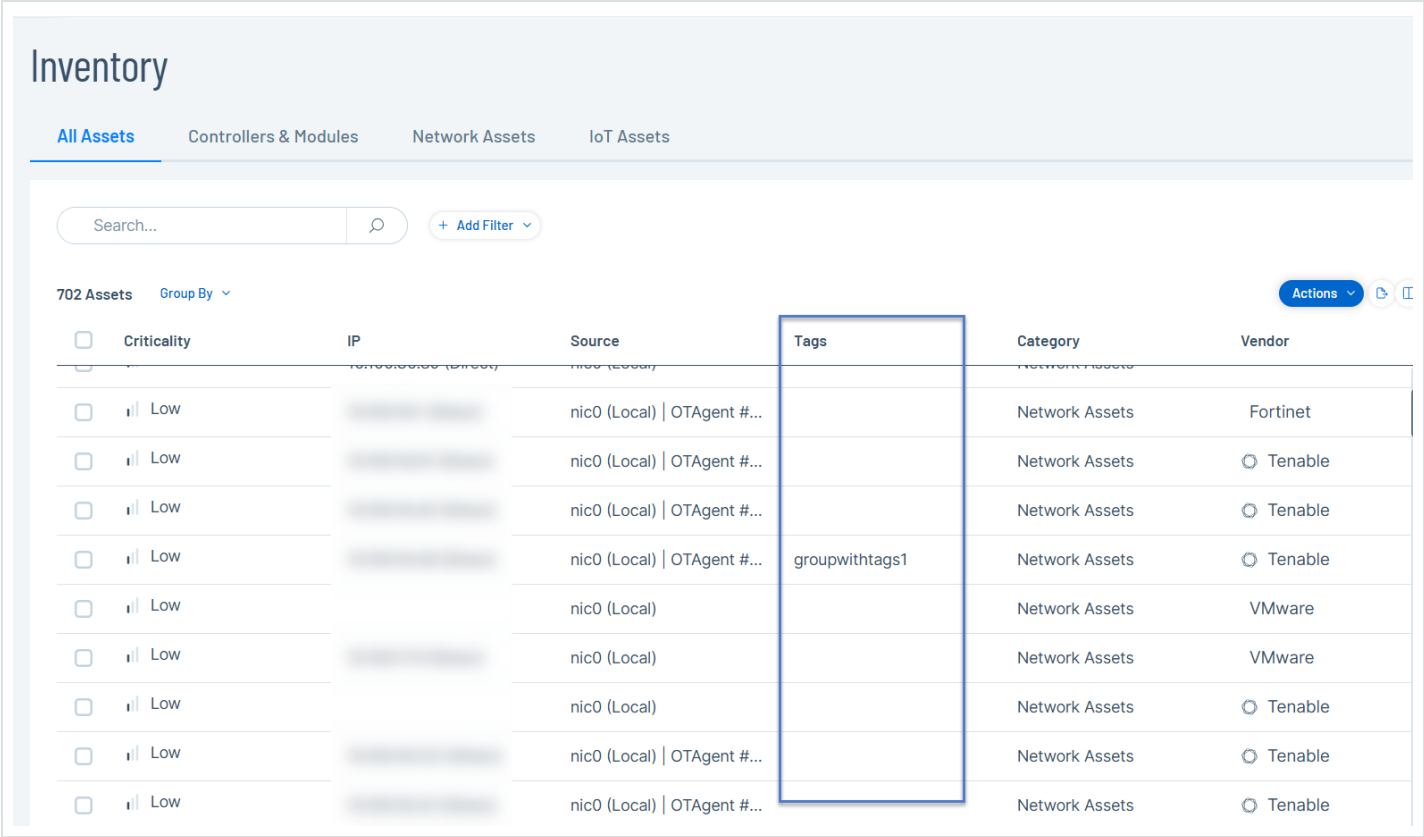
To display the tags on assets, select the Display tag on member assets checkbox when you create asset groups.


Create Asset Group
Group Type
Group Definition
NAME *
AssetGroup1
Display tag on member assets
Search...
1737 Assets
Group By
Name
Type
IP
Endpoint #1526
Endpoint
Endpoint #875
Endpoint
Endpoint #286
Endpoint
Endpoint #258
Endpoint
Endpoint #1458
Endpoint
Endpoint #1711
Endpoint
Back
Cancel
Create

To enable or disable display tags for multiple assets, select multiple assets and from the Bulk Actions menu, choose Enable Tag Display or Disable Tag Display as needed. You can also enable or disable the toggle in the Display Tag column for each asset.



These asset groups appear in the Tags column on the Inventory > All Assets page.



View Asset Groups and Tags

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.
ID	The ID assigned to the asset group.

Name	The name of the Policy.
Display Tag	The toggle to enable the display of tags on the Inventory > All Assets page.
Severity	The severity of the event. Possible values are: None, Low, Medium, or High. See section Severity Levels for more information.
Origin	The origin of the asset group: User Defined or System Defined.
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: • 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.
Type	The group type. Options are Static or Dynamic.
Members	Shows the list of assets included in this Group. No value is shown for Function Groups.

	Note: If there is no room to display all assets in this row then click Table Actions > View > Members tab.
Used in Policies	Shows the name of each policy that uses this Asset Group in its configuration. Note: To view more details about the policies in which the Group is used, click Table Actions > View > Used in Policies tab.
Used in Queries	Shows the name of the query that uses this asset group.
Used in Zones	Shows the name of the zone that uses this asset group.

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

Required OT Security User Role: Administrator, Supervisor, Security Manager

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 Selection – 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.

Note: For duplicated networks, use the Asset Selection option for creating asset group.

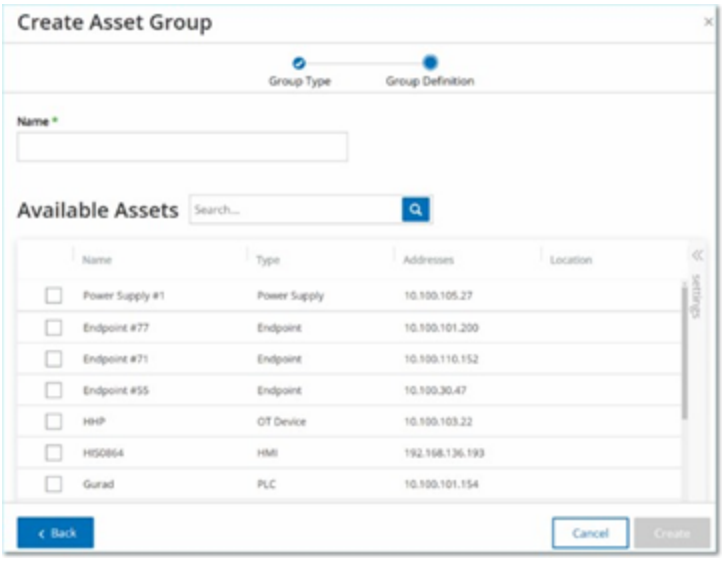
There are different procedures for creating each type of Asset Group.

To create an asset selection type asset group:

1. Go to Settings > 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. To display the tags on the assets, select the Display tag on member assets checkbox.

   Note: If this option is selected, OT Security displays the tags in the Tags column in the Inventory > All Assets page.
6. 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.
7. Select the checkbox next to each asset you want to include in the group.

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.

To create an IP range type asset group:

1. Go to Settings > 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.
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 Settings > Groups > Asset Groups.
2. Click Create Asset Group.

The Create Asset Group panel appears.

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.

Create Asset Groups and Tags

You can create custom asset groups to use when configuring policies. Grouping similar assets enables you to create policies that apply to all assets in the group. You can create groups either by selecting the required assets or by setting a filter rule to group assets in a specific category. Grouping assets dynamically based on selected criteria helps you streamline and scale processes, such as prioritization and reporting.

To create asset group:

1. Go to Groups > Asset Groups & Tags.

   The Asset Groups & Tags page appears.

2. To create an asset group, click Create Asset Group.

   The Create Asset Group window appears.

3. In the Group Type section, select one of the following:

   - Static (Manual Selection) – Static asset groups are defined by manually picking assets and adding them to the group. Once you set the group, its members do not change unless you edit them.
   - Dynamic (Rule Based) – Dynamic asset groups use rules to filter your asset inventory. As ongoing asset discovery and enrichment continues, the members are automatically added to or removed from the group, which keeps the group up to date.

4. Click Next.

   The Group Definition panel appears.

5. In the Name box, provide a name for the asset group. Choose a name that describes a common element that categorizes the assets included in the group.

6. If you selected Static, do the following:

   a. Select the checkboxes next to the assets you want to add to the group.

7. If you selected Dynamic, click Add Filter to enable a rule for group creation. See Filter Assets.

   > Note: You must add at least one filter to enable group creation.

8. To display the tags for each asset, select the Display tag on member assets checkbox. This option is selected by default.

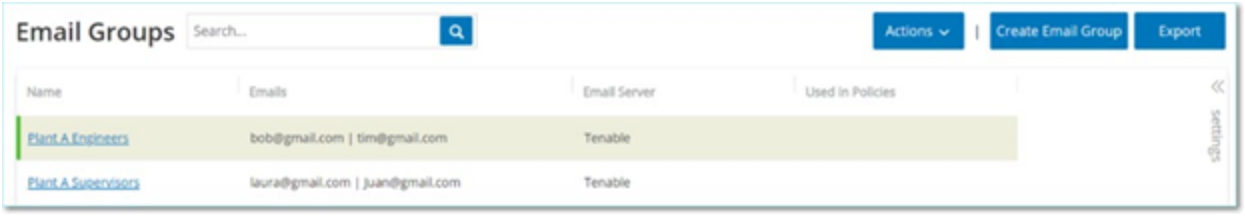
9. Click Create.

   OT Security creates the asset group and displays it on the Asset Groups & Tags page. You can now use this group when configuring policies.

Email Groups

Email 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 and department enables you to send the notifications for specific Policy Events to the relevant parties.

View Email Groups



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

Required OT Security User Role: Administrator, Supervisor, Security Manager

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 Settings > Groups > Email Groups.
2. Click Create Email Group.

   The Create Email Group panel appears.
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 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

Required OT Security User Role: Administrator, Supervisor, Security Manager

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 Settings > Groups > Port Groups.
2. Click Create Port Group.

   The Create Port Group panel appears.
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, for instance Modbus, PROFINET, and CIP. You can also create your own user-defined Protocol Groups.

View Protocol Groups

The Protocol Groups screen shows all Protocol Groups that are currently configured in the system. The Predefined tab shows Groups that are built into the system. 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

Required OT Security User Role: Administrator, Supervisor, Security Manager

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 Settings > Groups > Protocol Groups.
2. Click Create Protocol Group.

   The Create Protocol Group appears.
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

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: • 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

Required OT Security User Role: Administrator, Supervisor, Security Manager

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 Settings > 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 Settings > 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.

Controller Tag Groups

Tags are parameters in controllers that contain specific operational data. Controller 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 Controller Tag Groups

The Controller Tag Groups page shows all tag groups currently configured in the system.

The Controller 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 Controller Tag Groups

Required OT Security User Role: Administrator, Supervisor, Security Manager

You can create custom Controller 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 Controller Tag Groups.

To create a new tag group:

1. Go to Settings > Groups > Controller Tag Groups.
2. Click Create Controller Tag Group.

   The Create Controller 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 Controller 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 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. Note: To view additional details about the Policies in which this Group is used, click Actions > View > Used in Policies tab.

Create Rule Groups

Required OT Security User Role: Administrator, Supervisor, Security Manager

To create a new Rule Group:

1. Go to Settings > 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

Required OT Security User Role: Administrator, Supervisor, Security Manager

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 group type.

   The page for the selected group type appears

2. Select the group you want to view.

   OT Security enables the Actions button.

3. Do one of the following:

   - Click Actions and select View.
   - Right-click the required group and select View.

4. Select View.

   The Group details page appears.

Edit a Group

You can edit the details of an existing Group.

To edit details of a group:

1. In Groups, select the required group type.

   The page for the selected group type appears

2. In the Groups page, select the group you want to edit.

   OT Security enables the Actions button.

3. Do one of the following:

   - Click Actions and select Edit.
   - Right-click the required group and select Edit.

4. Select Edit.
5. The Edit Group window appears, showing the relevant parameters for the specified Group type.
6. Modify as needed.
7. 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. In Groups, select the required group type.

   The page for the selected group type appears.

2. Select the group you want to duplicate.

   OT Security enables the Actions button.

3. Do one of the following:

   - Click Actions and select Duplicate.
   - Right-click the required group and select Duplicate.

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. In Groups, select the required group type.

   The page for the selected group type appears

2. Select the group you want to delete.

   OT Security enables the Actions button.

3. Do one of the following:

   - Click Actions and select Delete.
   - Right-click the required group and select Delete.

4. Select Delete.

   A confirmation window appears.

5. Click Delete.

   OT Security permanently deletes the group from the system.

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

> Required OT Security User Role: Administrator

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. In the Tenable OT Security interface, navigate to 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

Required OT Security User Role: Administrator

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. In the Tenable OT Security interface, navigate to 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

> Required OT Security User Role: Administrator

To integrate with Tenable One, follow the steps in Integrate with Tenable One.

Palo Alto Networks – Next Generation Firewall

> Required OT Security User Role: Administrator

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. In the Tenable OT Security interface, navigate to 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

Required OT Security User Role: Administrator

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

To integrate OT Security with your Aruba ClearPass account:

1. In the Tenable OT Security interface, navigate to 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 and view assets and risk scores data on Tenable Exposure 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.

After the integration, OT Security sends the following data to Tenable One:

- OT Security synchronizes all assets and asset attributes with the Exposure Management > Inventory page. These attributes include the vendor, make, model, state, firmware, and serial number. The synchronization includes the following fields:
    - OT_BACKPLANE_ID
    - OT_BACKPLANE_NAME
    - OT_CATEGORY
    - OT_CRITICALITY
    - OT_DESCRIPTION
    - OT_FAMILY
    - OT_FIRMWARE
    - OT_ID
    - OT_LOCATION

- OT_MODEL
- OT_SERIAL_NUMBER
- OT_SLOT
- OT_STATE
- OT_VENDOR
- OT_SENSOR_NAME
- OT_DIRECT_IP_ADDRESSES
- OT_RISK

- All vulnerability findings associated with assets, including the plugin IDs, plugin names, and plugin output. Tenable One uses this data to track whether the vulnerability status is Active or Fixed for each asset.
- (Version 4.4 and later) All policy violation findings associated with each asset. This data includes the policy event type, detailed plugin output describing the event, and the involved assets. It also includes the relevant MITRE ATT&CK Tactics, Techniques, and Procedures (TTP) for the observed activity.
- (Version 4.5 and later) All dynamic tags associated with assets. These appear in Tenable One as External Tags.

