Tenable OT Security Enterprise Manager 3.15 User Guide

Last Revised: November 07, 2023

Table of Contents

Introduction

OT Security (formerly Tenable.ot) Enterprise Manager (EM) 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 Enterprise Manager enables you to access the full functionality of all of your OT Security instances from a single application.

OT Security Functionality

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

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

OT Security has the following key features:

- **360-Degree Visibility** - Attacks can easily propagate in an IT/OT infrastructure. With a single platform to manage and measure cyber risk across your OT and IT systems, you have complete visibility into your converged attack surface. OT Security also natively integrates with leading IT security and operational tools, such as your Security Information and Event Management (SIEM) solution, log management tools, next-generation firewalls, and ticketing systems. Together, this builds an ecosystem of trust where all of your security products can work together as one to keep your environment secure.

- **Threat Detection and Mitigation** - OT Security leverages a multi-detection engine to find high-risk events and behaviors that can impact OT operations. These engines include policy, behavioral and signature-based detection.

- **Asset Inventory and Active Detection** - Leveraging groundbreaking patented technology, OT Security provides unparalleled visibility into your infrastructure—not only at the network level, but down to the device level. It uses native communication protocols to actively query both IT and OT devices in your ICS environment in order to identify all of the activities and actions occurring across your network.

- **Risk-Based Vulnerability Management** - Drawing on comprehensive and detailed IT and OT asset tracking capabilities, OT Security generates vulnerability and risk levels using Predictive Prioritization for each asset in your ICS network. These reports include risk-scoring and detailed insights, along with mitigation suggestions.
- **Configuration Control** – OT Security provides a full granular history of device configuration changes over time, including specific ladder logic segments, diagnostic buffers, tag tables and more. This enables administrators to establish a backup snapshot with the “last known good state” for faster recovery and compliance with industry regulations.

OT Security Technologies

The OT Security comprehensive solution comprises two core collection technologies:

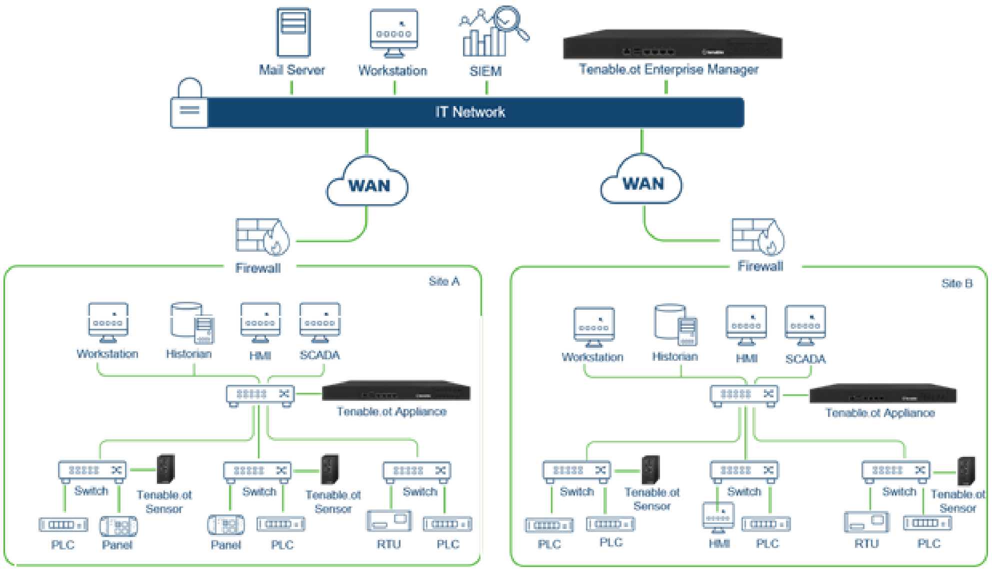
- **Network Detection** – OT Security network detection technology is a passive deep-packet inspection engine specifically designed to address the unique characteristics and requirements of industrial control systems. Network Detection provides in depth, real time visibility into all activities performed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

Solution Architecture

OT Security Components

The OT Security solution is comprised of two components:

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



Network Components

OT Security supports interaction with the following network components:

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

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

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

System Elements

Assets

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

Risk Assessment

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

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

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

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

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

Policies and Events

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

There are two types of policy events:

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

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

Policy-Based Detection

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

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

place between two assets that have never communicated before.

