



# **Tenable OT Security Enterprise Manager 3.16 User Guide**

---

Last Revised: March 12, 2024



## Table of Contents

<b>Welcome to Tenable OT Security Enterprise Manager .....</b>	<b>4</b>
OT Security Technologies .....	6
Solution Architecture .....	7
OT Security Components .....	8
Network Components .....	9
System Elements .....	9
Assets .....	10
Policies and Events .....	11
Policy-Based Detection .....	12
Anomaly Detection .....	13
Policy Categories .....	14
Groups .....	15
Events .....	16
<b>Deployment Specifications .....</b>	<b>17</b>
<b>Set Up OT Security EM .....</b>	<b>19</b>
<b>OT Security EM Management Console Elements .....</b>	<b>25</b>
Site Mode .....	26
Enterprise Mode .....	27
Main User Interface Elements .....	28
Other Actions .....	31
Customize Tables .....	32
<b>Pair ICP with Enterprise Manager .....</b>	<b>33</b>
<b>Use OT Security EM in Site Mode .....</b>	<b>36</b>



<b>Use OT Security EM in Enterprise Mode .....</b>	<b>37</b>
Dashboards .....	38
Appliances .....	40
Local Settings .....	42
OT Security EM License .....	46
Users Management .....	47
Integrations .....	48
Syslog Servers .....	54
System Actions .....	56
System Log .....	58
Send System Log to a Syslog Server .....	59
<b>Revision History .....</b>	<b>60</b>



---

# Welcome to Tenable OT Security Enterprise Manager

---

Tenable OT Security Enterprise Manager (OT Security EM)(formerly Tenable.ot Enterprise Manager) provides an additional layer of enterprise-wide visibility and control on top of the standard functionality of OT Security. Each instance of OT Security offers full threat detection and asset management capabilities for the site at which it is deployed. The OT Security EM enables you to access the full functionality of all of your OT Security instances from a single application.

## Tenable OT Security Functionality

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 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 \(Tenable University\)](#)



---

## 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**

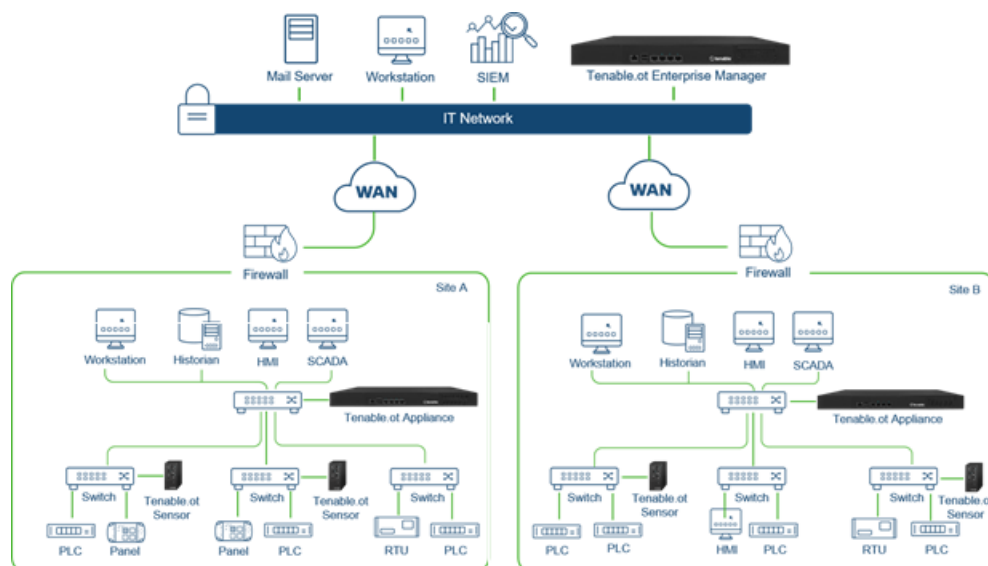
---



# OT Security Components

The OT Security solution is composed of these components:

- **Tenable OT Security Enterprise Manager (OT Security EM)** – This component collects data from OT Security at multiple sites, enabling you to configure, manage, control, and report on everything that happens across your OT enterprise. The OT Security EM can be deployed on premises as part of your NOC/SOC on a dedicated appliance (same model as the on-site OT Security appliance), or it can be deployed on a private or public cloud such as a virtual machine or AWS cloud service.
- **OT Security** – 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 OT Security 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. The sensors are available in two form factors: compact rack mount or DIN-Rail mount. OT Security sensors provide full visibility into these network segments by capturing all the traffic, analyzing it and then communicating the information to the OT Security appliance. 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.

- **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<sup>1</sup>.

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

## System Elements



## Assets

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

## Risk Assessment

OT Security applies sophisticated algorithms to assess the degree of risk posed to each asset on the network. A Risk Score (from 0 to 100) is given for each Asset in the network. The Risk score is based on the following factors:

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

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

- **Vulnerabilities** – CVEs that affect assets in your network, as well as other threats identified in your network (for example, obsolete operating systems, usage of vulnerable protocols, vulnerable open ports, and so on.). In the OT Security, these are detected as plugin hits on your assets.
- **Asset Criticality** – A measure of the importance of the device to the proper functioning of the system.

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



## Policies and Events

---

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

There are two types of policy events:

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

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



---

## Policy-Based Detection

---

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

The following are some examples of possible policy configurations:

- **Anomalous or unauthorized ICS control-plane activity (engineering)** – An HMI should not query the firmware version of a controller (may indicate reconnaissance), and a controller should not be programmed during operational hours (may indicate unauthorized, potentially malicious activity).
- **Change to controller's code** – A change to the controller logic was identified ("Snapshot mismatch").
- **Anomalous or unauthorized network communications**– An un-allowed communication protocol was used between two network assets or a communication took place between two assets that never communicated before.
- **Anomalous or unauthorized changes to the asset inventory** – A new asset was discovered or an asset stopped communicating in the network.
- **Anomalous or unauthorized changes in asset properties** – The asset firmware or state has changed.
- **Abnormal writes of set-points** – Events are generated for changes made to specific parameters. The user can define the allowed ranges for a parameter and generate Events for deviations from that range.



## Anomaly Detection

---

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

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



---

## Policy Categories

---

The Policies are organized by the following categories:

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



---

## Groups

---

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



---

## Events

---

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

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





## Deployment Specifications

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

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

Specification	On-Premises	Public Cloud	Private Cloud
Hardware	Intel® Xeon™ D1548, 2.0 GHz  2 X 32GB DDR4, 2400 MHz  Data: 2 x 2TB Fixed SATA3 HDD  OS: 1 X 64 GB SSD	AWS	4 CPUs, 64GB RAM, Storage (3 disks): 64GB, 1TB and 1TB or more for network traffic captures, 3 NICs ESX version: 6.0 (or later)
Form Factor	Dimensions: 438 x 44 x 321 mm  Weight: 6 kg	N/A	N/A
Power	220W; Single PS Input AC 90V~264V	N/A	N/A
Cooling	CPU heatsink with fan duct 2 X cooling fans	N/A	N/A
Temperature	Operating: 0°C ~40°C/32°F ~104°F	N/A	N/A