> Note: OT Security findings do not appear in Tenable Vulnerability Management, unless you integrate Tenable Vulnerability Management with OT Security or use the OT Discovery engine in your scans.

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. In the Tenable OT Security interface, navigate to 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.

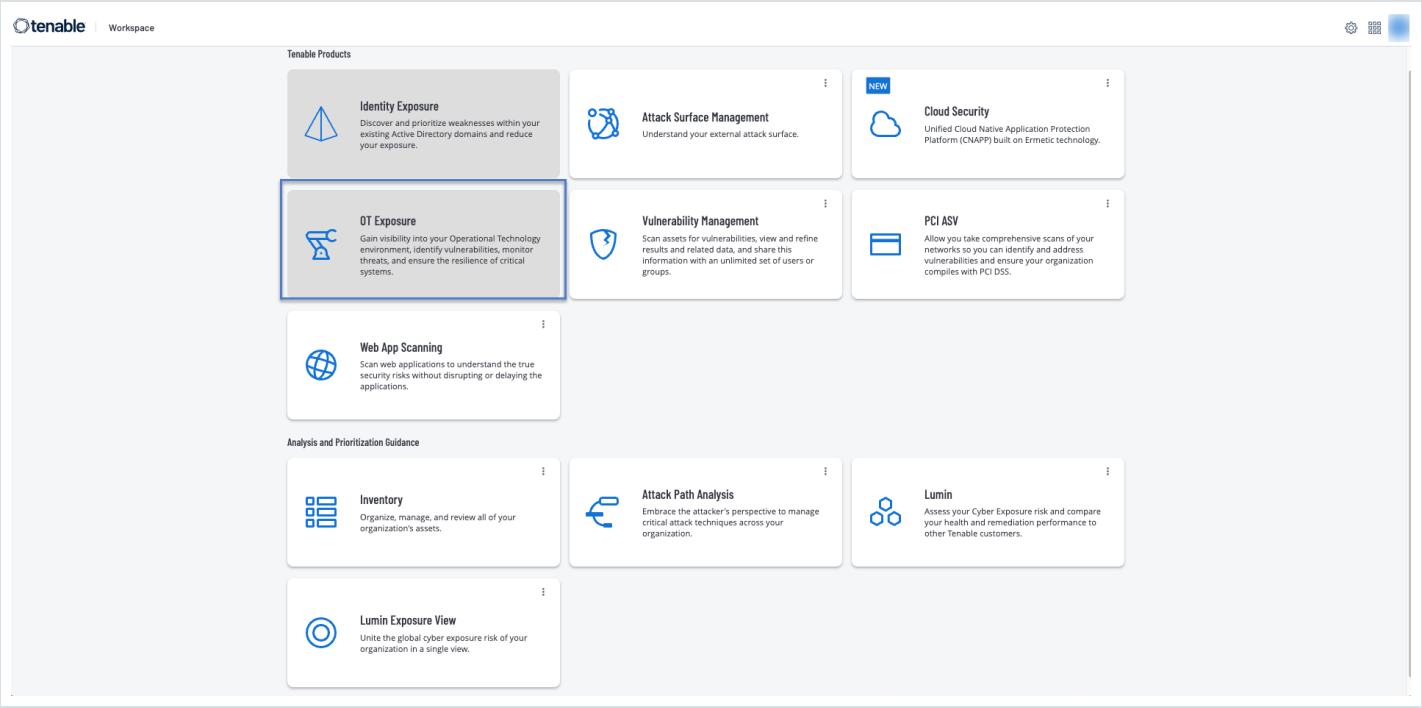
> Note: If you change the name of your site in OT Security after it is already paired, you can manually modify the sensor name within Tenable Vulnerability Management to match the new site name. Alternatively, you can delete the integration on both OT Security and Tenable Vulnerability Management, and 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.

Configure SAML Integration for Tenable One

Configure SAML on your Tenable One instance to access OT Security using SSO.

The OT Exposure tile on the Tenable One Workspace page is disabled by default. To enable the OT Exposure tile, you must first configure SAML for Tenable One.



Before you Begin

- Make sure you have a valid Tenable One and OT Security license.

To configure SAML for Tenable OT Security:

1. Retrieve SAML Identity Provider (IDP) details and group object IDs from Tenable One:

   a. In a supported browser, log into https://cloud.tenable.com to access the Workspace page.

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

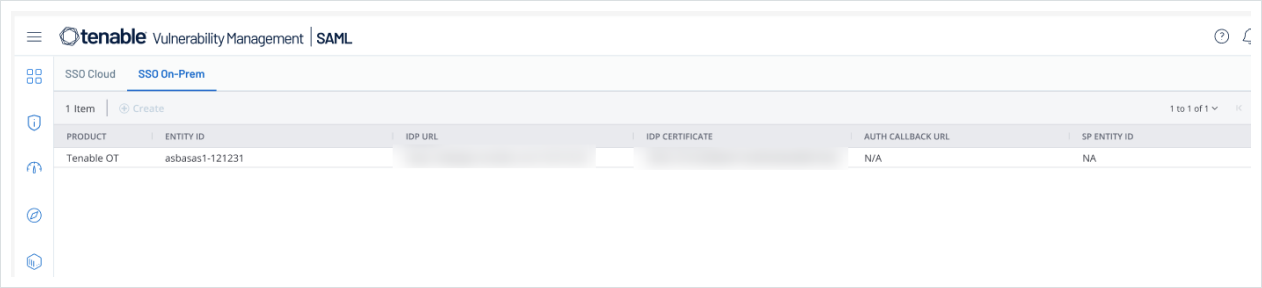
      The Settings page appears.

   c. Click the SAML tile.

      The SAML page appears.

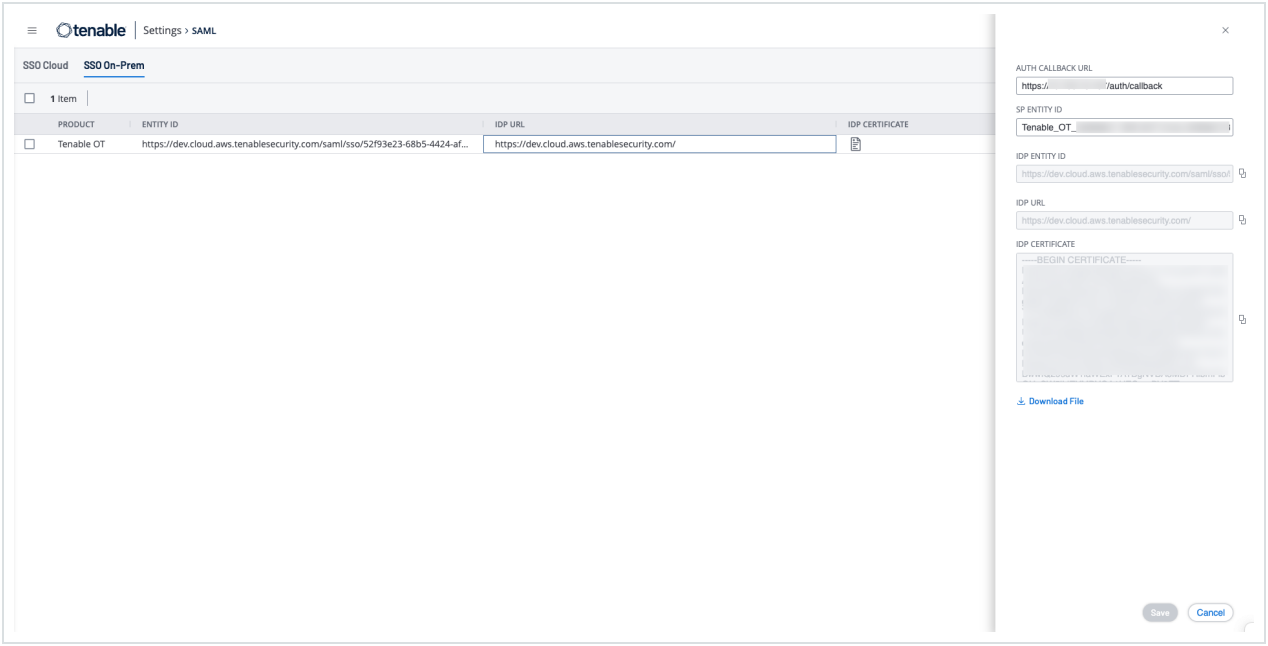
   d. Click the SSO On-Prem tab.

      The SSO On-Prem page appears with the SSO configuration for Tenable OT Security.



   e. Hover over and click the Tenable OT Security row.

      The IDP details panel appears on the right.



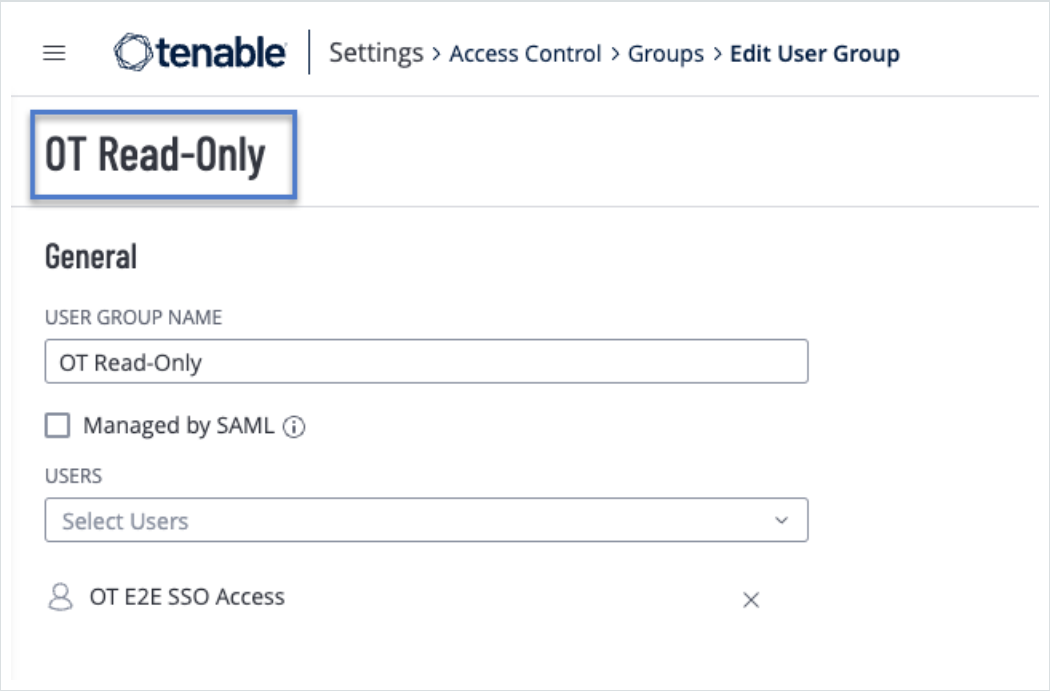
f. Use the button to copy these details.

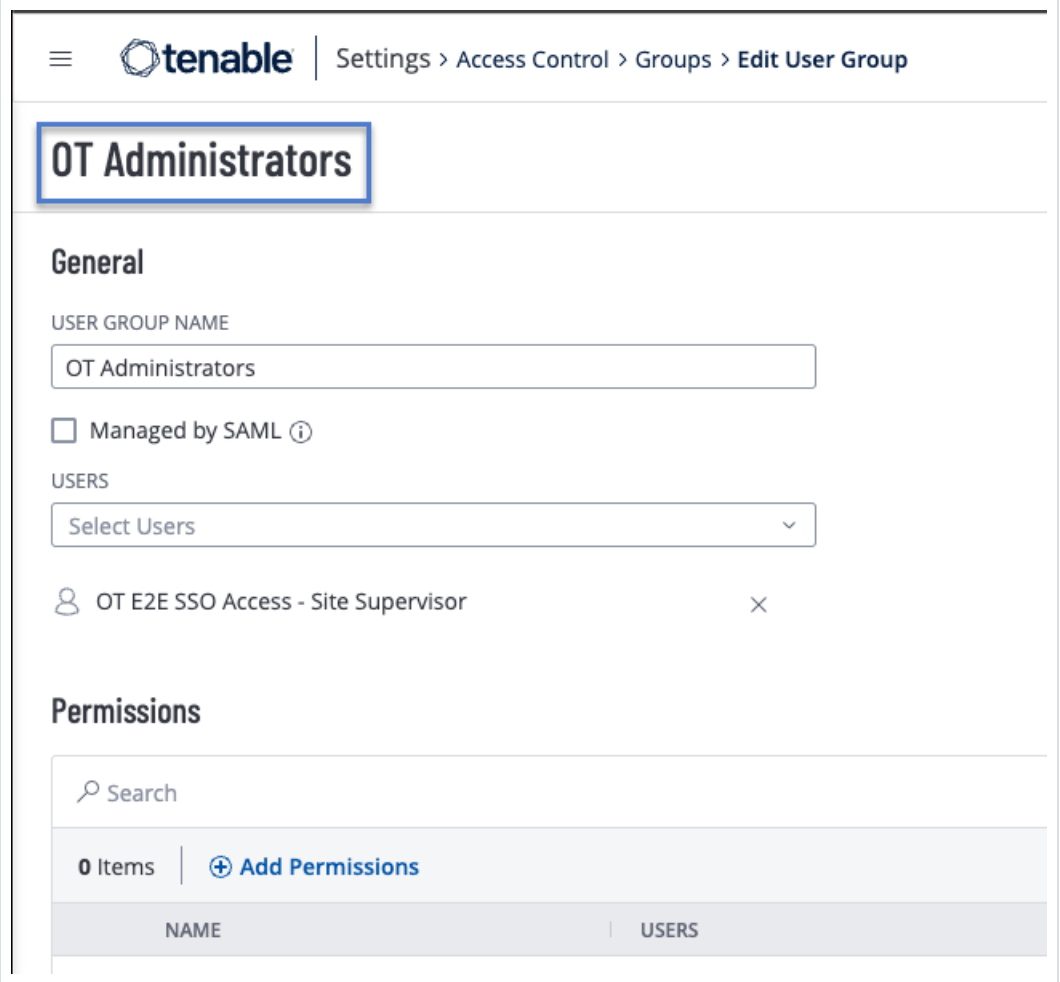
- IDP Entity ID
- IDP URL
- IDP Certificate

g. Click Download File to download the certificate to your local system.

h. Retrieve the mapping data for groups. To find the group object ID information, go to Settings > Access Control > Groups and find or add the relevant groups.