- **Anomalous or unauthorized changes to the asset inventory**: for example, a new asset was discovered or an asset stopped communicating in the network.
- **Anomalous or unauthorized changes in asset properties**: for example, the asset firmware or state has changed.
- **Abnormal writes of set-points**: Events are generated for changes made to specific parameters. The user can define the allowed ranges for a parameter and generate Events for deviations from that range.

Anomaly Detection

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

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

Policy Categories

The Policies are organized by the following categories:

- **Configuration Event Policies** – these Policies relate to the activities that take place in the network. There are two sub-categories of Configuration Event Policies:
  - **Controller Validation** - these Policies relate to changes that take place in the controllers in the network. This can involve changes in the state of a controller as well as changes

    to the firmware, asset properties or code blocks. The Policies can be limited to specific schedules (e.g. firmware upgrade during a work day), and/or specific controller/s.

  - **Controller Activities** – these policies relate to specific engineering commands that impact controllers' state and configuration. It is possible to define specific activities that always generate Events or to designate a set of criteria for generating Events. For example, if certain activities are performed at certain times and/or on certain controllers. Both black listing and white listing of assets, activities and schedules are supported.

- **Network Events Policies** – these Policies relate to the assets in the network and the communication streams between assets. This includes assets that were added to or removed from the network. It also includes traffic patterns that are anomalous for the network or that have been flagged as raising particular cause for concern. For example, if an engineering station communicates with a controller using a protocol that is not part of a pre-configured set of protocols (e.g. protocols that are used by controllers manufactured by a specific vendor), an Event is triggered. These policies can be limited to specific schedules and/or specific assets. Vendor specific protocols are organized by vendor for convenience, while any protocol can be used in a policy definition.

- **SCADA Event Policies** – these Policies detect changes in set-point values which can harm the industrial process. These changes may result from a cyber-attack or human error.

- **Network Threats Policies** – these Policies use signature-based OT and IT threat detection to identify network traffic that is indicative of intrusion threats. The detection is based on rules that have been catalogued in Suricata's Threats engine.

Groups

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

Events

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

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

OT Security Enterprise Manager Deployment

The OT Security Enterprise Manager can be deployed as an appliance installed onsite or on a Public or Private cloud server.

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

Specification	On Premise	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 90~264V	N/A	N/A
Cooling	CPU heatsink with fan duct 2 X cooling fans	N/A	N/A
Temperature	Operating: 0 ~40°C/32 ~104°F	N/A	N/A

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

Management Console UI Elements

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

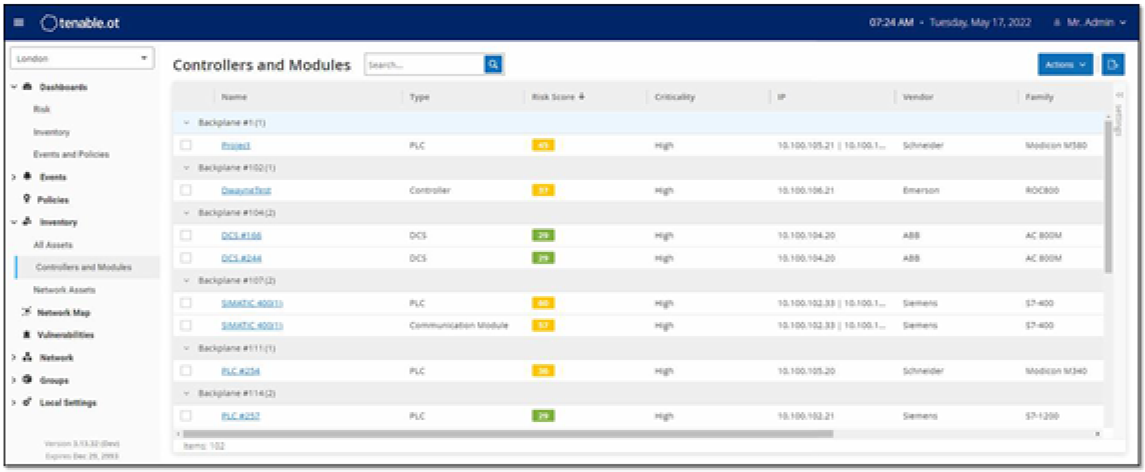
This chapter gives a brief overview of the UI elements. Details about specific UI functionality are provided in Using OT Security Enterprise Manager in Site Mode and Using OT Security Enterprise Manager in Enterprise Mode.