	<p>Storage: - 20~70° C / -4°F ~158°F</p> <p>Humidity: 5% ~ 90%</p>		
--	--	--	--



## Set Up OT Security EM

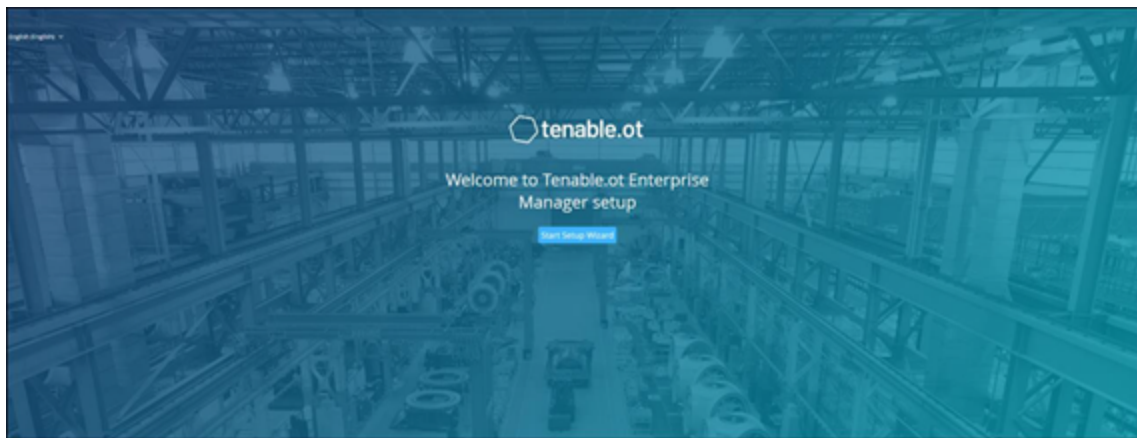
The Initial setup of OT Security EM involves two steps:

1. Run the Setup Wizard and provide relevant configuration information.
2. [Pair ICP with OT Security EM](#). . You can also contact your Tenable support agent and ask them to connect each of your sites to the OT Security EM.

To initiate the OT Security EM setup:

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

The Welcome page of the OT Security EM setup wizard opens.



**Note:** You can access the user interface from the latest Chrome browser version.

2. Click **Start Setup Wizard**.

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

The OT Security EM Setup Wizard takes you through the process of configuring the basic system settings.

**Note:** To change the configuration later, you can do so from **Local Settings** in the Management Console (user interface).

### Setup Wizard – User Information

On the **User Info** page, provide your user account information:



1. In the **Username** box, type a username for logging into the system.

The username must include only lowercase letters and numbers.

The screenshot shows the 'IEM Setup Wizard' interface. At the top, there is a progress bar with three steps: 'User Info' (active, indicated by a blue dot), 'Device', and 'System Time'. Below the progress bar, the form contains five input fields, each with a red asterisk indicating a required field: 'USERNAME', 'RETYPE USERNAME', 'FULL NAME', 'PASSWORD', and 'RETYPE PASSWORD'. The 'PASSWORD' and 'RETYPE PASSWORD' fields have a small eye icon on the right side, indicating a password field. At the bottom right of the form, there is a 'Next >' button.

2. In the **Retype Username** box, re-type the identical username.
3. In the **Full Name** box, type your complete first and last name.

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

4. In the **Password** box, type a password to be used for logging into the system.

The password must contain at least:

- 12 characters
- One uppercase letter



- One lowercase letter
- One digit
- One special character

5. In the **Retype Password** box, re-type the identical password.

6. Click **Next**.

The **Device** page appears.

## Setup Wizard – Device

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

1. In the **Device Name** box, type a unique identifier for the OT Security EM.

**IEM Setup Wizard**

Progress: User Info (completed), Device (current), System Time (pending)

**DEVICE NAME \***  
The name of the tenable.ot enterprise manager

**IP \***

**SUBNET MASK \***

**GATEWAY**

Next >



2. In the **IP** box, type an IP address (within the network subnet) to apply to the OT Security EM.

This becomes the OT Security EM IP address.

3. In the **Subnet Mask** box, type the subnet mask of the network.
4. To set up a Gateway (optional), type the gateway IP for the network in the **Gateway** box.

**Note:** If you do not provide this value, OT Security cannot communicate with external components outside of the subnet (for example, email servers, syslog servers and so on.).

5. Click **Next**.

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

### Setup Wizard – System Time

On the **System Time** page, the correct time and date are set automatically. If the correct date and time are not set, do as follows:

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

To set the date and time:

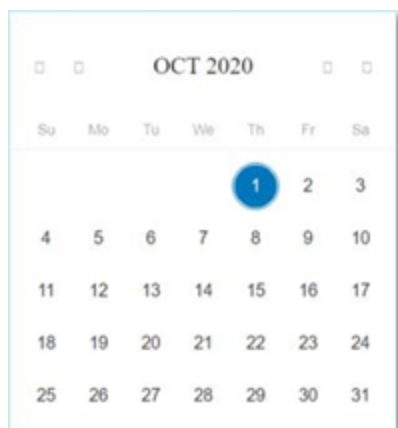


1. In the **Time Zone** drop-down box, select the local time zone at the site location.

The screenshot shows the 'IEM Setup Wizard' with three steps: 'User Info', 'Device', and 'System Time'. The 'System Time' step is active. It contains three fields: 'TIME ZONE' with a dropdown menu showing 'Etc/UTC', 'DATE' with the value '05/18/2022' and a calendar icon, and 'TIME' with the value '11:23:04' and a clock icon. At the bottom are two buttons: '< Back' and 'Complete and Restart'.

2. In the **Date** box, click the calendar icon .

A pop-up calendar appears.





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

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

5. To complete the setup procedure, click **Complete** and **Restart**.
6. Once the restart is complete, OT Security EM redirects you to the **Login** page.

After completing the setup wizard, contact Tenable Support to add your sites to OT Security EM.





---

## OT Security EM Management Console Elements

---

The OT Security EM Management Console (user interface) provides easy access to enterprise-wide data that OT Security appliances discover at the various sites. This data relates to asset management, network activity, and security events. OT Security EM also enables you to configure and manage the OT Security appliance for each of your sites.

For information about specific user interface functionality, see [Use OT Security EM in Site Mode](#) and [Use OT Security EM in Enterprise Mode](#).



# Site Mode

In Site mode, the user interface shows data for one particular site. In this mode, the OT Security EM user logs in as an administrator, with full access to all OT Security functionality such as viewing data, configuring policies, and adjusting system settings except for creating and managing local users. For information about using the OT Security EM in Site mode see [Use OT Security EM in Site Mode](#).

tenable.ot

10:02 AM • Monday, Oct 9, 2023 • admin (behalf of IEM)(External)

CB

Controllers and Modules

Search...

Actions

Dashboards

Risk

Inventory

Events and Policies

Events

Policies

Inventory

All Assets

Controllers and Modules

Network Assets

Network Map

Vulnerabilities

Active Queries

Network

Backplane #1 (2)

☐

S71500/ET200MP station\_1

PLC

48

High

(Direct)

Siemens

S7-1500

CPU 1511-1 PN

2.9.4

☐

Backplane Module #13

Backplane M...

29

High

Siemens

SIMATIC

Backplane #10 (2)

☐

PLC #23

PLC

55

High

Schneider

Concept

☐

Comm. Adapter #22

Communicati...

26

High

(Direct)

Schneider

Backplane #105 (2)

☐

PLC #137

PLC

16

High

Siemens

S7-1200

2.1.2

☐

siemensegy

PLC

16

High

(Direct)

Siemens

S7-1200

CPU-1200

2.1.2

Backplane #120 (2)

☐

PLC #139

PLC

64

High

Siemens

S7-300

2.0.5

☐

acrq

Communicati...