For example: In Tenable One, create two groups: OT Administrators and OT Read-Only. To map them to the user roles in OT Security, add the group names to the respective Administrators Group Object ID and Read-Only Users Group Object ID fields in the OT Security SAML page.


Settings > Access Control > Groups > Edit User Group
OT Read-Only
General
USER GROUP NAME
OT Read-Only
Managed by SAML
USERS
Select Users
OT E2E SSO Access


Settings > Access Control > Groups > Edit User Group
OT Administrators
General
USER GROUP NAME
OT Administrators
Managed by SAML
USERS
Select Users
OT E2E SSO Access - Site Supervisor
Permissions
Search
0 Items
Add Permissions
NAME
USERS

2. Configure SAML in OT Security:

    a. Log into OT Security.

    b. Go to Settings > User Management > SAML.

    The SAML page appears.

    c. Click Configure or Edit if you are editing an existing configuration.

    The Configure SAML page appears.

    d. Provide the following details that you copied from Tenable One SAML > SSO On-Prem page:

        a. In the IDP ID box, paste the IDP Entity ID copied from the Tenable One SAML page.

        b. In the IDP URL box, type the IDP URL copied from the Tenable One SAML page.

        c. In the Certificate Data box, browse to the location where you downloaded the certificate file and upload it.

        d. In the Username Attribute box, type:

        ```
        http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddres
        s
        ```

        e. In the Group Attribute box, type **`groups`** (it must be in lower case and not Groups).

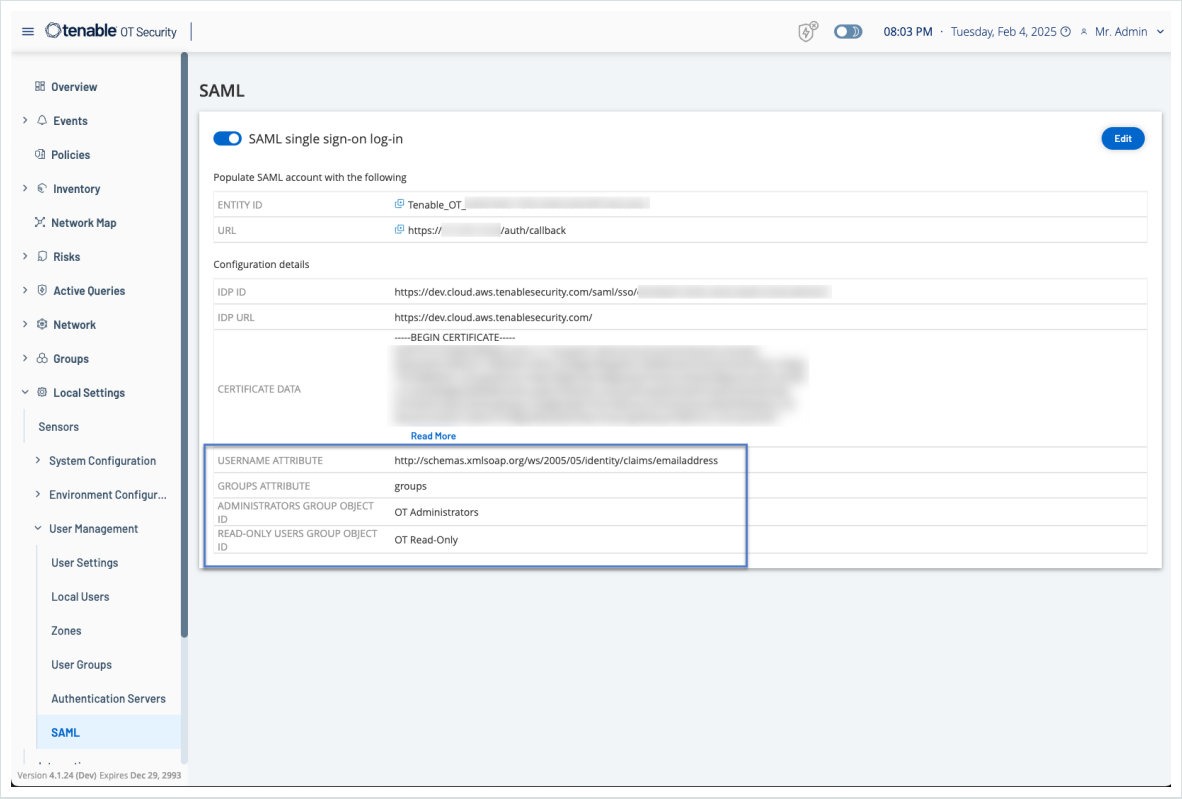
        f. Provide the group object ID information that you retrieved from Tenable One.

        For example: In step h, you created two groups in Tenable One: OT Administrators and OT Read-Only. Add these group names to the corresponding Administrators Group Object ID and Read-Only Users Group Object ID fields in the Configure

SAML page.

g. Click Save.

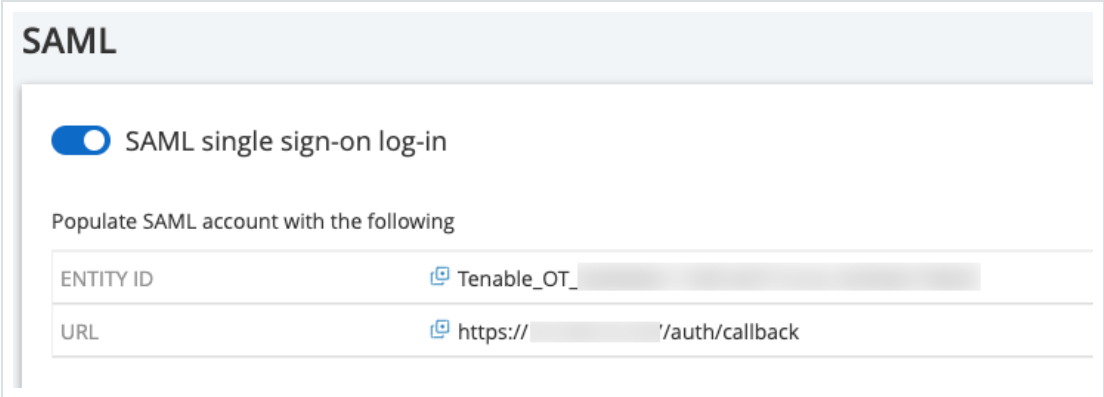
OT Security saves the configuration and displays the following information:



> Important: Do not reboot after saving the configuration. Only reboot after you complete the configuration steps on both OT Security and Tenable One.

h. On the SAML page, copy the following values. You need these values for the final configuration on Tenable One.

- Entity ID
- URL



3. Complete the final configuration on Tenable One:

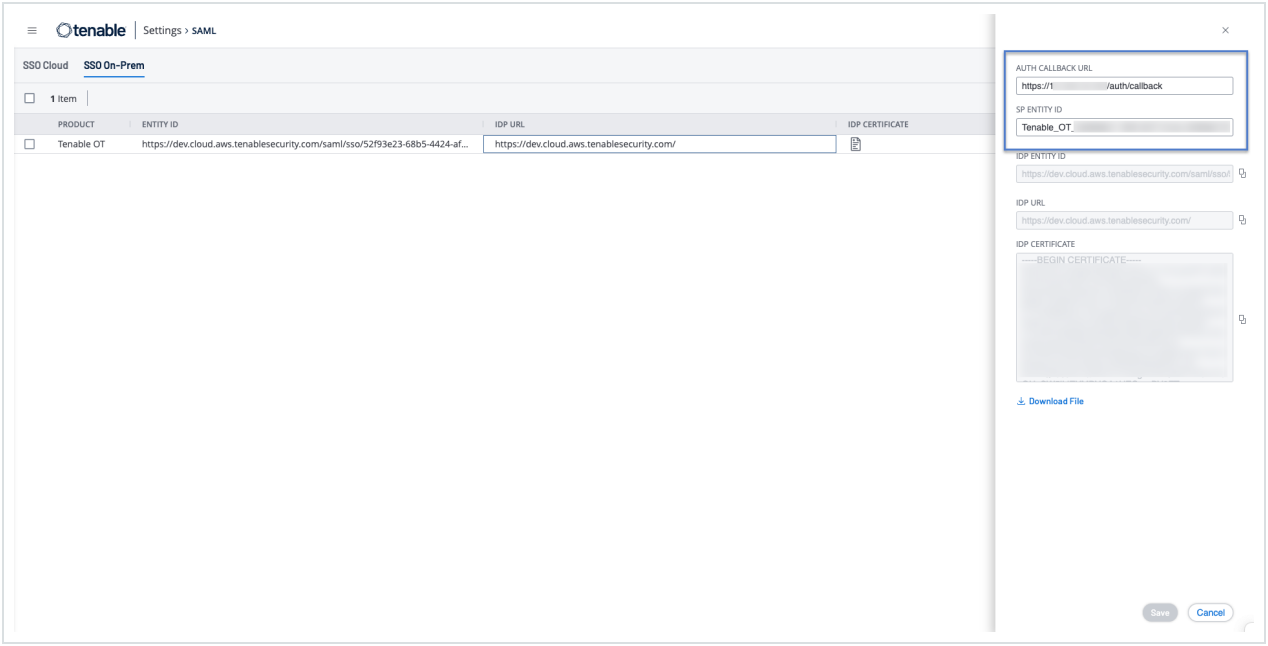
    a. In Tenable One, navigate to the Settings > SAML> SSO On-Prem page.

    The SSO On-Prem page appears with the SSO configuration for Tenable OT Security.

    b. Click the OT Security row.

    The OT Security configuration details panel appears.

    c. Provide the Auth Callback URL and SP Entity ID details copied from the OT Security SAML page.



d. Click Save.

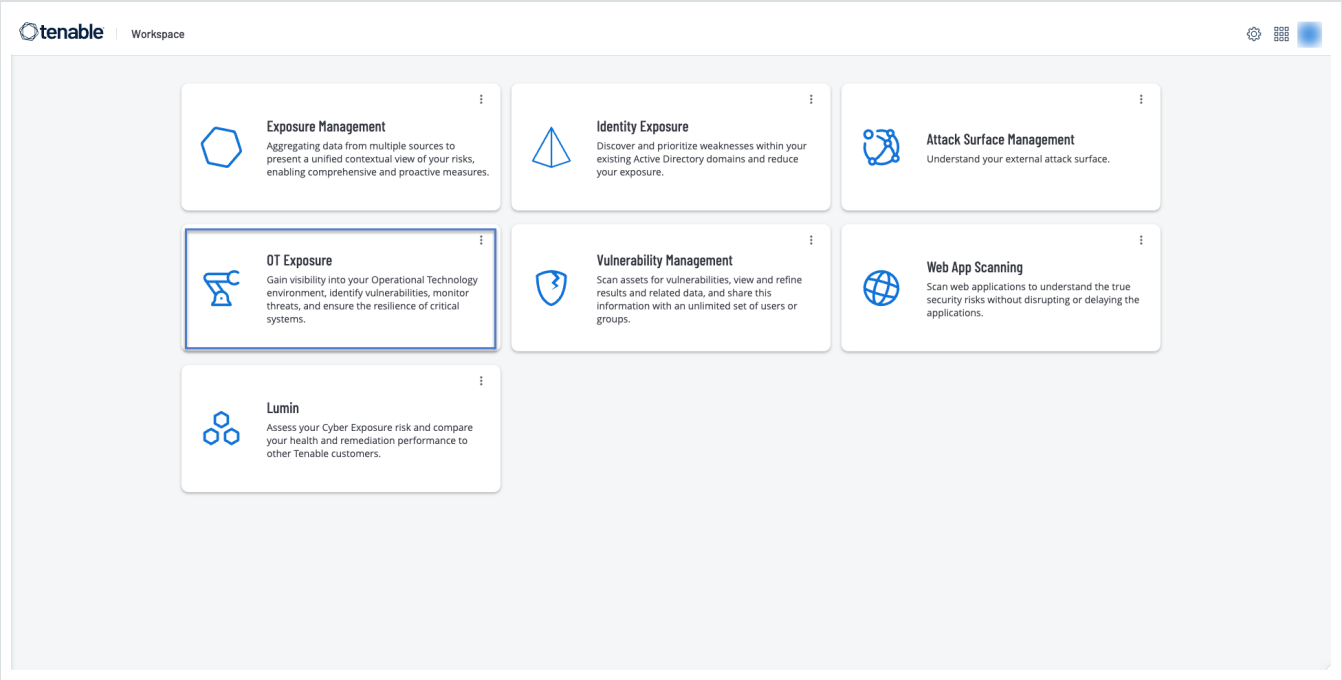
   OT Security saves the SAML configuration.

4. Click the SAML single sign-on log in toggle to enable SAML.

   OT Security prompts you to restart.

5. Restart OT Security.

   Tenable enables the OT Exposure tile on the Workspace page. Click the OT Exposure tile and access OT Security.



Servers

> Required OT Security User Role: Administrator, Supervisor

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 Settings > Servers > SMTP Servers.
2. Click Add SMTP Server.

   The SMTP Servers configuration window appears.
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.