Site and Enterprise Modes

The OT Security Enterprise Manager UI has two different modes of operation, Site mode and Enterprise mode. Select the desired mode at the top of the Main Navigation pane.

Site Mode

In Site mode, the UI shows data for one particular site. In this mode, the OT Security Enterprise Manager user is logged in as an admin, 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 a complete explanation of the procedures for using the OT Security Enterprise Manager in Site mode see the Using OT Security Enterprise Manager in Site Mode.



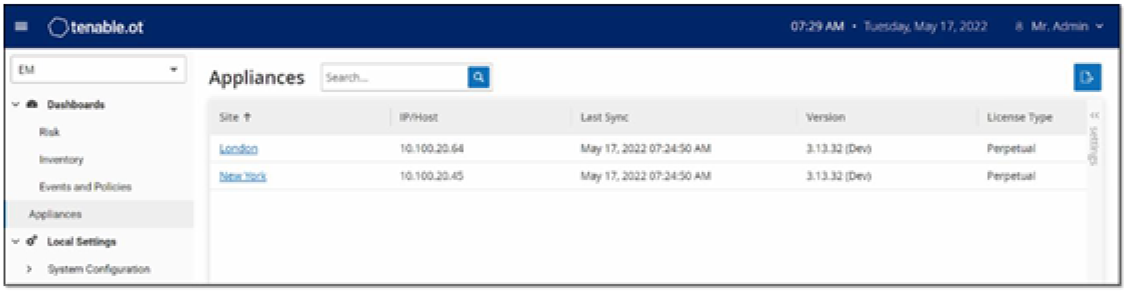
Controllers and Modules

	Name	Type	Risk Score	Criticality	IP	Vendor	Family
Backplane #1 (1)							
□	Project	PLC	45	High	10.100.105.21 | 10.100.1...	Schneider	Modicon M580
Backplane #102 (1)							
□	DwayneTest	Controller	37	High	10.100.106.21	Emerson	ROC800
Backplane #104 (2)							
□	DCS #166	DCS	29	High	10.100.104.20	ABB	AC 800M
□	DCS #244	DCS	29	High	10.100.104.20	ABB	AC 800M
Backplane #107 (2)							
□	SIMATIC 400(1)	PLC	60	High	10.100.102.33 | 10.100.1...	Siemens	S7-400
□	SIMATIC 400(1)	Communication Module	57	High	10.100.102.33 | 10.100.1...	Siemens	S7-400
Backplane #111 (1)							
□	PLC #254	PLC	38	High	10.100.105.20	Schneider	Modicon M340
Backplane #114 (2)							
□	PLC #252	PLC	29	High	10.100.102.21	Siemens	S7-1200