62

High

(Direct)

Siemens

S7-300

CP 343-1

3.1.1



# Enterprise Mode

In Enterprise mode, the user interface shows information about each of your appliances. You can also view and adjust the local EM settings, including local user management. For more information about the data and actions available in Enterprise mode, see [Use OT Security EM in Enterprise Mode](#).

tenable.ot

10:09 AM • Monday, Oct 9, 2023 • Mr. Admin

EM

Dashboards

Risk

Inventory

Events and Policies

Appliances

Local Settings

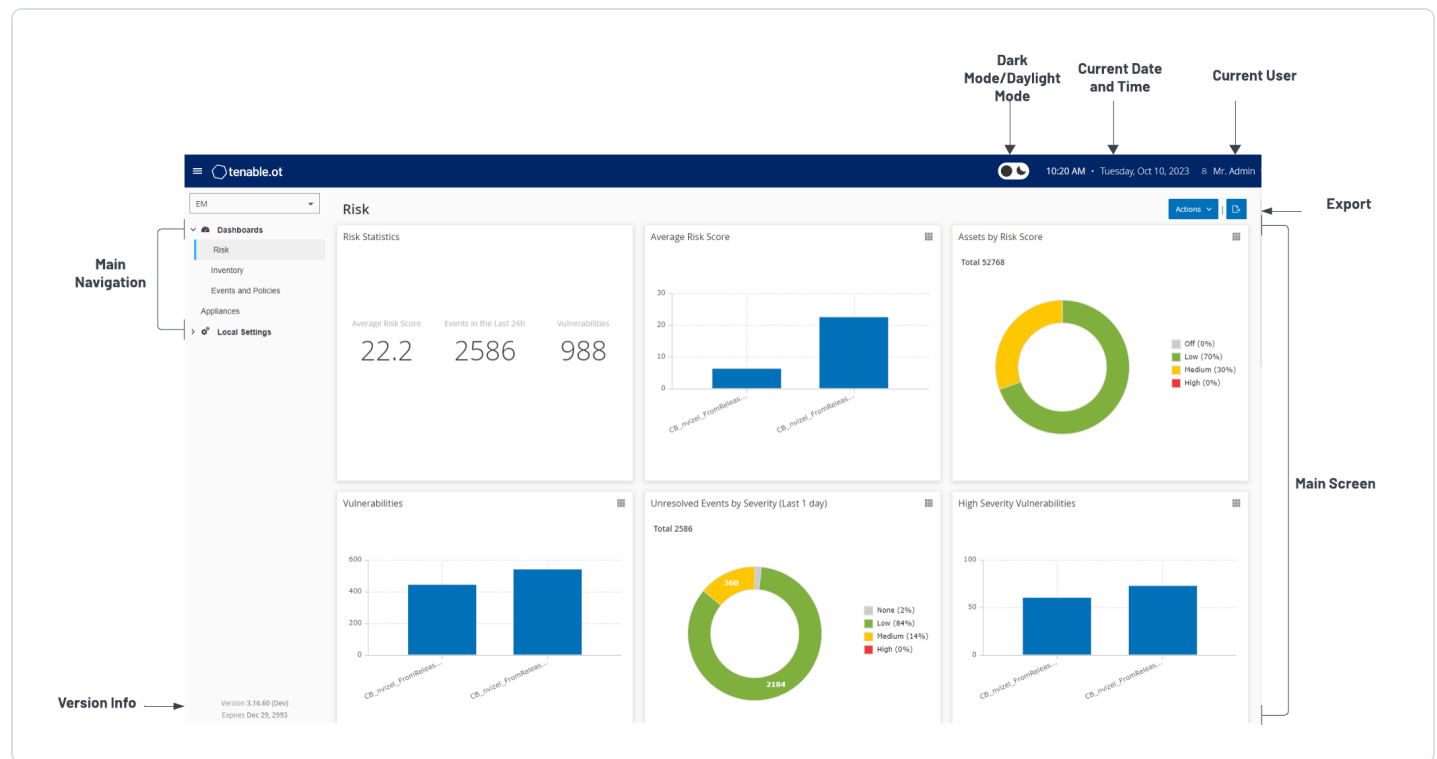
Appliances

Search...


Site ↑	IP/Host	Last Sync	Version	License Type	License Expires	Licensed Ass
<a href="#">CB_nvizel_FromReleaseC...</a>		Oct 9, 2023 10:09:15 AM	3.16.60 (Dev)	Perpetual	Dec 29, 2993 03:30:00 PM	Unlimited
<a href="#">CB_nvizel_FromReleaseC...</a>		Oct 9, 2023 10:09:05 AM	3.16.60 (Dev)	Perpetual	Dec 29, 2993 03:30:00 PM	Unlimited



# Main User Interface Elements



The following table describes the main user interface elements:

User interfaceElement	Description
<b>Mode Selection</b>	Select a mode: <b>EM</b> for Enterprise mode or select a particular site for Site mode.
<b>Main Navigation</b>	Main navigation menu. Click the  icon to show/hide the main navigation menu.
<b>Current Date and Time</b>	The current date and time as in the system.
<b>Current User</b>	The name of the user currently logged in. Click the down arrow for a selection menu. Options are: <b>About</b> (shows software information) and <b>Logout</b> .
<b>Version Info</b>	The version of OT Security EM.



<b>Main Screen</b>	The screen that you select in the main navigation.
<b>Dark Mode/Daylight Mode</b>	Change the display color scheme to Dark mode or Daylight mode.
<b>Export</b>	Downloads a PDF of the dashboard.

## Enterprise Mode and Site Mode Navigation Pages

### Enterprise Mode

For Enterprise mode (EM), the following navigation options are available:

- **Dashboards** — View widgets containing graphs and tables that give an at-a-glance view of your entire enterprise's inventory and security posture based on the aggregated data from your sites. There are separate dashboards for **Risk**, **Inventory**, and **Events and Policies**. See [Dashboards](#).
- **Appliances** — Displays information about each of the sites connected to EM. See [Appliances](#).
- **Local Settings** — View and configure the EM settings, and view and generate a certificate for secure HTTPS connections for the EM. See [Local Settings](#).
- **User Management** — View and configure users for the OT Security EM. See [Users Management](#).
- **System** — Displays system-level options. For example: **Factory Reset**, **Download Diagnostics Data**, **Restart**, and **Shut Down**. See [Syslog Servers](#).

### Site Mode

For Site mode, the following navigation options are available for a specified site:

- **Dashboards** — View widgets containing graphs and tables that give an at-a-glance view of your Site's inventory and security posture. There are separate dashboards for Risk, Inventory, and Events and Policies. See [Dashboards](#) in the OT Security User Guide.



- **Events** – Shows all events that occurred as a result of Policy hits. There is a screen for viewing All Events as well as separate screens for viewing Events of each specific type (Configuration Events, SCADA Events, Network Threats, or Network Events). See [Events](#) in the OT Security User Guide.
- **Policies** – View, edit, and activate policies. See [Policies](#) in the OT Security User Guide.
- **Inventory** – Displays an inventory of all the discovered assets, allowing comprehensive asset management, monitoring of the status of each asset, and viewing their related events. View **All assets** as well as view assets of specific types (**Controllers and Modules**, **Network Assets**, and **IoT**). See [Inventory](#) in the Tenable OT Security User Guide.
- **Network Map** – A visual representation of the network assets and their connections throughout time. See [Network Map](#) in the OT Security User Guide.
- **Vulnerabilities** – A detailed list of all the threats in the network detected by OT Security Plugins, and recommended remediation steps. This section also includes CVEs and other threats to the assets in your network. For example, obsolete operating systems, usage of vulnerable protocols, vulnerable open ports, and so on. See [Vulnerabilities](#) in the OT Security User Guide.
- **Network** – A comprehensive view of the network traffic based on data about conversations that took place between assets in the network over time. See [Network](#) in the OT Security User Guide. You can view the details on three separate pages:
  - **Network Summary** – An overview of network traffic.
  - **Packet Captures** – Full-packet captures of network traffic.
  - **Conversations** – A list of all conversations detected in the network, with details about the time that it occurred, involved assets and so on.
- **Groups** – View, create, and edit groups, which are used in policy configuration. See [Groups](#) in the Tenable OT Security User Guide.
- **Local Settings** – View and configure the system settings. See [Local Settings](#) in the OT Security User Guide.