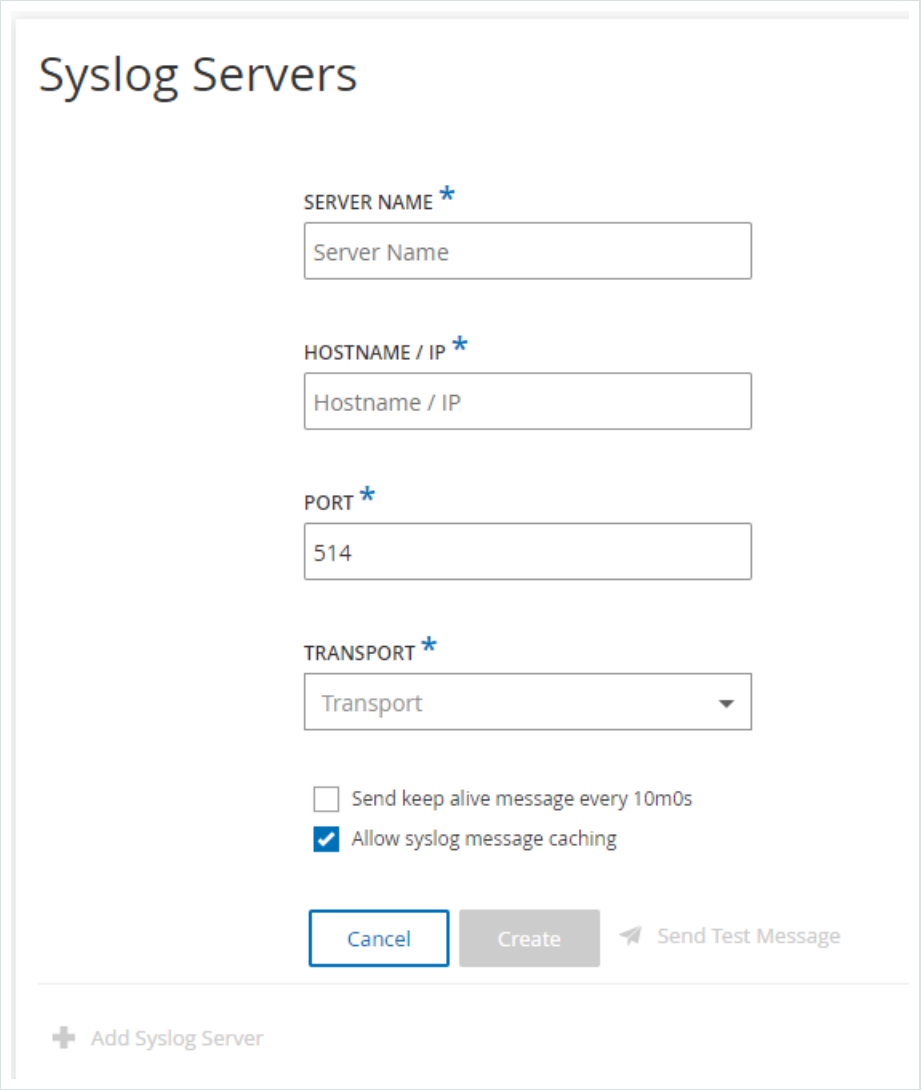
   You can set up additional SMTP Servers by repeating the procedure.

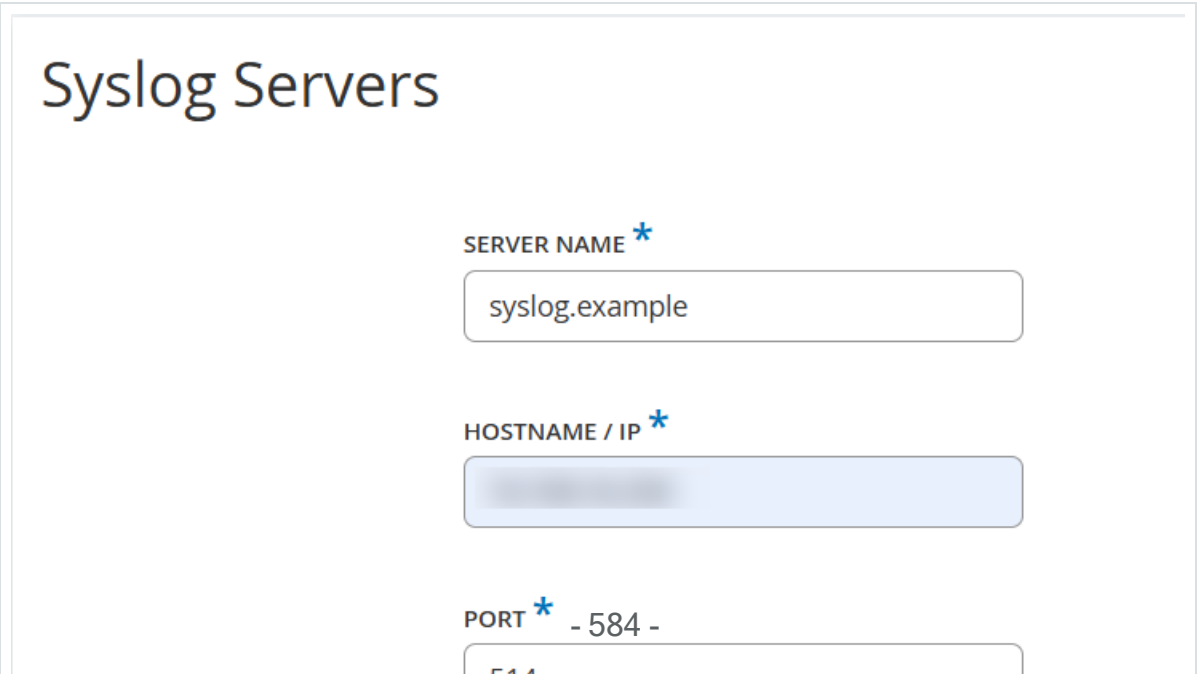
Syslog Servers

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 Settings >Servers > Syslog Servers.
2. Click + Add Syslog Server. The Syslog Servers configuration window appears.





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. To encrypt syslog transmission using TLS encryption, select the TLS checkbox.

    > Note: When TLS is selected, the standard port 6514 (RFC 5425) is automatically suggested.

11. Click Save.

    You can set up additional Syslog Servers by repeating the procedure.

FortiGate Firewalls

To set up a FortiGate server:

1. Go to Settings > Servers > FortiGate Firewalls.
2. Click Add Firewall.

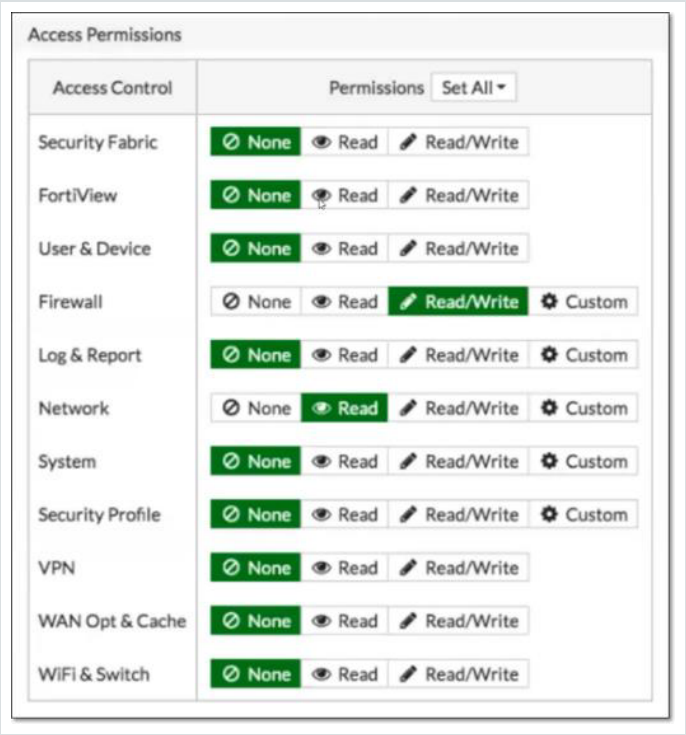
   The Add FortiGate Firewall configuration window appears.
3. In the Server Name box, type the name of a FortiGate Server you want to use.
4. In the Host/IP box, type a hostname or an IP address of the FortiGate server.
5. In the API Key box, type the API token you generated from FortiGate.

   > 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

> Required OT Security User Role: Administrator

The System Log page shows a list of all system events (for example, Policy turned on, Policy edited, and Event Resolved.) 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. For information about how to customize tables, see Management Console User Interface Elements.

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.

Send System Log to a Syslog Server

To configure the system to send system events to a Syslog server:

1. Go to 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 required server.

   OT Security sends the System Log events to the specified Syslog server.

Appendix – SAML Integration for Microsoft Azure

OT Security supports integration with Azure via SAML protocol. This enables Azure users assigned to OT Security to log in to OT Security via Single Sign-on (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 SSO integration for OT Security with Azure. The configuration involves setting up the integration by creating a OT Security application in Azure. You can then provide information about this newly created OT Security application and upload your identity provider's Certificate to the OT Security SAML page. The configuration is complete when you map groups from your identity provider to User Groups in OT Security.

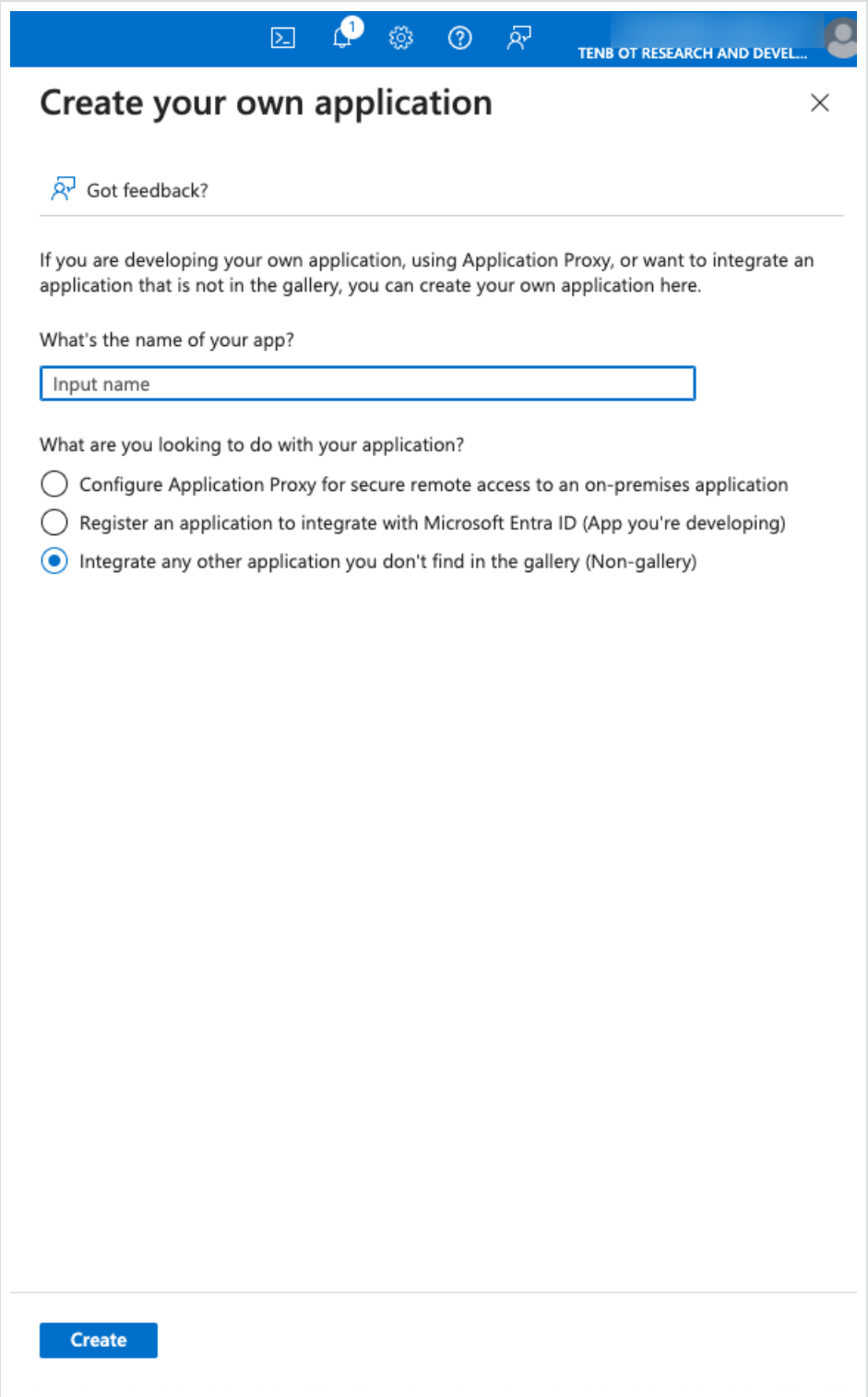
To set up the configuration, you need to be logged in as an administrator user in both Microsoft Azure and OT Security.

Step 1 - Create the Tenable Application in Azure

To create the Tenable application in Azure:

1. In Azure, go to Microsoft Entra ID > Enterprise Applications and click + New application.

   The Browse Microsoft Entra ID Gallery page appears.



2. Click + Create your own application.

   The Create your own application side panel appears.

3. In the What's the name of your app? box, type 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), then click Create to add the application.

Step 2- Initial Configuration

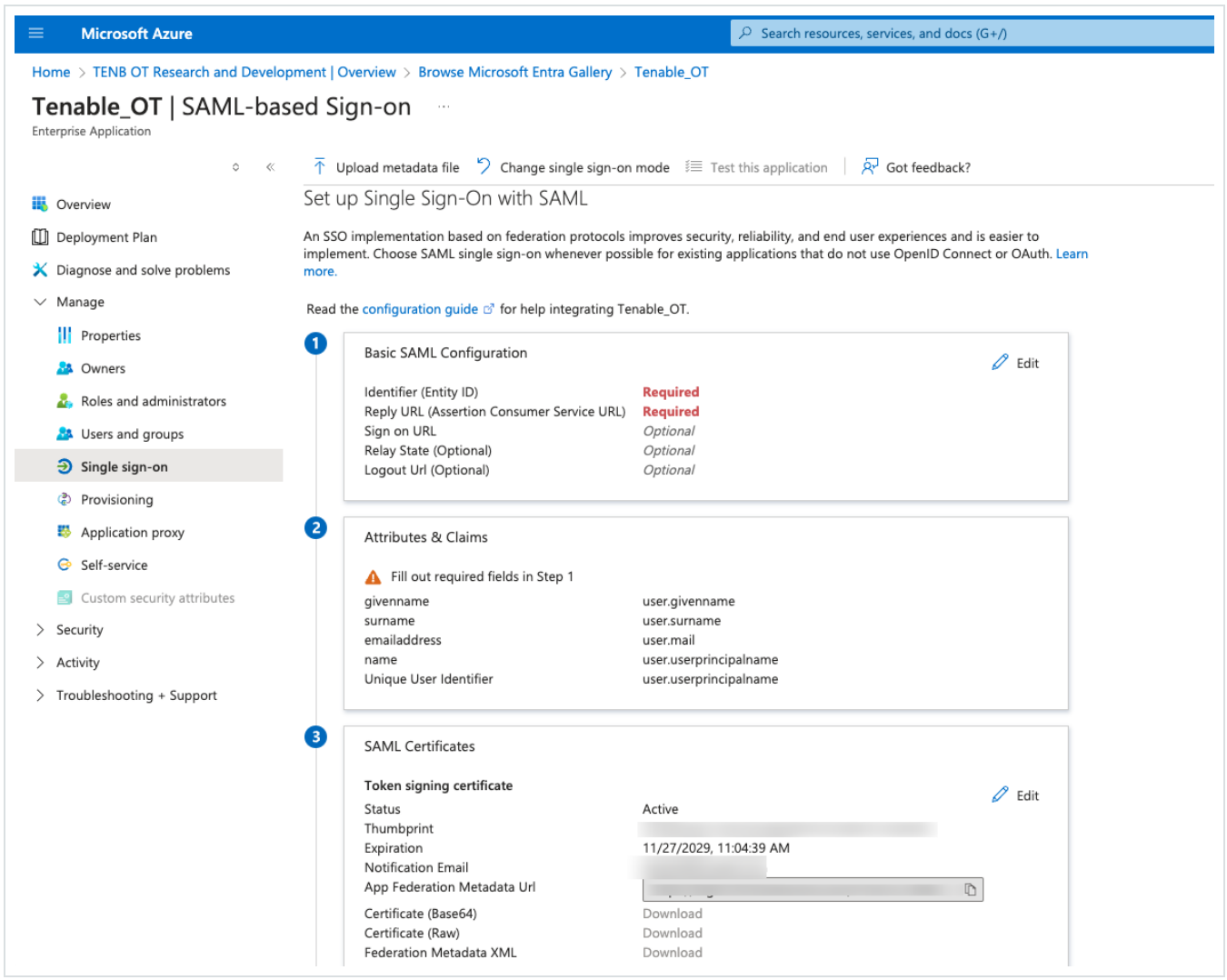
This step is the initial configuration of the OT Security application in Azure, consisting of creating temporary values for basic SAML configuration values – Identifier and Reply URL to download the required certificate.