Items: 102

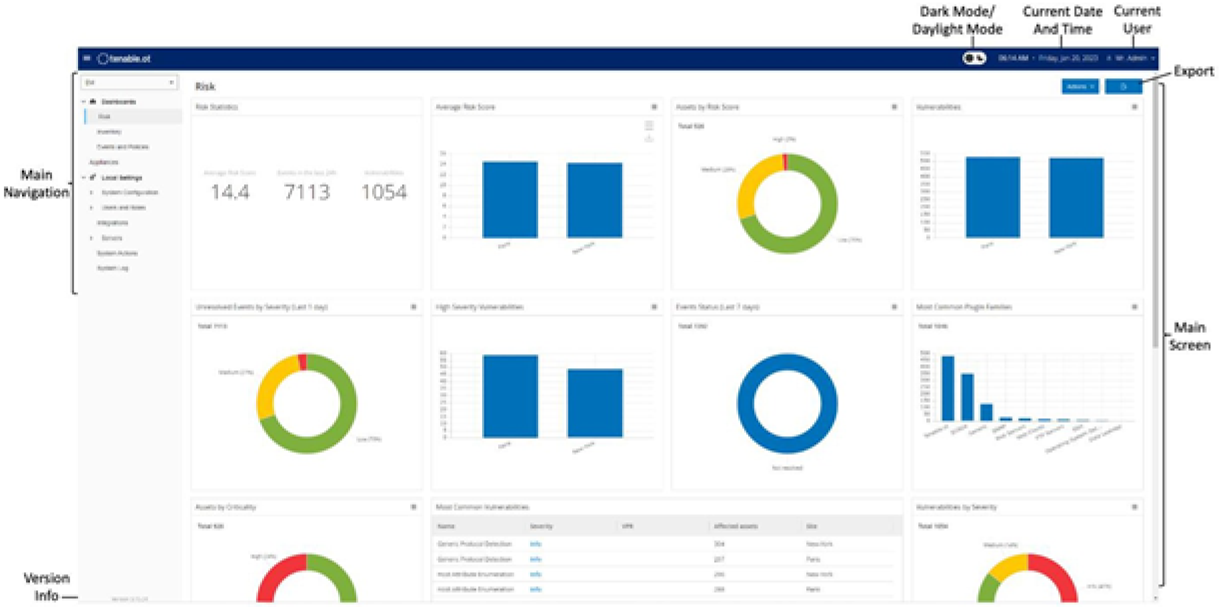
Enterprise Mode

In Enterprise mode, the UI shows information about each of your appliances. You can also view and adjust the local EM settings, including local user management. For an explanation of the data shown and the actions available in Enterprise mode see Using OT Security Enterprise Manager in Enterprise Mode.



Site	IP/Host	Last Sync	Version	License Type
London	10.100.20.64	May 17, 2022 07:24:50 AM	3.13.32 (Dev)	Perpetual
New York	10.100.20.45	May 17, 2022 07:24:50 AM	3.13.32 (Dev)	Perpetual

Main UI Elements



The following table describes the Main UI elements which are shown at all times.

UIElement	Description
Mode Selection	Select a mode: select "EM" for Enterprise mode or select a particular site for Site mode.
Main Navigation	Main navigation menu. Click on the ☰icon to show/hide the main navigation menu
Current Date and Time	Shows the current date and time as registered in the system.
Current User	Shows the name of the user who is currently logged into the system. Click on the down arrow for a selection menu. Menu options are About (shows software info) or Logout.
Version Info	Shows the software version OT Security Enterprise Manager.
Main Screen	Displays the screen that was selected in the Main Navigation.
Dark Mode/Daylight	Changes the display color scheme to Dark mode or Daylight mode.

Mode	
Export	Downloads a PDF of the dashboard.

Main Screens

The UI has several main screens that can be accessed from the **Main Navigation**. The following is a brief description of the various screens.

Enterprise Screens

When Enterprise mode (EM) is selected, 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 aggregated data from your Sites. There are separate dashboards for Risk, Inventory, and Events and Policies. See the Dashboards section.
- **Appliances** – displays info about each of the sites connected to the EM. See the Appliances Screen section.
- **Local Settings** – view and configure the EM settings, and view and generate a certificate for secure HTTPS connections for the EM. See the Local Settings section.
- **User Management** – view and configure users for the EM. See the Users and Roles section.
- **System** – displays system-level options (e.g. Factory Reset, Download Diagnostics Data, Restart, and Shut Down). See the Syslog Servers

Site Screens

When Site mode is selected, the following navigation options are available for the 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 Chapter Dashboards in the OT Security User Guide.
- **Events** – shows all Events that have occurred, as a result of Policy hits, in the system. There is a screen for viewing All Events as well as separate screens for viewing Events of each specific type (Configuration Events, SCADA Events, Network Threats or Network Events). See Chapter Events in the OT Security User Guide.