## Other Actions

### Enable or Disable Dark Mode

You can use the Dark Mode color scheme on all pages by toggling the Dark Mode switch.

To enable or disable Dark Mode:

1. In the upper-right corner of the page, click the  (Dark Mode) button to enable the Dark Mode.

OT Security EM applies the setting to all pages.

2. To restore the Daylight Mode setting, click the  (Daylight Mode) button.

### Export the Dashboard

You can use the **Export** button on the **Dashboard** page to export a PDF with each Dashboard widget on a separate page.

To export the Dashboard:

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

The PDF downloads automatically to the default download folder.

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

2. Navigate to the downloaded file to view or share it.



## Customize Tables

---

OT Security displays the data in a table format with a record for each item. These tables have standardized customization features such as show / hide columns, filter, and sort results.

For more information about interacting with tables, see [Customize Tables](#) in the OT Security User Guide.





## Pair ICP with Enterprise Manager

You can pair your Industrial Core Platform (ICP) with OT Security EM and manage all your sites.

### Before you Begin

Make sure that:

- OT Security EM can connect via API to the ICP.
- SSH connection exists between ICP and OT Security EM in both directions.
- HTTPS connections exist between ICP and OT Security EM.

Use the following curl commands to verify the SSH and HTTPS connections:

- From OT Security EM, run:

```
curl -v telnet://<ICP_IP>:22
```

- From ICP, run:

```
curl -v telnet://<ICP_IP>:22
```

- From OT Security EM, run:

```
curl -k https://<ICP_IP> ()
```

- From ICP, run:

```
curl -k https://<IEM_IP>
```

To pair ICP with OT Security EM:

1. Create a pairing object on the OT Security EM for each system you want to connect.

Make sure the .bin file is a unique name, as you need to call it later.



```
sudo /home/indegy/tools/klee --user <IEM_USER> --password <IEM_USER_PASSWORD> --url https://<IEM_IP> iem pairing create --outfile /home/indegy/<pairing_icp_name>.bin
```

Where:

- IEM\_User is the user ID of the system.
- IEM\_User\_Password is the password of the system.
- IEM\_IP is the IP address of the system.
- pairing\_icp\_name is the name of the .bin file.

## 2. Attach to the ICP from the OT Security EM.

```
sudo /home/indegy/tools/klee --url https://<ICP_IP> --user <ICP_USER> --password <ICP_USER_PASSWORD> iem attach --infile /home/indegy/<pairing_icp_name>.bin
```

Where:

- ICP\_IP is the IP address of the ICP.
- ICP\_User is the user ID of the ICP.
- ICP\_User\_Password is the password of the ICP.
- pairing\_icp\_name is the name of the .bin file.

## 3. To confirm that the pairing is succeeded, run the following command from OT Security EM:

```
sudo ./klee --user <IEM_USER> --password <IEM_USER_PASSWORD> --url https://<IEM_IP> iem status
```

OT Security EM pairs with the ICP and you can start managing your sites.

## Cancel a Pairing Process

To cancel or delete a pending pairing process:



1. From OT Security EM, run this command:

```
sudo ./klee --url https://<IEM_URL> --user <IEM_USER>--password <IEM_USER_PASSWORD> iem pairing  
delete
```



## Use OT Security EM in Site Mode

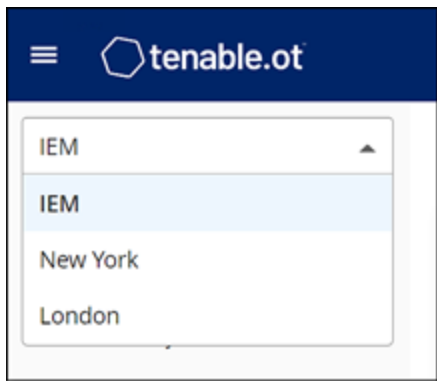
OT Security EM in Site mode is almost similar to the functionality of OT Security for that site. You have full administrator capabilities except that you cannot create or manage users for that site.

For more information about how to use OT Security, see the [Tenable OT Security User Guide](#).

To use OT Security EM in Site Mode:

1. Log in to OT Security EM.
2. Click **Mode Selection**.

A drop-down list appears.



3. Select the site you want to access.

**Note:** Alternatively, when viewing the **Appliances** page in Enterprise Mode, click the site you want to access.

The navigation bar on the left shows the options available for the selected site.

4. Select the required option.

OT Security EM opens the specific page and you can start interacting with OT Security EM in the same way you interact with the OT Security Management Console.



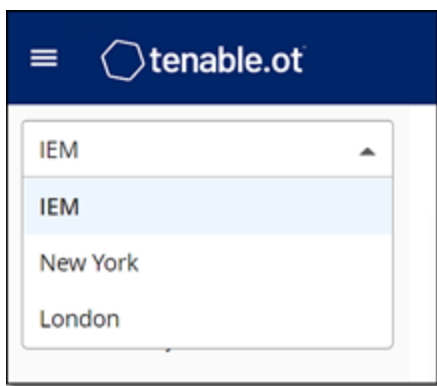
## Use OT Security EM in Enterprise Mode

In Enterprise mode, you can view details about all of your appliances. You can configure and view information about the different appliances and also configure the EM settings.

To use the OT Security EM in Enterprise Mode:

1. Log in to the OT Security EM.
2. Click **Mode Selection**.

A drop-down list appears.



3. Select **EM**.

The navigation bar on the left shows the options available for the Enterprise mode.

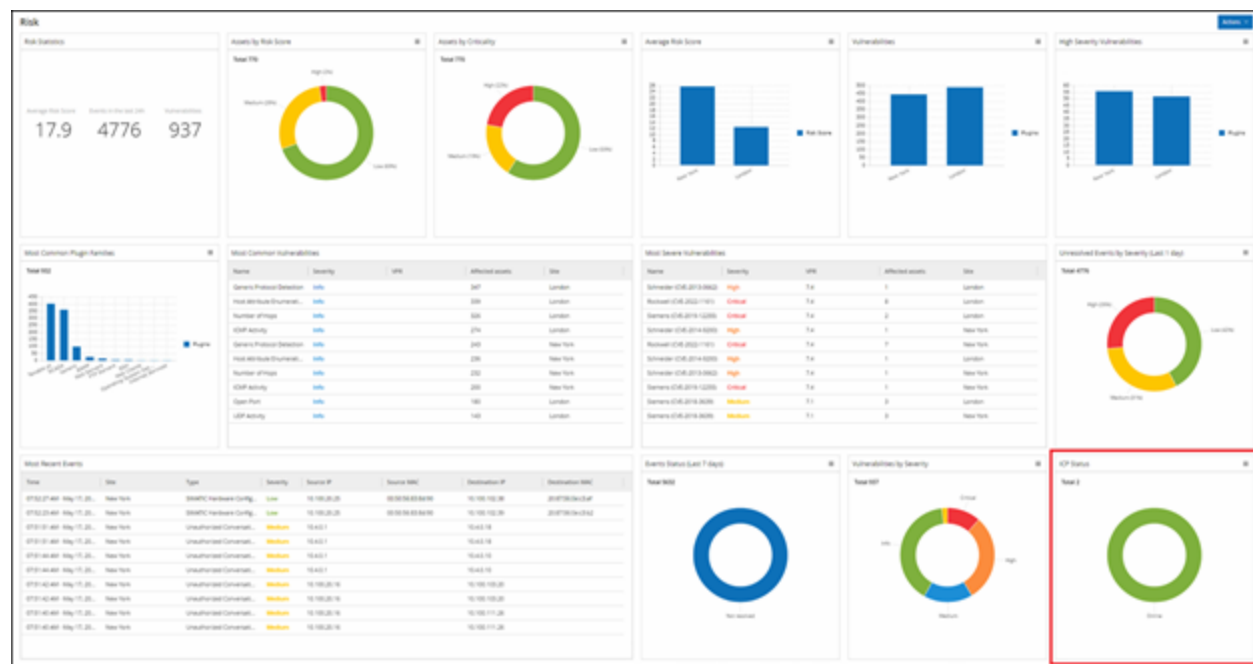
4. Select the required option.