> Note: Configure only parameters mentioned in this procedure. Retain the default values for the other parameters.

To perform the initial configuration:

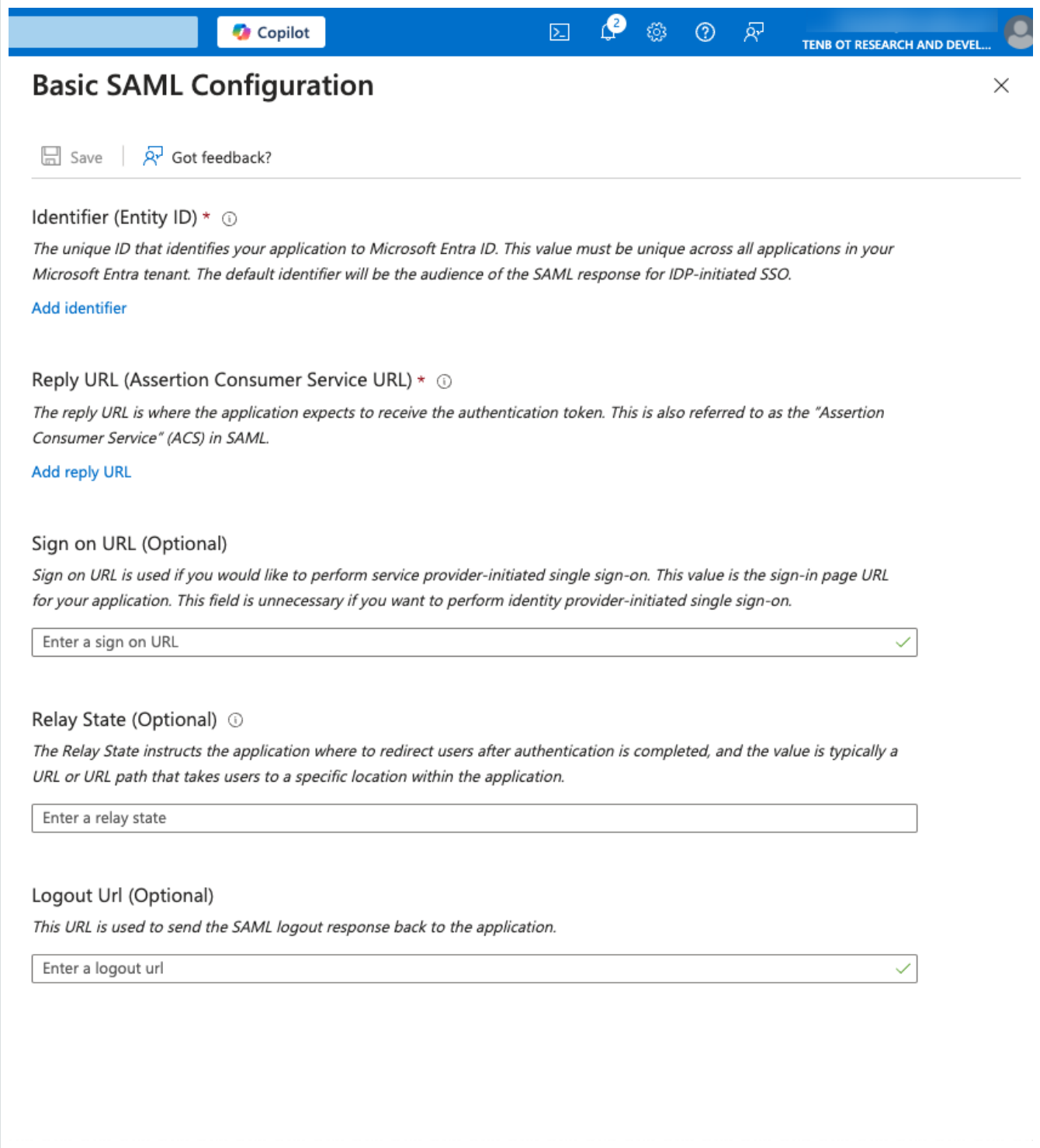
1. In the Azure navigation menu, click Single sign-on, then select SAML as the single sign-on method.

   The SAML-based Sign-on page appears.



2. In section 1 - Basic SAML Configuration, click Edit .

The Basic SAML Configuration side panel appears.



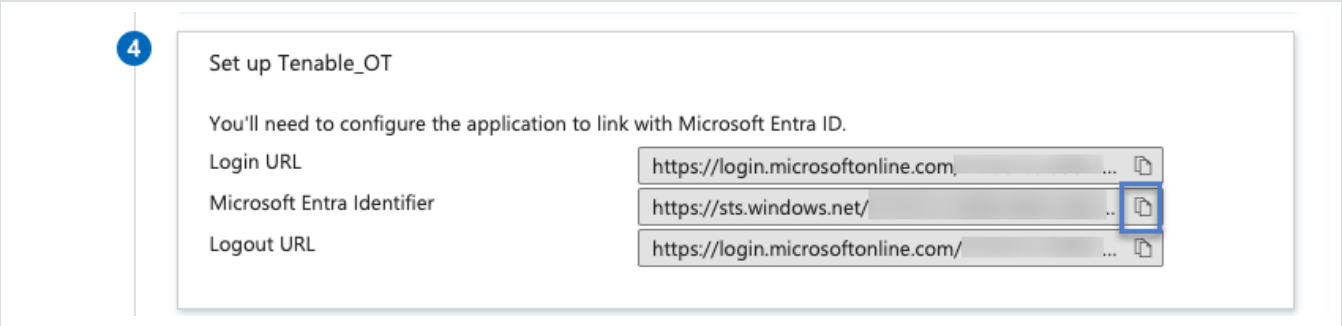
3. In the Identifier (Entity ID) box, type a temporary ID for the Tenable application, for example: `tenable_ot`.

4. In the Reply URL (Assertion Consumer Service URL) box, type a valid URL, for example: `https://OT Security`.

   > Note: The Identifier and Reply URL values are temporary values, which you can change later in the configuration process.

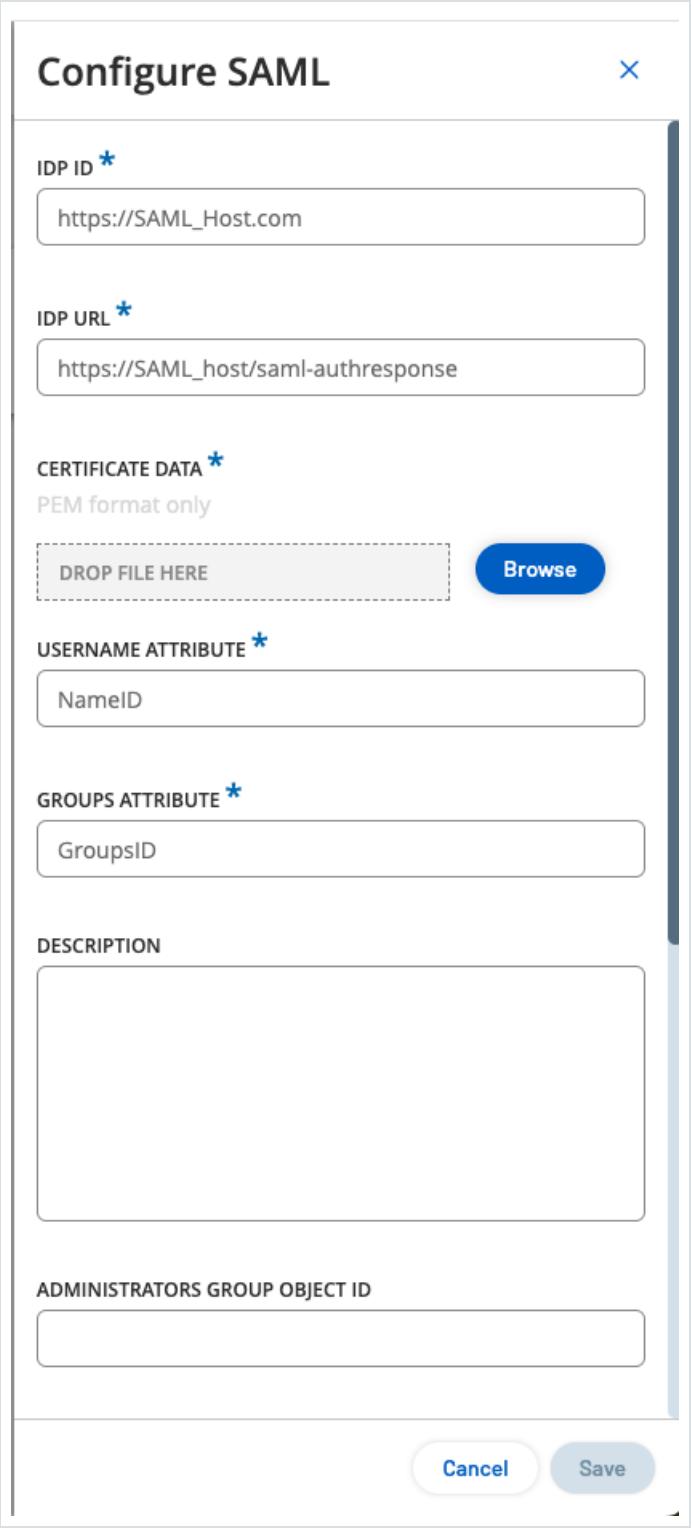
5. Click Save to save the temporary values and close the Basic SAML Configuration side panel.

6. In section 4 - Set up, click the button to copy the Microsoft Entra ID Identifier.



7. Switch to the OT Security console, and go to User Management > SAML.

8. Click Configure to display the Configure SAML side panel, and paste the copied value into the IDP ID box.



9. In the Microsoft Azure console, click the button to copy the Login URL.

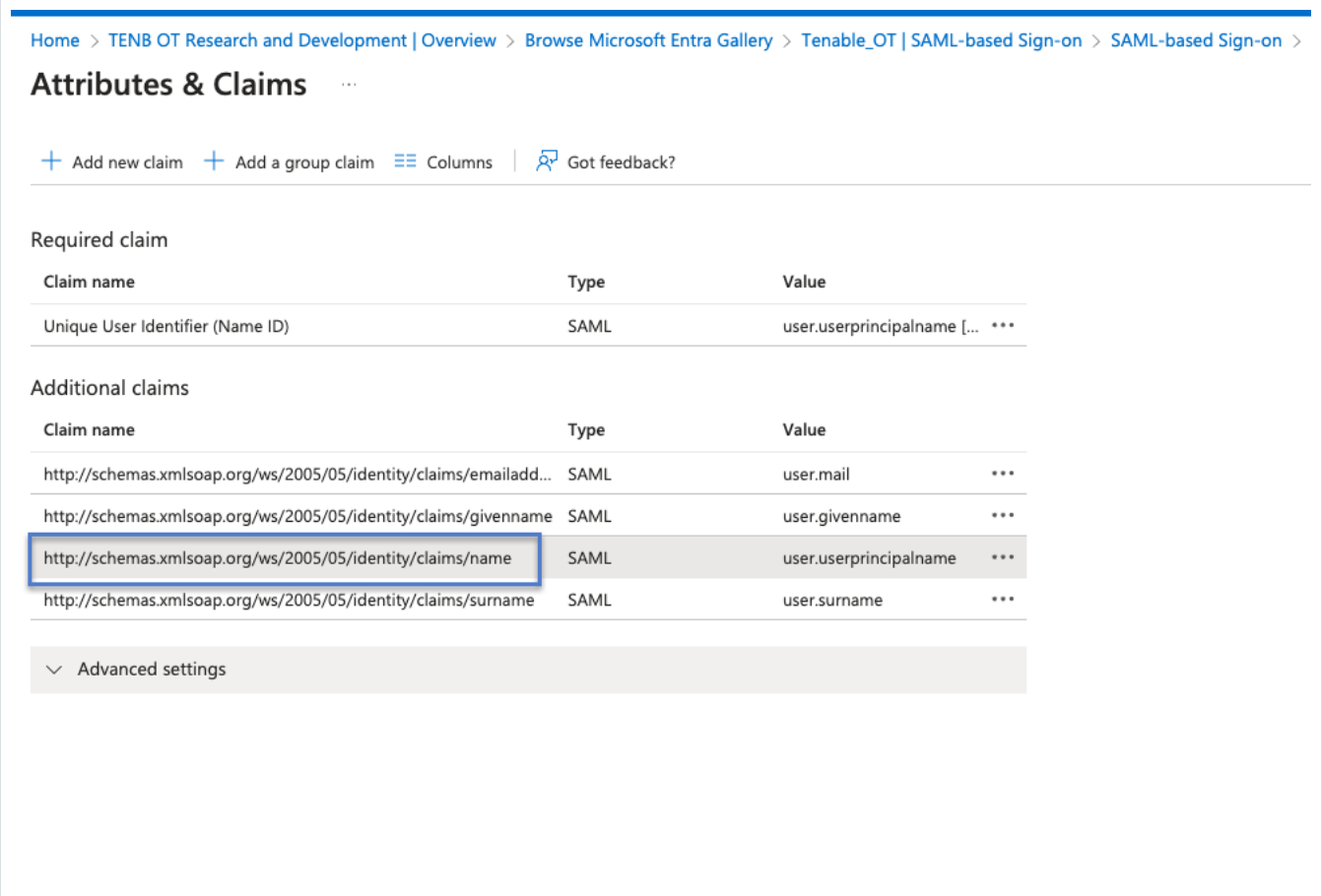
10. Return to the OT Security console and paste the copied value into the IDP URL box.