- **Policies** – view, edit and activate Policies in the system. See Chapter 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. There is a screen for viewing All assets as well as separate screens for viewing assets of specific types (Controllers and Modules, Network Assets and IoT). See Chapter Inventory in the OT Security User Guide.
- **Network Map** – shows a visual representation of the network assets and their connections throughout time.
- **Vulnerabilities** – shows a detailed list all the threats in the network detected by OT Security Plugins, and provides recommended remediation steps. This section includes CVEs as well as other threats to the assets in your network (e.g. obsolete operating systems, usage of vulnerable protocols, vulnerable open ports, etc.).
- **Network** – provides a comprehensive view of the network traffic by showing data about conversations that took place between assets in the network over time. See Chapter Network in the OT Security User Guide. The information is shown on three separate screens:
  - **Network Summary** - shows an overview of network traffic
  - **Packet Captures** - shows full-packet captures of network traffic
  - **Conversations** – shows a list of all conversations detected in the network, with details about the time that it occurred, involved assets etc.
- **Groups** – view, create and edit Groups, which are used in Policy configuration. See Chapter Groups in the OT Security User Guide.
- **Local Settings** – view and configure the system settings. See Chapter Local Settings in the OT Security User Guide.

Turning On/Off Dark Mode

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

To turn on/off Dark Mode:

1. Click the **Dark Mode** button at the top of the screen to turn on Dark Mode.

   The setting is applied to all screens and the **Daylight Mode** button is shown.

2. To restore the Daylight Mode setting, click the **Daylight Mode** button.

Exporting the Dashboard

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

To export the Dashboard:

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

   The PDF downloads automatically to the default download folder.

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

2. Navigate to the file that was just downloaded to view or share it.

Working with Lists

The various OT Security screens display the data relevant to that screen in table format with a record for each item. These tables have standardized customization features such as showing/hiding columns and filtering and sorting results.

For a full explanation of the methods of interacting with tables, see Working with Lists in the OT Security User Guide.

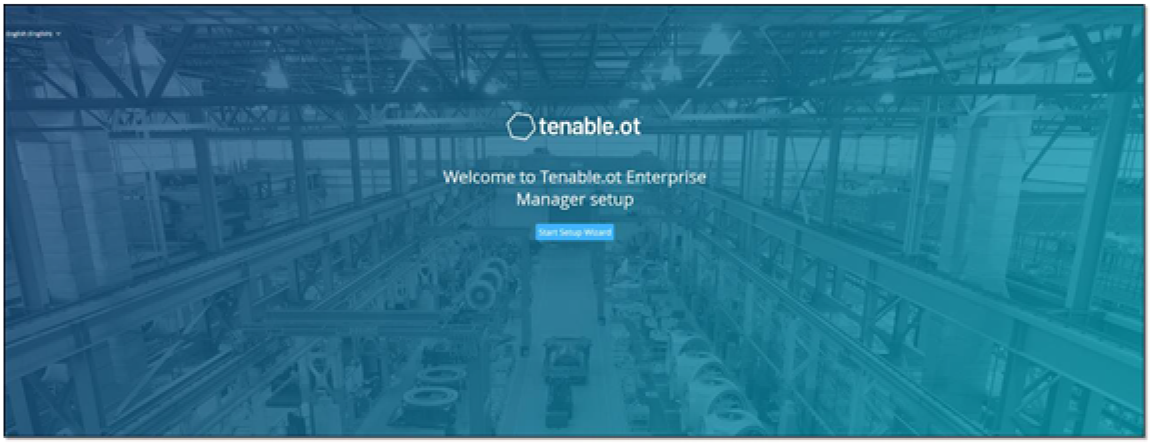
Setting Up OT Security Enterprise Manager

Initial setup of the OT Security Enterprise Manager involves two steps. First, run the Setup Wizard and fill in the relevant configuration info. Then, you will need to contact your Tenable support agent and ask them to connect each of your Sites to the Enterprise Manager.

To initiate the OT SecurityEnterprise Manager setup:

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

   The Welcome screen of the OT Security Enterprise Manager setup wizard opens.