OT Security EM opens the specific page.



## Dashboards

The dashboards contain widgets that offer an at-a-glance view of your complete enterprise inventory and security posture. OT Security EM collects data from all your sites and displays the aggregated data in widgets. In addition to the standard widgets for individual sites, the EM dashboards contain an ICP Status widget that displays the connectivity status of each of your sites.



You can view the following dashboards:

- **Risk** – Provides insights on your entire enterprise's cyber exposure by looking into asset risk scores and vulnerability management metrics. The **Risk** dashboard displays aggregated data in widgets such as: Risk Statistics, Assets by Risk Score, Assets by Criticality, Average Risk Score, Vulnerabilities, Sensors Status and so on.
- **Inventory** – Provides visibility into the entire enterprise's asset inventory, facilitating asset management and tracking. The **Inventory** dashboard displays aggregated data in widgets such as: Inventory Statistics, Assets, Assets by Category, Controllers and Modules by Type, Assets by Purdue Level, and so on.
- **Events and Policies** – Provides a means to detect threats to the enterprise by monitoring the identified events and the policies violations that they generate. The **Events and Policies** dashboard displays aggregated data in widgets such as: Events and Policies Statistics, Hourly Events Breakdown, High Severity Events, Events Status, and so on.




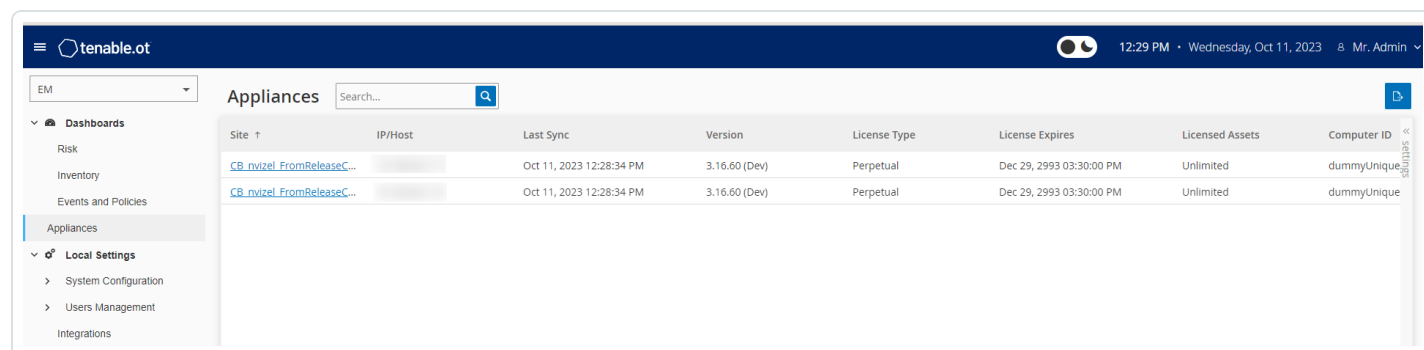
The **Risk** dashboard is the initial default view; however, you can change the default view to a different dashboard by clicking the **Actions** button in the upper-right corner.

You can interact with dashboards by adjusting the display settings and setting filters, see [Interacting with Dashboards](#) in the Tenable OT Security User Guide.



# Appliances

The **Appliances** page lists all your appliances associated with OT Security EM. You can customize the display settings by adjusting the column display and position. To download a CSV file with the appliance information, click the  (Export) button in the upper-right corner. You can also sort and filter the appliances list as well as search for a specific appliance in the **Search** box. For information about customizing tables, see [Customize Tables](#) in the Tenable OT Security User Guide.



Site	IP/Host	Last Sync	Version	License Type	License Expires	Licensed Assets	Computer ID
<a href="#">CB_invizel_FromReleaseC...</a>		Oct 11, 2023 12:28:34 PM	3.16.60 (Dev)	Perpetual	Dec 29, 2993 03:30:00 PM	Unlimited	dummyUnique
<a href="#">CB_invizel_FromReleaseC...</a>		Oct 11, 2023 12:28:34 PM	3.16.60 (Dev)	Perpetual	Dec 29, 2993 03:30:00 PM	Unlimited	dummyUnique

The **Appliances** page includes the following details.

Parameter	Description
<b>Site</b>	The site where the OT Security instance is deployed. The site name is a link to open OT Security EM in Site mode for that site.
<b>IP/Host</b>	The IP or hostname of the OT Security instance.
<b>Last Sync</b>	The date and time when site data synchronized with OT Security EM.
<b>Version</b>	The OT Security software version.
<b>License Type</b>	The license type associated with this appliance. Options are: <b>Subscription</b> or <b>Perpetual</b> .
<b>License Expires</b>	The date and time when the license ages out.
<b>Licensed Assets</b>	The number of licensed assets. The options are: <ul style="list-style-type: none"><li>The number of assets that you are using out of the total number that you are licensed for, and the percentage of licenses used (for example, 464/500 (93%)).</li></ul>





	<ul style="list-style-type: none"><li>• Unlimited.</li></ul>
<b>Computer ID</b>	The unique ID of the site computer.



## Local Settings

You can use the **Local Settings** to view and configure the OT Security EM settings. The **Local Settings** section includes these pages for configuring your settings:

- [Device](#)
- [Certificates](#)
- [License](#)
- [Users Management](#)
- [Local Users](#)
- [Integrations](#)
- [Syslog Servers](#)
- [System Actions](#)

### Device

The page allows you to view and edit device details and network information such as port configuration and system time, automatic logout (inactivity timeout).



tenable.ot

08:23 AM • Wednesday, Jan 18, 2023 • Mr. Admin

EM

Dashboards

Appliances

Local Settings

System Configuration

Device

Port Configuration

Certificates

Users and Roles

Integrations

Servers

System Actions

System Log

Device

Device Name

The name of Tenable.ot management system.

Edit

Device URL

Device URL allows you to set the single URL from which the system can be accessed (FQDN). Editing it is a critical change. The new FQDN will not be presented again. Failure to make note of the exact string will make the UI inaccessible. Please make sure to verify the resolution before proceeding (Change requires restart).

Edit

System Time

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

MANUAL SYSTEM TIME Jan 18, 2023 08:22:06 AM

Edit

Timezone

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

TIMEZONE Etc/UTC

Edit

DNS Servers

DNS servers are used by Tenable.ot to assign DNS names to the assets Tenable.ot identifies. Several servers can be defined.