11. In the Azure console, in section 3 - SAML Certificates, for Certificate (Base64), click Download.

12. Return to the OT Security console and in the Certificate Data section, Browse to the security certificate file and select it.

13. In the Azure console, in section 2 - Attributes & Claims, click Edit.

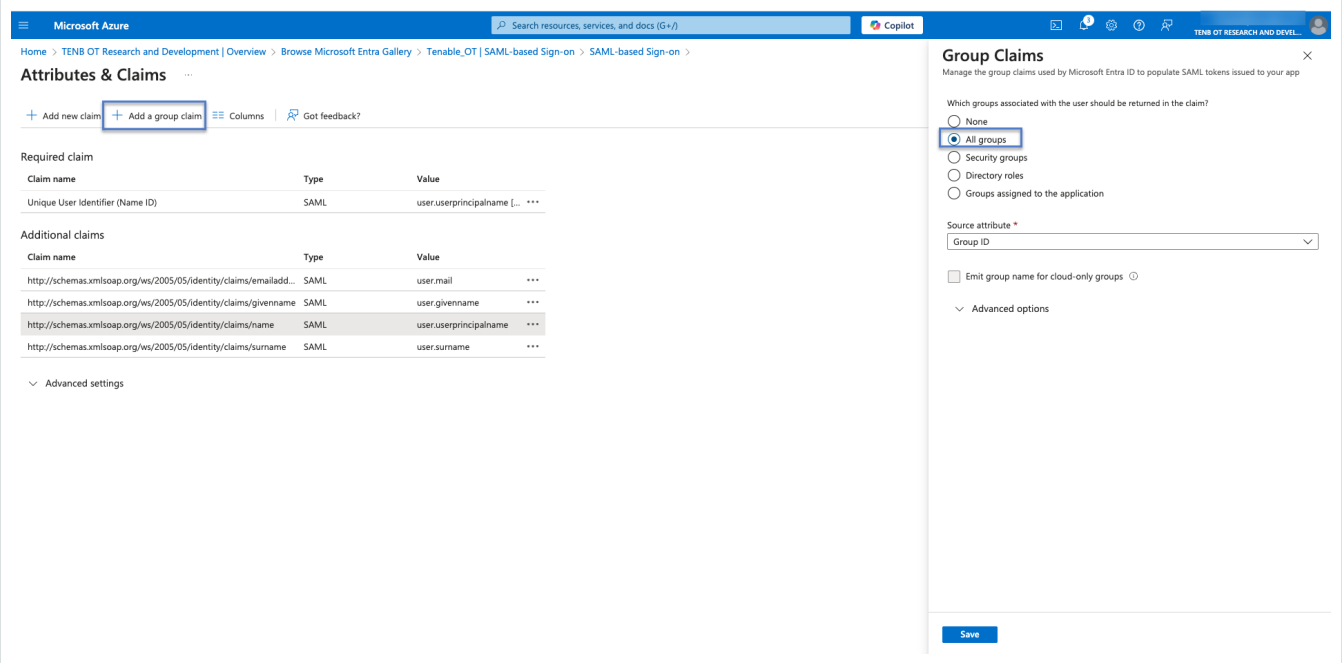
14. In the Additional claims section, select and copy the Claim name URL corresponding to the Value - user.userprincipalname.



15. Return to the OT Security console and paste this URL in the Username Attribute box.

16. In the Azure console, click + Add a group claim.

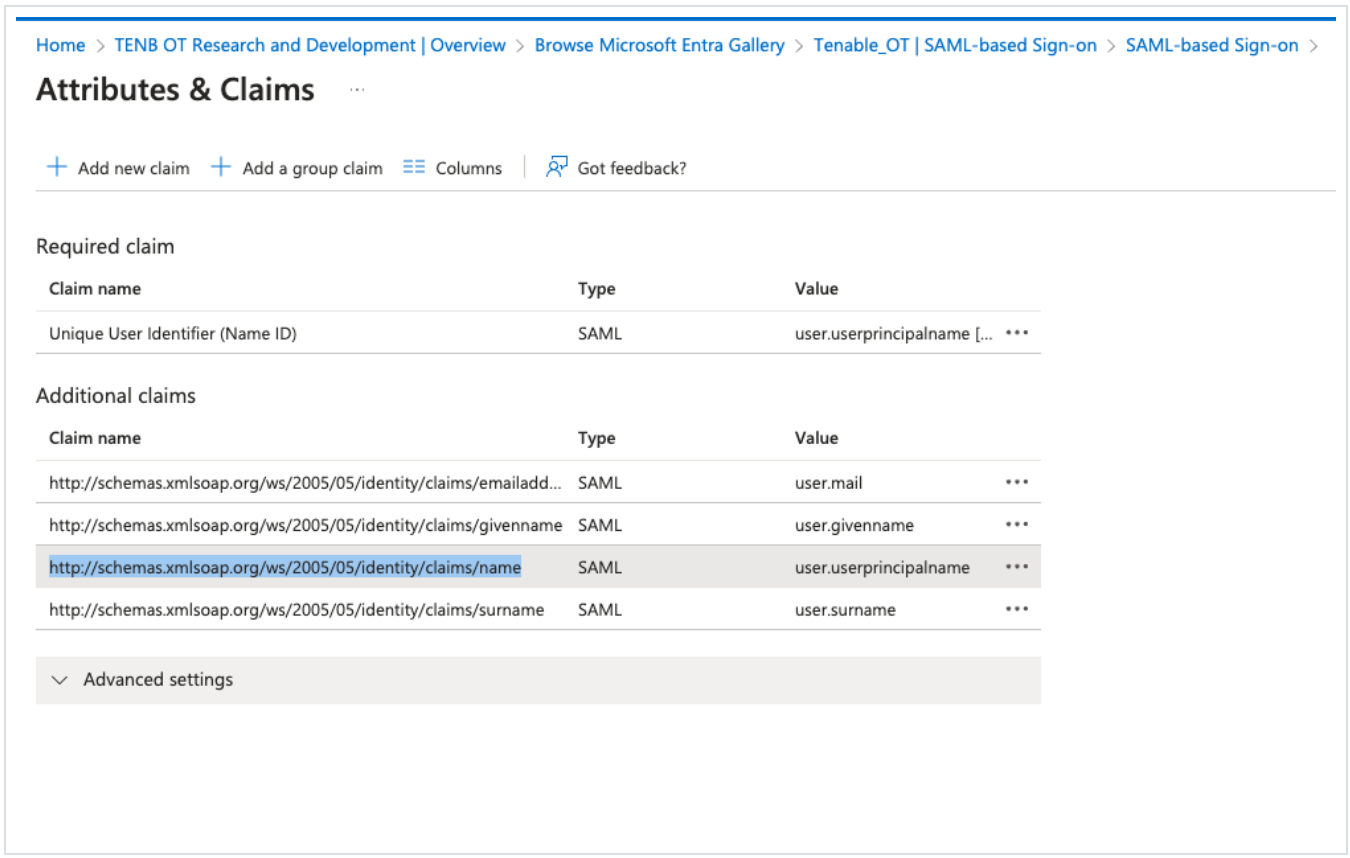
    The Group Claims side panel appears.



17. In the Which groups associated with the user should be returned in the claim? section, select All groups and click Save.

> Note: If you enable the groups setting in Azure, you can select Groups assigned to the application instead of All Groups, and Azure provides only the user groups assigned to the application.

18. In the Additional claims section, highlight and copy the Claim name URL associated with the Value– user.groups [All].



19. Return to the OT Security console and paste the copied URL in the Groups Attribute box.
20. (Optional) Add a description of the SAML configuration in the Description box.

Step 3 - Map Azure Users to Tenable Groups

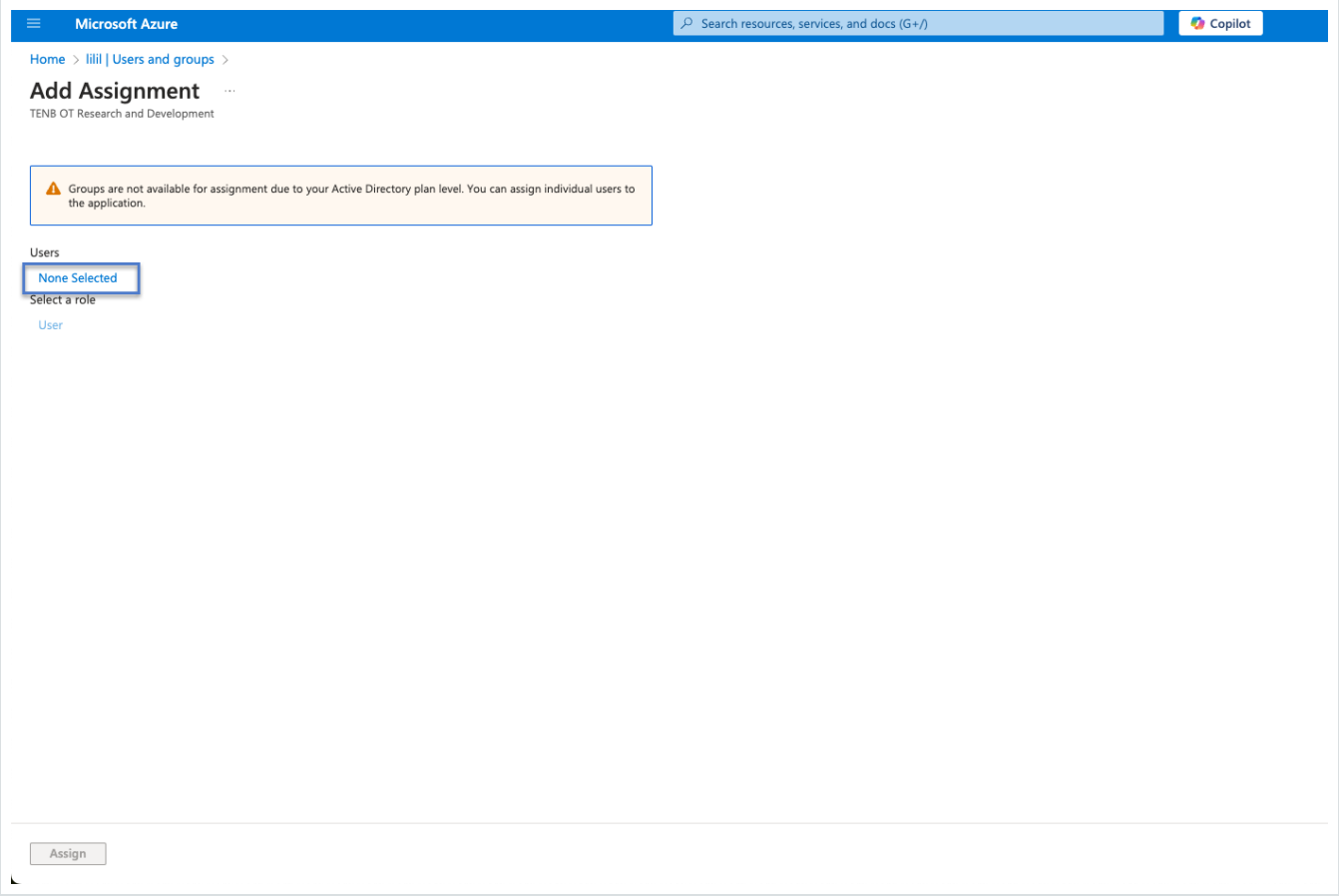
In this step, you assign Azure users to the OT Security application. The permissions granted to each user are designated by mapping between the Azure groups to which they are assigned and a pre-defined OT Security User Group, which has an associated role and set of permissions. The OT Security pre-defined 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 mapped to a OT Security User Group.

Note: Administrator users logged in via SAML are considered Administrators (External) users and are not granted all the privileges of local Administrators. Users assigned to multiple User Groups are granted the highest possible permissions from among their groups.