   Welcome to Tenable.ot Enterprise Manager setup

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

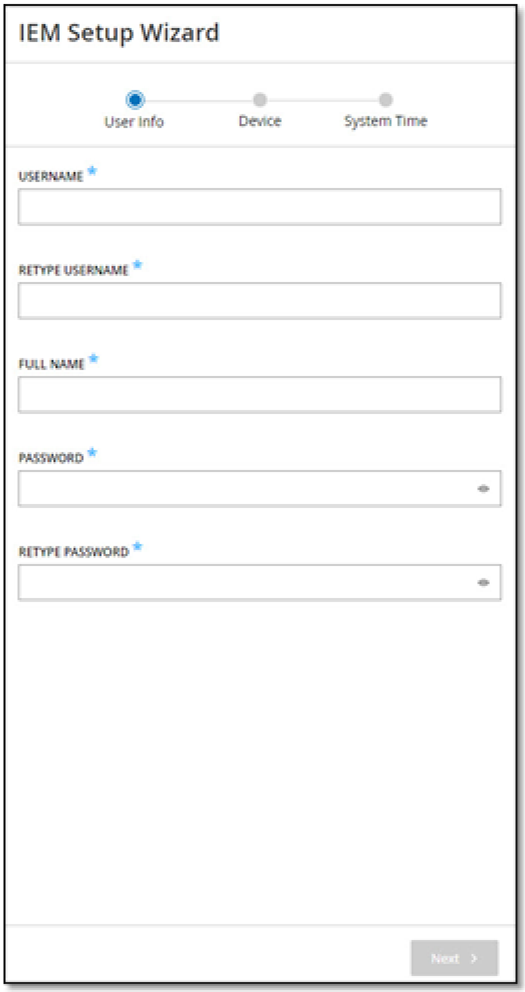
2. Click Start Setup Wizard.

   The setup wizard opens, showing the **User Info** page.

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

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

Screen 1 - User Info



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

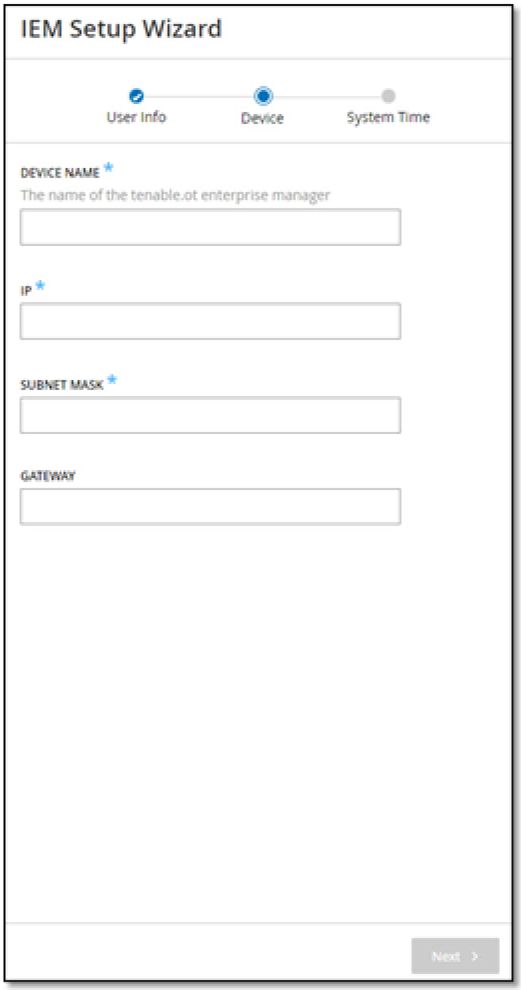
1. In the **Username** field, enter a username to be used for logging into the system. The username must include only lowercase letters and numbers.
2. In the **Retype Username** field, re-enter the identical username.
3. In the **Full Name** section, enter your complete first and last name.