IP 1 10.100.30.11

Edit

Automatic Logout

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

LOGOUT AFTER 2 Weeks

Edit

☒ Ping Requests

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

Version 3.15.24

The **Device** page shows the following information:

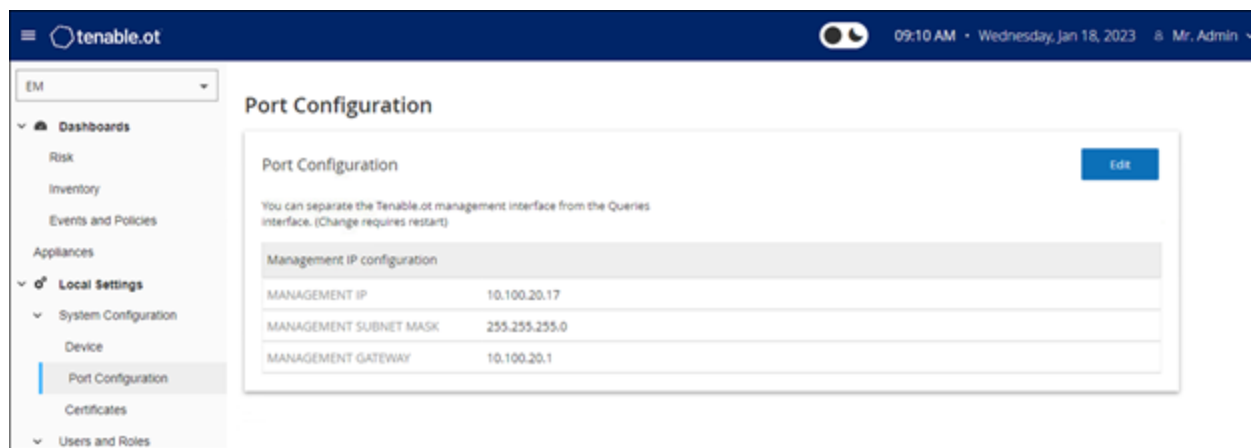
Parameter	Description
Device Name	The name of the OT Security management system.
Device URL	The URL used to access the OT Security EM console in a DNS environment.
System Time	The date and time in the system. You can use an NTP server to synchronize



	the system time with other assets in the network.
<b>Timezone</b>	The time zone of the system.
<b>DNS Servers</b>	You can enter the IPs of one or more DNS servers used in the network. This helps OT Security to identify DNS names of assets in the network.
<b>Automatic Logout</b>	The period of inactivity that causes the system to log out automatically.
<b>Ping Requests</b>	Set to detect whether or not the OT Security platform responds to ping requests.

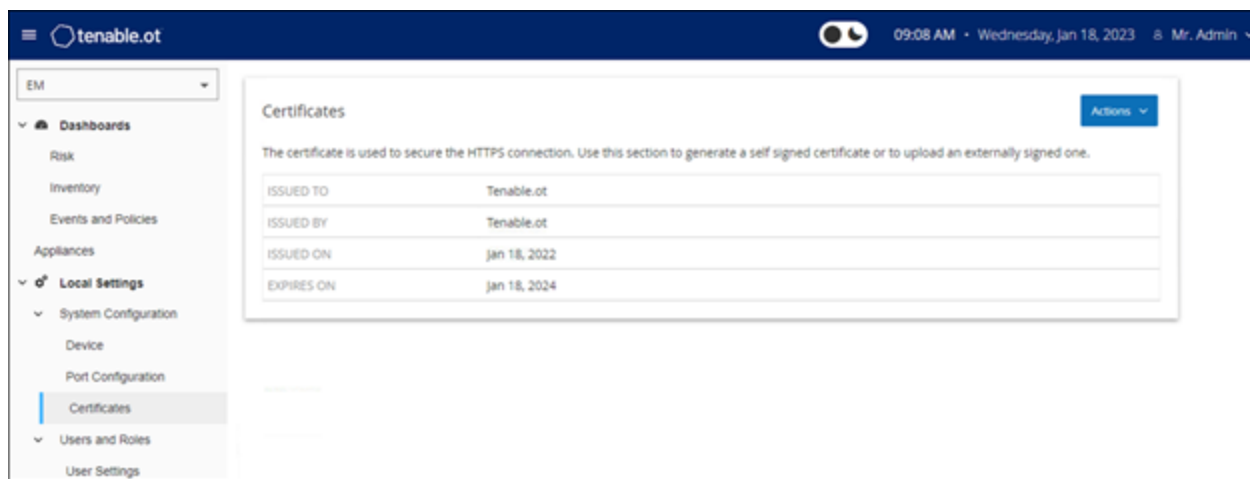
## Port Configuration

The **Port Configuration** page shows details of the configured ports on the device. For more information on Port Configuration, see [Port Configuration](#) in the Tenable OT Security User Guide.



## Certificates

On the **Certificate** page, you can view information about your HTTPS certificate and generate a new certificate for secure HTTPS connections for the OT Security EM. Generating a new certificate overrides the current certificate. A certificate is valid for one year.



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

Parameter	Description
<b>Issued to</b>	The entity to which the certificate was issued.
<b>Issued by</b>	The entity that issued the certificate.
<b>Issued on</b>	The issue date of the certificate.
<b>Expires on</b>	The date when the certificate ages out.



# OT Security EM License

Starting with OT Security version 3.16 or later, the OT Security EM requires a license. You can view the license status here: **Local settings > System configuration > License**.

tenable.ot

EM

Dashboards

Risk

Inventory

Events and Policies

Appliances

Local Settings

System Configuration

Device

Port Configuration

Certificates

License

Users Management

Integrations

Servers

System Actions

System Log

License

LICENSE TYPE	Perpetual
MAINTENANCE EXPIRES	Dec 29, 2993
LICENSE CODE	
COMPUTER ID	

Follow these steps in order to reinitialize your license

1

Enter license code

Enter license code

2

Generate activation certificate

Generate Certificate

3

Enter activation code, obtain an activation code from your sales rep. or from the [Self-service portal](#)

Enter Activation Code

Cancel



## Users Management

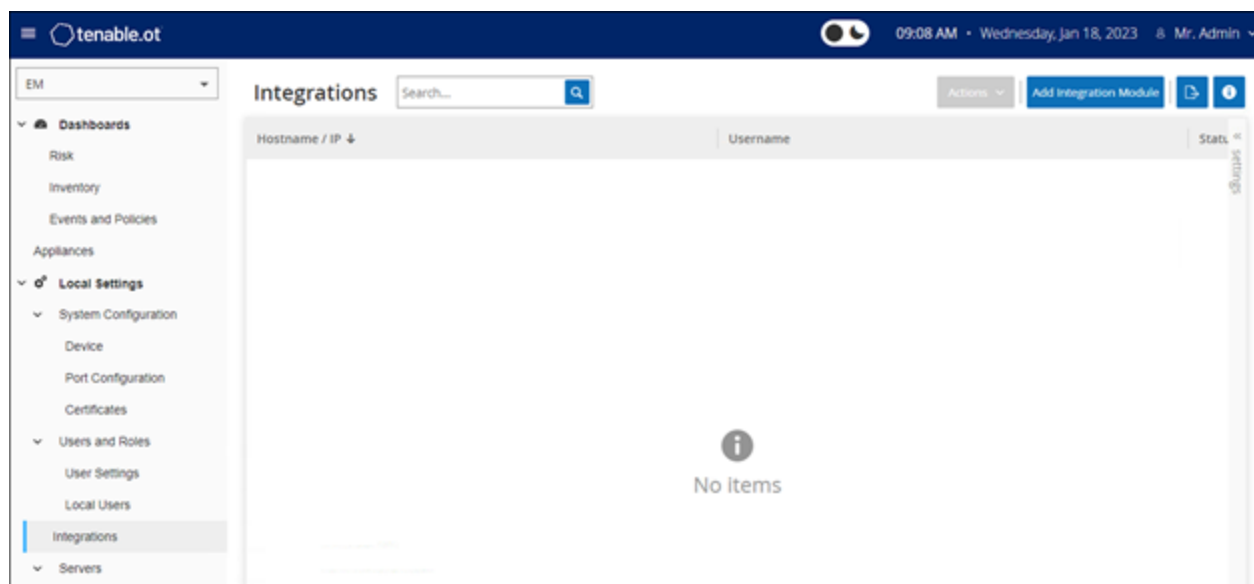
---

You can use the **Users Management** to view and configure users and user settings. These controls are split between two pages: **User Settings** and **Local Users**.