To map Azure users to OT Security:

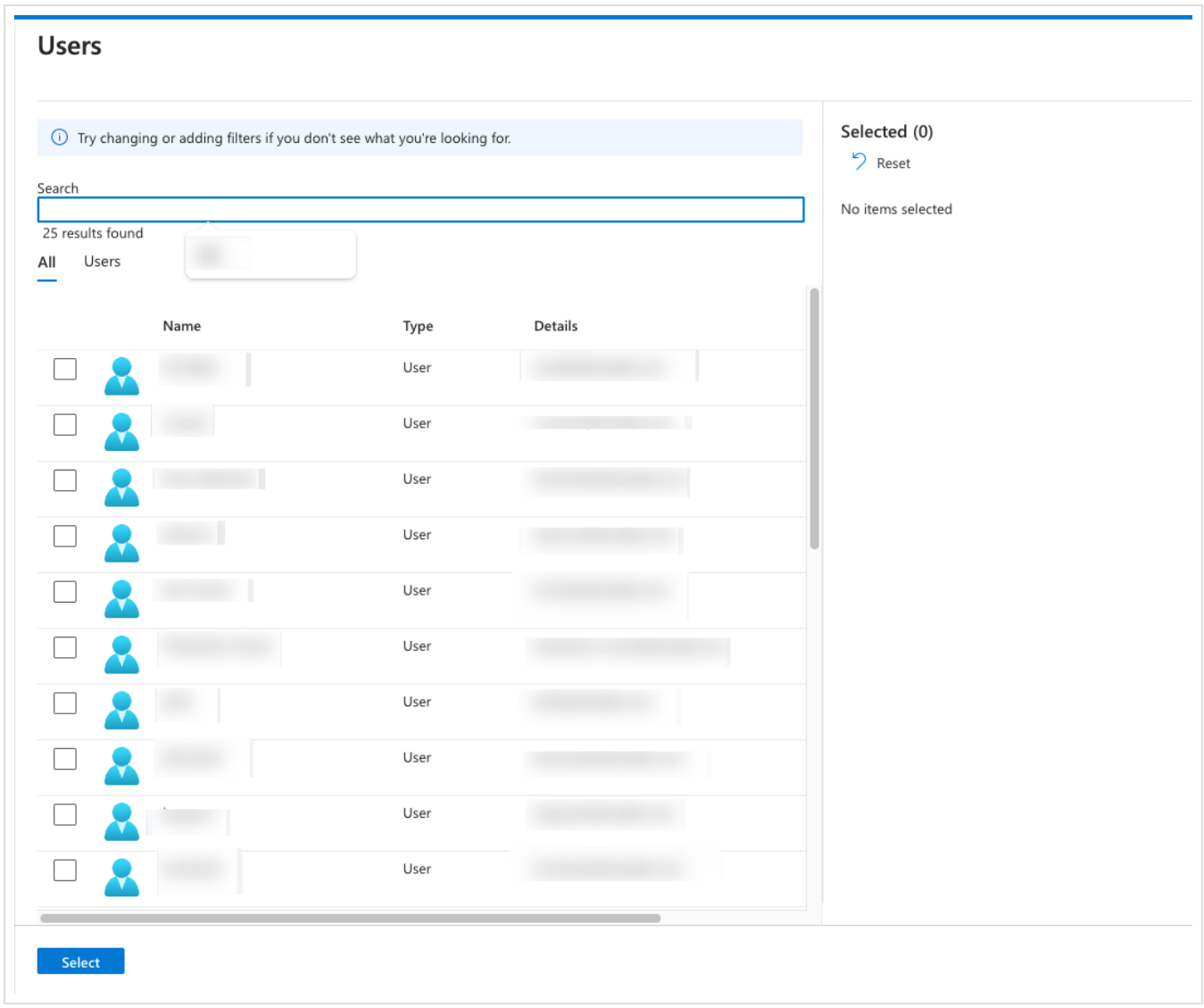
1. In Azure, navigate to the Users and groups page and click + Add user/group.
2. In the Add Assignment page, under Users, click None Selected.

   The Users page appears.



Note: If you enable the groups setting in Azure and select Groups assigned to the application instead of All Groups, you can assign groups instead of individual users.

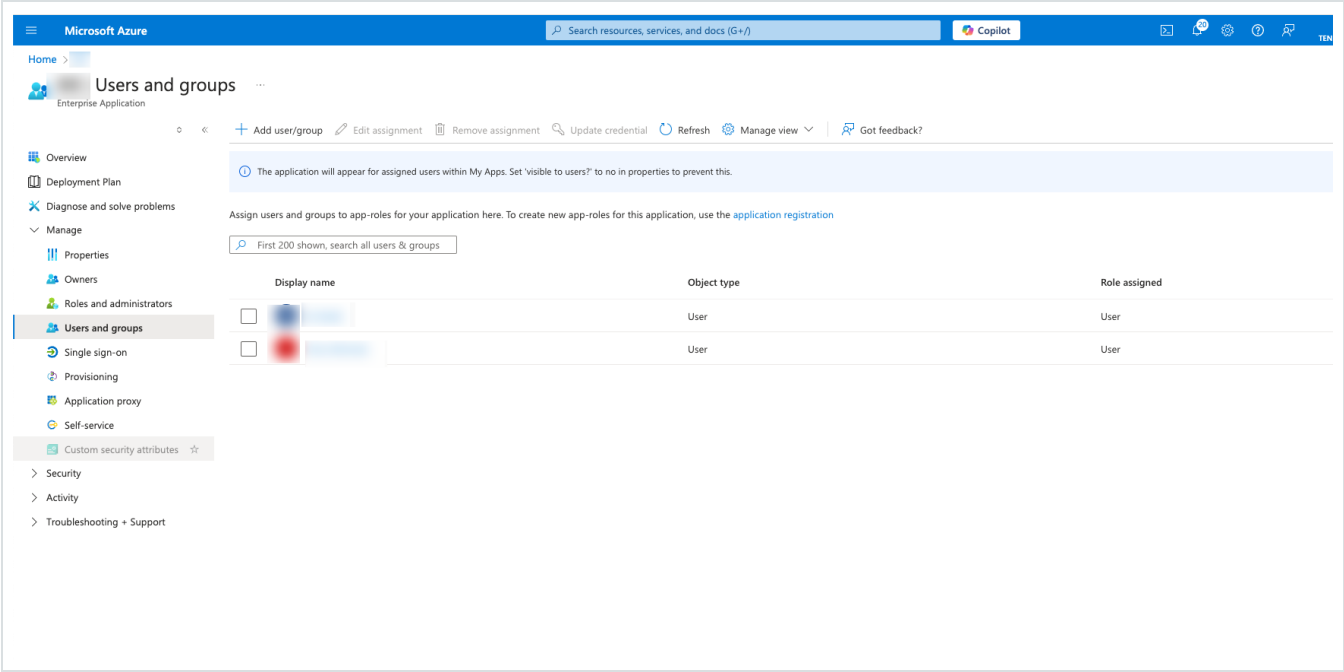
3. Search and select all required users, then click Select.



4. Click Assign to assign them to the application.

   The Users and groups page appears.

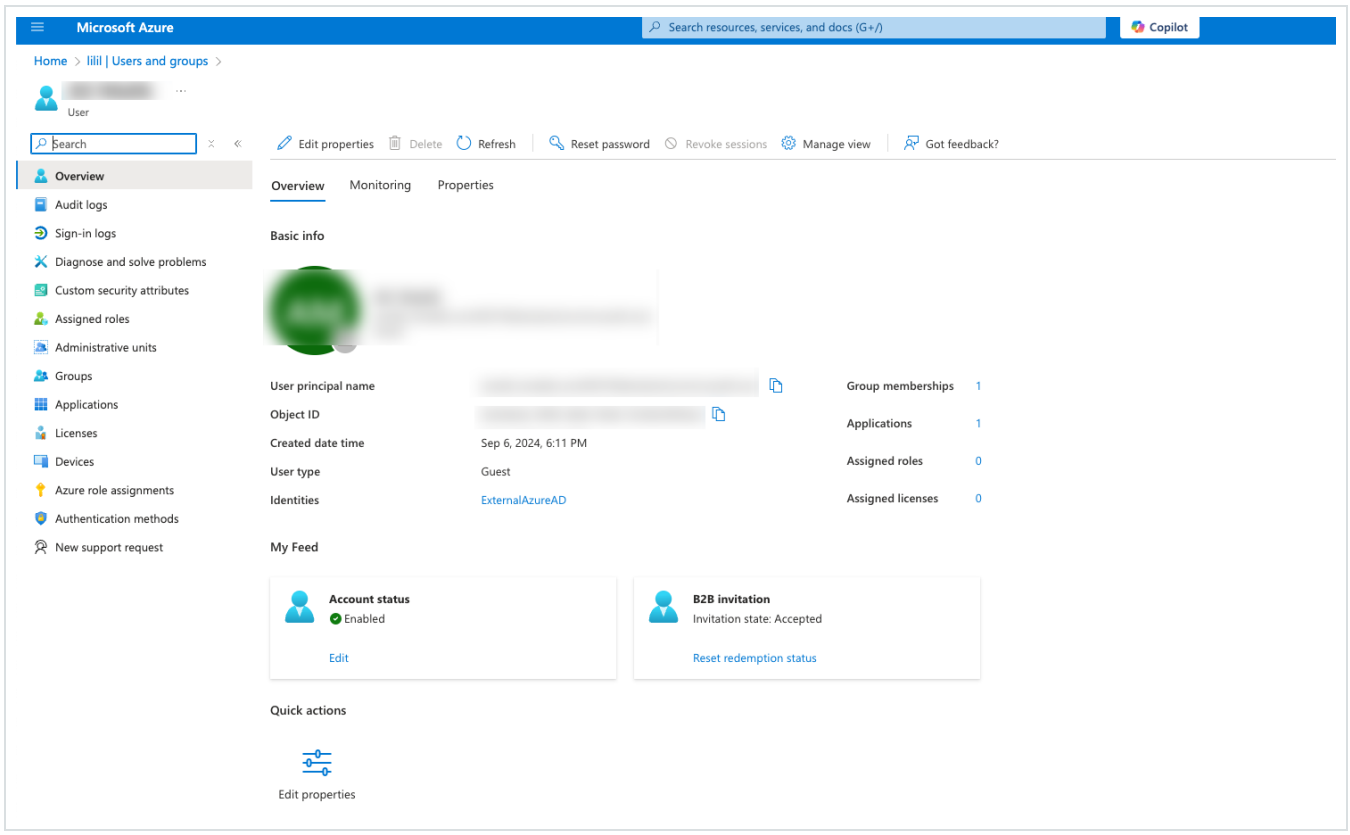
5. Click the Display Name of a user (or group) to display that user's (or group's) Profile.



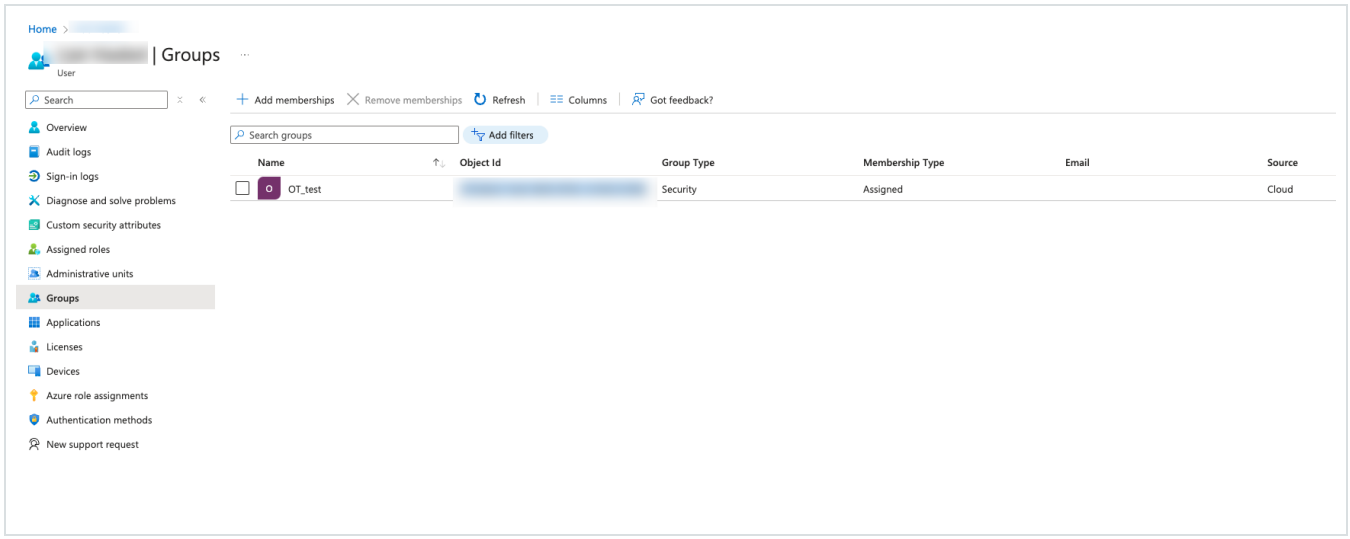
The Profile page appears.

6. In the left navigation bar, select Groups.

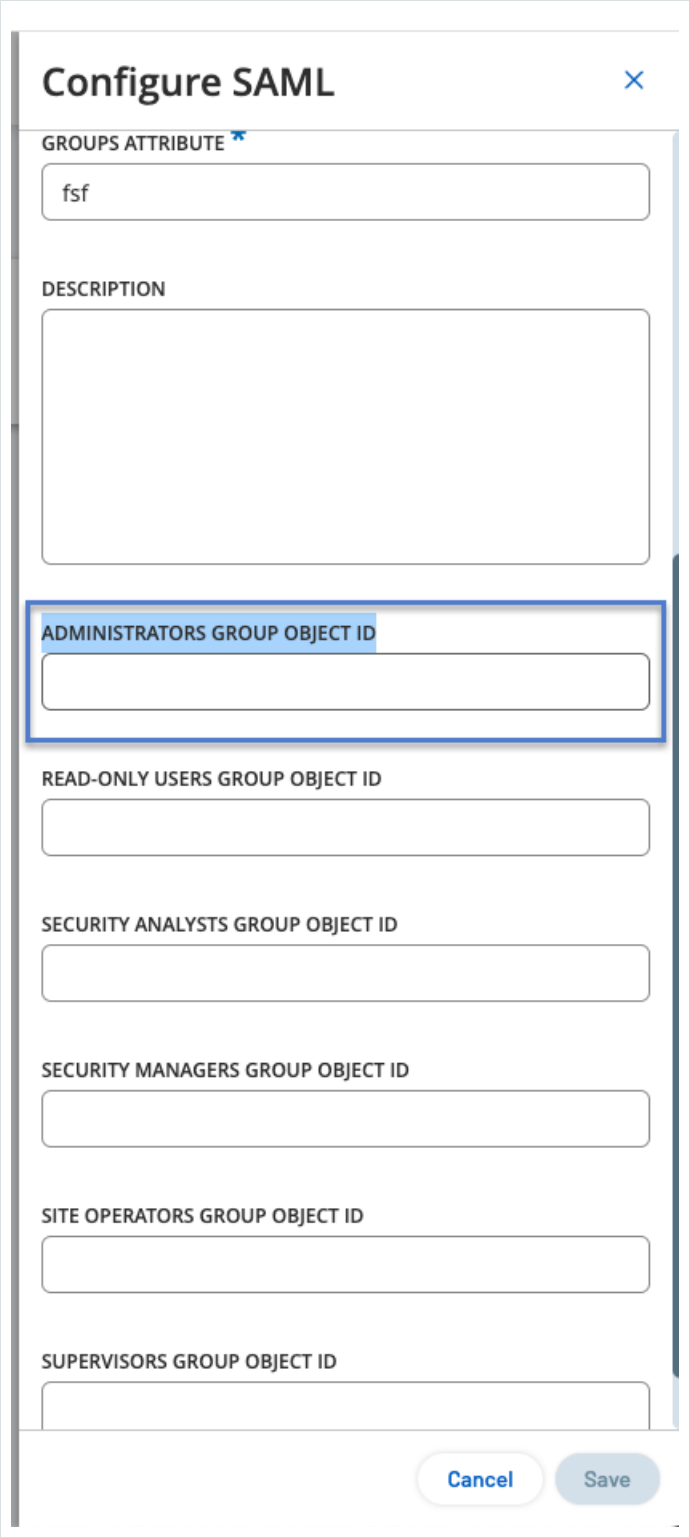
   The Groups page appears.