## Integrations

You can set up integrations for OT Security EM with other Tenable products – Tenable Security Center and Tenable Vulnerability Management. This enables OT Security to send data to Tenable Security Center and Tenable Vulnerability Management. The data from OT Security EM includes OT Security vulnerabilities as well as data discovered by IT-type Tenable Nessus scans initiated from OT Security. By setting up the integrations on the OT Security EM level, you provide a single source of data, and alleviate the need to configure separate integrations for each site.



**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.


### Integrate with Tenable Security Center

You can integrate Tenable Security Center with OT Security EM so that OT Security EM sends information to the designated repositories.

**Note:** Tenable recommends that you create Tenable Security Center repositories with matching names to OT Security Sites to optimize the mapping of Sites to repositories. The exact OT Security Site names must be contained within the Tenable Security Center repository names. For example, for a site named “London”, a repository name of “OT\_London” or “London – OT”. Sites without a matching repository send information





to the default repository that you designate during the integration setup. For detailed instructions, click the  button on the **Integrations** page.

To integrate Tenable Security Center:

1. Go to **Local Settings > Integrations**.
2. Click **Add Integration**.

The **Add Integration** wizard opens with the **Module Type** page.



3. Click **Tenable Security Center**, then click **Next**.

The **Module Definition** page appears.

**Add Integration Module** [X]

Module Type [✓]    Module Definition [●]

Tenable.sc

**i** Click the info button on the integration modules page for detailed instructions

**HOSTNAME / IP \***

**USERNAME \***

**PASSWORD \***

**DEFAULT REPOSITORY ID \***

**SYNC FREQUENCY \***  
Sync frequency is identical to all Tenable.sc integrations  
Every 6 hours

Test Connection

< Back    Cancel    Save

4. In the **Hostname\IP** box, type a hostname or an IP address of the Tenable Security Center system.
5. In the **Username** box, type the username associated with the Tenable Security Center system.
6. In the **Password** box, type the password associated with the Tenable Security Center system.
7. In the **Default Repository ID** box, type the ID for the repository that can serve as the default destination for any synced information that does not have a designated repository (see the [note](#)).
8. In the **Sync Frequency** box, set the sync frequency for the integration.
9. To test the connection, click **Test Connection**.
10. Click **Save**.



**Note:** Tenable recommends that you create a specific user on Tenable Security Center to integrate with OT Security EM. The user must have the **Security** role.

## Integrate with Tenable Vulnerability Management

You can integrate Tenable Vulnerability Management with OT Security EM after generating an API key in the Tenable Vulnerability Management console.

**Note:** 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 provide in the OT Security console when configuring the integration. For more information, see [Generate API Keys](#) in the Tenable Vulnerability Management User Guide.

To integrate Tenable Vulnerability Management:

1. Go to **Local Settings > Integrations**.
2. Click **Add Integration**.

The **Add Integration** wizard opens with the **Module Type** page.



The image shows a screenshot of the 'Add Integration Module' wizard. At the top, the title 'Add Integration Module' is followed by a close button (X). Below the title is a progress indicator with two steps: 'Module Type' (active, indicated by a blue dot) and 'Module Definition' (inactive, indicated by a grey dot). Under 'Module Type', there are two buttons: 'Tenable.sc' and 'Tenable.io'. The 'Tenable.io' button is highlighted with a blue border and background. At the bottom of the wizard, there are two buttons: 'Cancel' and 'Next >'. The 'Next >' button is highlighted with a blue background.

3. Click **Tenable Vulnerability Management**, then click **Next**.

The **Module Definition** page of the **Add Integration Module** wizard opens.

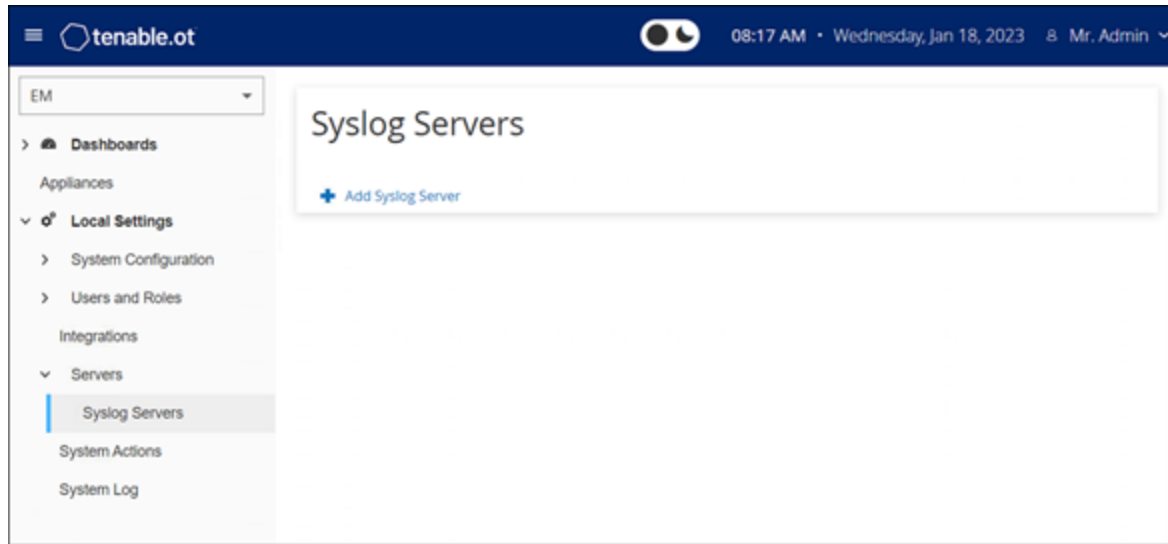


4. In the **Access Key** box, type the access key for the API.
5. In the **Secret Key** box, type the secret key for the API.
6. In the **Sync Frequency** box, set the sync frequency for the integration.
7. To test the connection, click **Test Connection**.
8. Click **Save**.



## Syslog Servers

To collect log events on an external server, you need to set up a Syslog server. If you do not want to set up a Syslog server, the event logs can only be saved on the OT Security EM platform.



To set up a Syslog server:

1. Go to **Local Settings > Servers > Syslog Servers**.
2. Click **+ Add Syslog Server**.

The **Syslog Servers** configuration window appears.

3. In the **Server Name** box, type the name of a Syslog server 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 that receives the events. (Default: 514)
6. In the **Transport** drop-down box, select the transport protocol you want to use. Options are **TCP** or **UDP**.
7. To send a test message to verify that the configuration is successful, click **Send Test Message**.