7. In the Object Id column, select and copy the value for the group that will be mapped to Tenable.



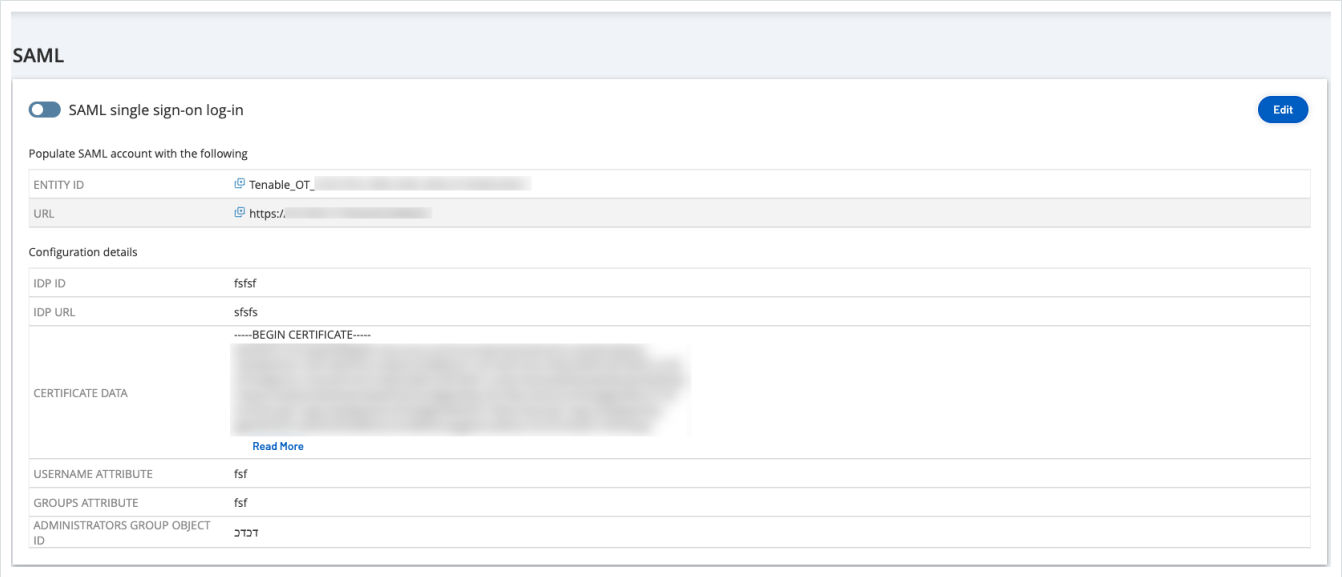
8. Return to the OT Security console and paste the copied value in the required Group Object ID box. For example, the Administrators Group Object ID.



9. Repeat steps 1-7 for each group you want to map to a distinct user group in OT Security.

10. Click Save to save and close the side panel.

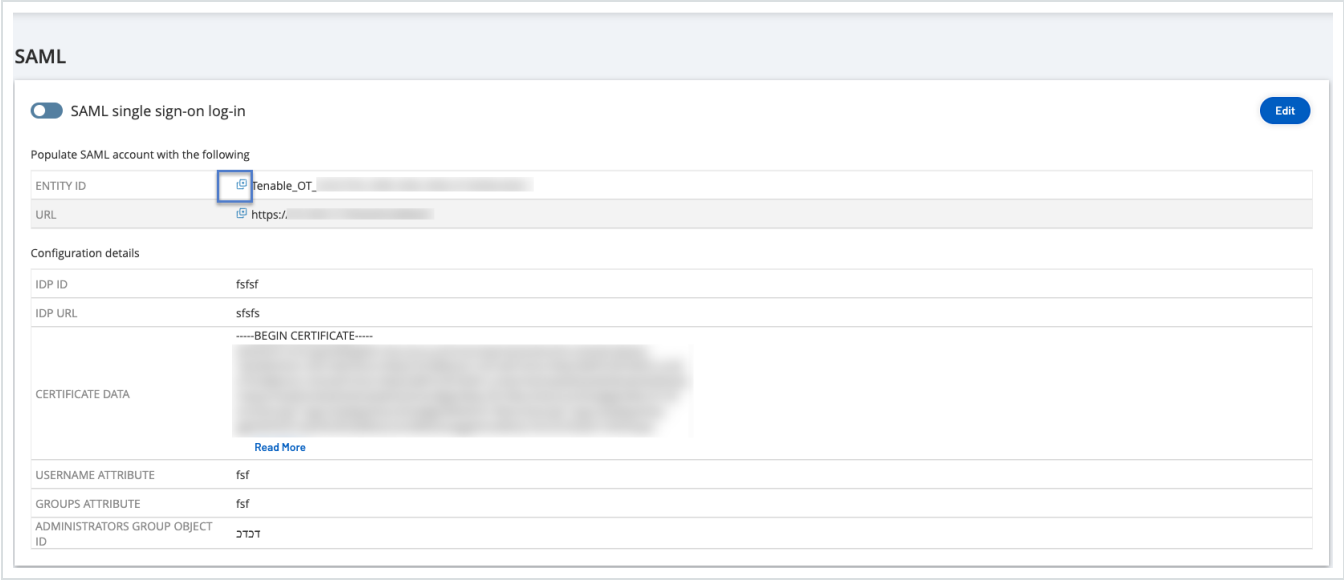
    The SAML page appears in the OT Security console with the configured information.



Step 4 - Finalizing the Configuration in Azure

To finalize the configuration in Azure:

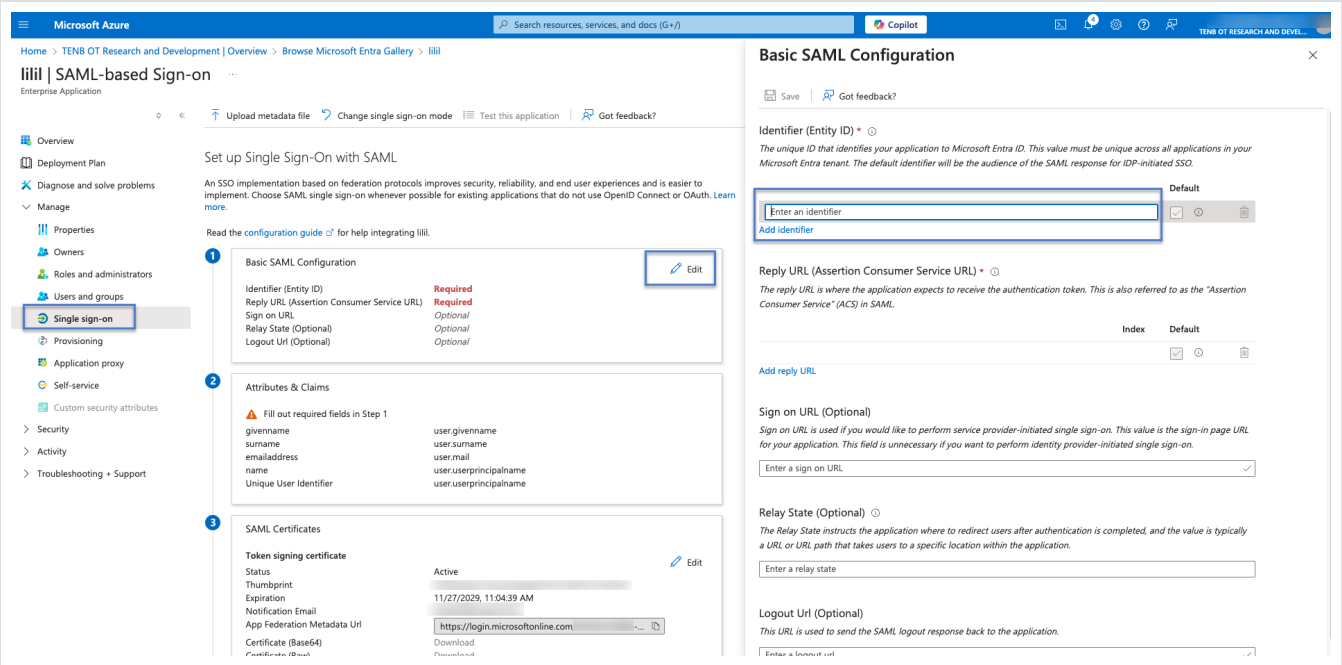
1. In the OT Security SAML page, click the the button to copy the Entity ID.



2. In the Azure console, click Single sign-on in the left navigation menu.

   The SAML-based Sign-on page appears.

3. In section 1 - Basic SAML Configuration, click Edit and paste the copied value in the Identifier (Entity ID) box, replacing the temporary value you entered earlier.



4. Switch to the OT Security and in the SAML page, click the button to copy the URL.

5. Switch to the Azure console and in the Basic SAML Configuration section, paste the copied URL in the Reply URL (Assertion Consumer Service URL) replacing the temporary URL you entered earlier.

6. Click Save to save the configuration, and close the side panel.

   The configuration is complete and the connection appears on the Azure Enterprise applications page.

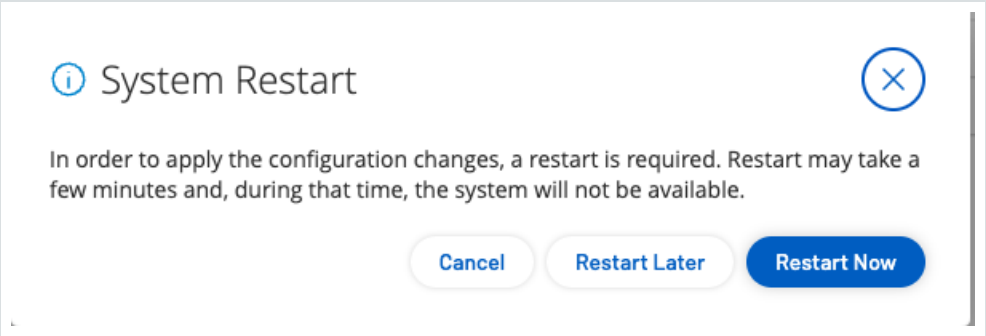
Step 5 – Activate the Integration

To activate the SAML integration, you must restart OT Security. You may restart the system immediately or choose to restart it later.

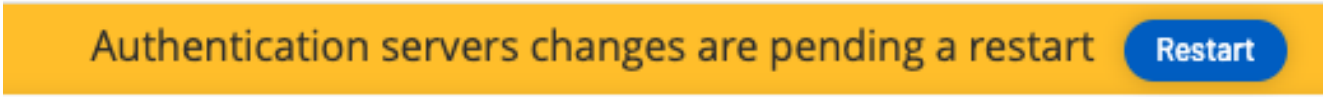
To activate the integration:

1. In the OT Security console, on the SAML page, click the SAML single sign on login toggle to enable SAML.

   The System Restart notification window appears.



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

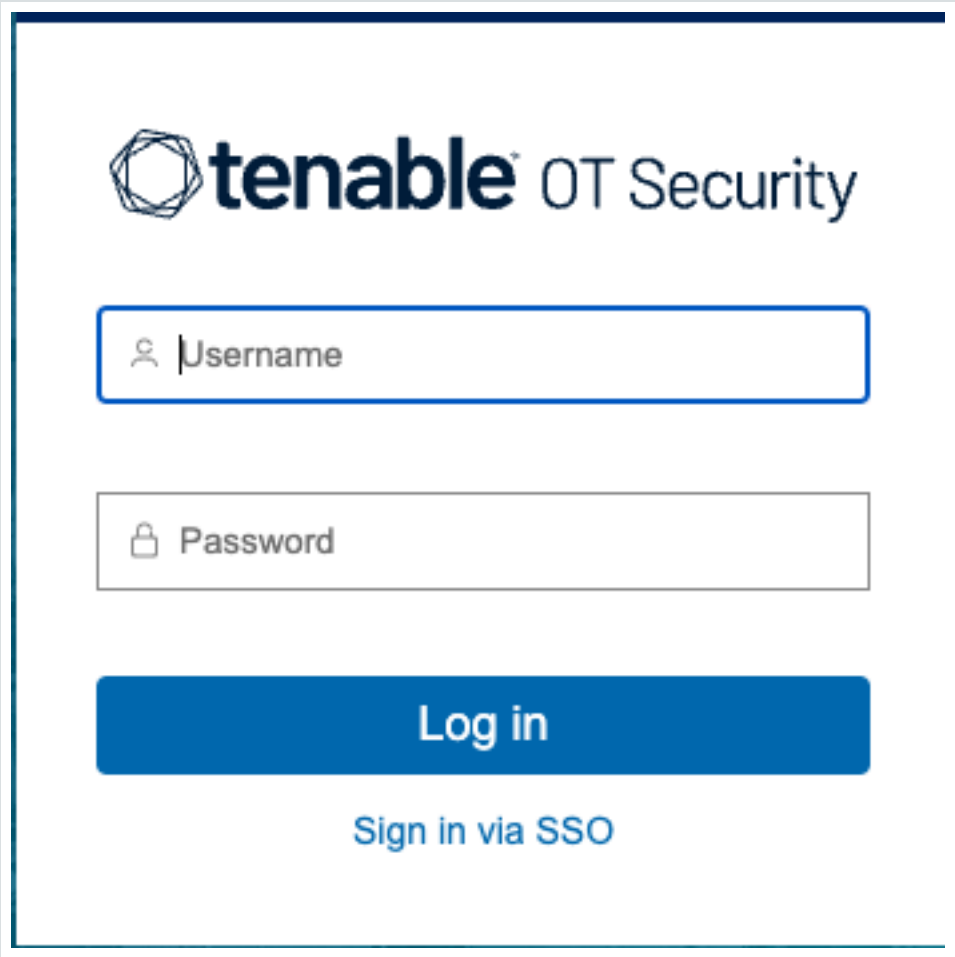


Sign in Using SSO

After the restart, the OT Security login window has a new Sign in via SSO link underneath the Log in button. Azure users 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 window, 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.

If you have more than one account, OT Security redirects you to the Microsoft Pick an account page, where you can select the required account for login.