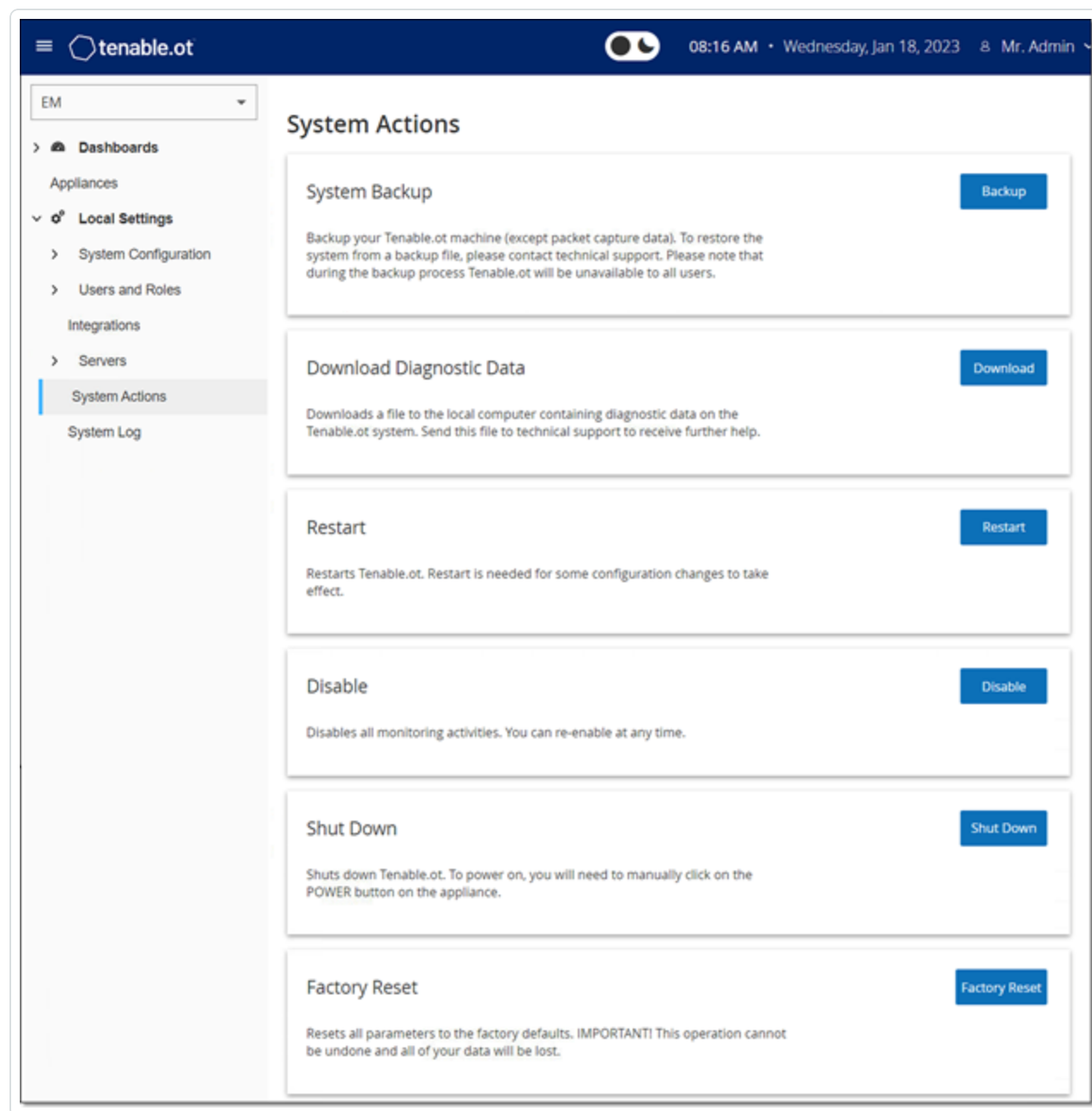
Verify if the message arrived. If the message did not arrive, then troubleshoot to discover the cause of the problem and rectify it.

8. Click **Save**.

You can set up additional Syslog servers by repeating this procedure.

# System Actions

The **System Actions** page shows a list of system activities that you can perform.



The **System Actions** page shows the following information:

Parameter	Description
<b>System Backup</b>	Back up your OT Security machine (except packet capture data). To restore the OT Security system from a backup file, contact Technical Support.



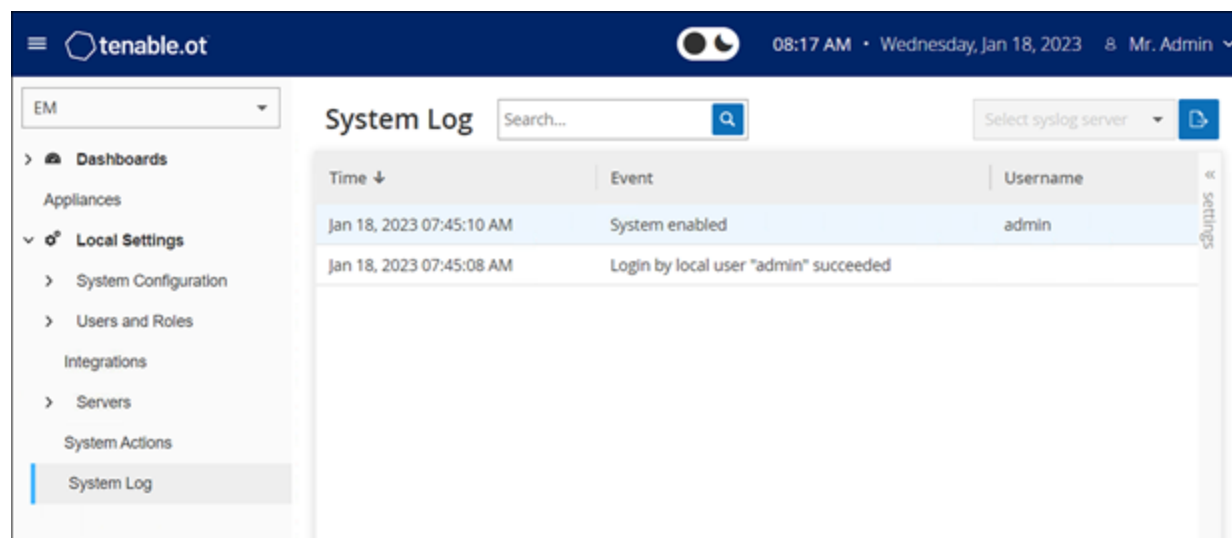


	<b>Note:</b> During the backup process, OT Security is unavailable to all users.
<b>Download Diagnostics Data</b>	Creates a file with diagnostic data on the OT Security system and stores it on the local computer. Send this file to Tenable Technical Support to receive further help.
<b>Restart</b>	Restarts the OT Security EM. This is needed for activation of certain configuration changes.
<b>Disable</b>	Disables all monitoring activities. You can reactivate the monitoring activities at any time.
<b>Shut Down</b>	Shuts down the OT Security EM. To power on, press the <b>Power</b> button on the OT Security EM.
<b>Factory Reset</b>	Returns all settings to the factory default settings. <b>Warning:</b> You cannot undo this operation and you lose all data in the system.



## System Log

The **System Log** page shows a list of all the system events that occurred in the system. For example, Policy turned on, Policy edited, Event Resolved and so on. 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 are shown on the **Events** page). 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.



The following information is available for each logged event:

Parameter	Description
<b>Time</b>	The time and date when the event occurred.
<b>Event</b>	A brief description of the event.
<b>Username</b>	The name of the user that initiated the event. For events that occur automatically, there is no username.



## Send System Log to a Syslog Server

To configure the system to send system events to a Syslog server:

1. Go to **Local Settings > System Log**.
2. In the header bar, click **Select syslog server**.

A drop-down list of servers appears.

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

3. Select the desired server.

OT Security EM sends the system log events to the specified Syslog server.



## Revision History

Product version: 3.16

Document revision history:

Document Revision	Date	Description
1.0	October 13, 2019	Created first version of User Guide for Version 3.1
1.1	June 23, 2020	Updated for version 3.6
1.2	July 27, 2021	Updated for version 3.11
1.3	June 28, 2022	Updated for version 3.13
1.4	January 31, 2023	Updated for version 3.15
1.5	July 25, 2023	Updated for version 3.16