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

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

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

Screen 2 – Device



IEM Setup Wizard

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

IP *

SUBNET MASK *

GATEWAY

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

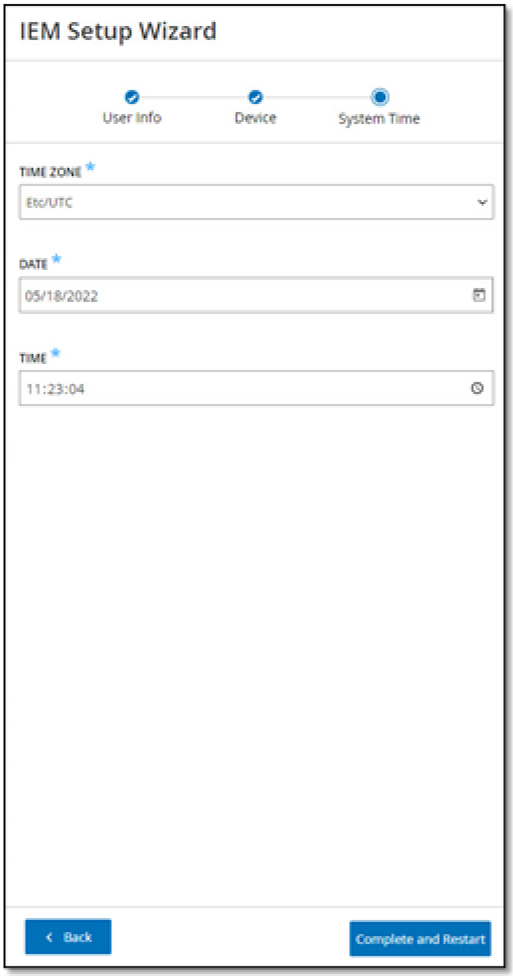
1. In the **Device Name** field, enter a unique identifier for the OT Security Enterprise Manager.
2. In the **IP** field, enter an IP address (within the network subnet) to be applied to the OT Security Enterprise Manager. This becomes the OT Security Enterprise Manager IP address.
3. In the **Subnet Mask** field, enter the subnet mask of the network.
4. If you would like to set up a Gateway (optional), enter the gateway IP for the network in the **Gateway** field.

Note: If you do not fill in this field then OT Security cannot communicate with external components outside of the subnet (e.g. email servers, syslog servers etc.).

5. Click **Next**.

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

Screen 3 – System Time



TIME ZONE *
Etc/UTC

DATE *
05/18/2022

TIME *
11:23:04

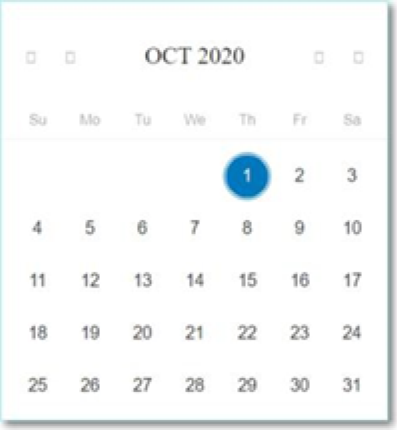
On the **System Time** page, the correct time and date are generally set automatically. If the correct date and time are not set, fill in the information using the following procedure.

> **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** field, select the local time zone at the site location from the dropdown list.
2. In the **Date** field, click the calendar icon 📅 .

   A pop-up calendar appears.



OCT 2020

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

3. Select the current date.

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

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

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

6. Once the restart is complete, you are redirected to the Login screen.

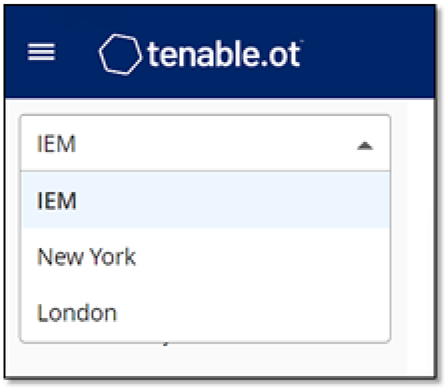
7. After completing the setup wizard, contact a Tenable support agent to have your Sites added to the Enterprise Manager.

Using OT Security Enterprise Manager in Site Mode

The functionality of the OT Security Enterprise Manager in Site mode is almost identical to the functionality of OT Security for that site. You have full admin capabilities except that you cannot create or manage users for that site. For a full explanation of how to use OT Security, see the *OT Security User Guide*.

To use the OT Security Enterprise Manager in Site Mode:

1. Login to the OT Security Enterprise Manager.
2. Click on the **Mode Selection** title to open a dropdown list of options.

3. Select the site that you would like to access.

   > **Note**: Alternatively, when viewing the **Appliances** screen in Enterprise Mode, click on the site you would like to access.

   The Main Navigation shows the screens available for the selected site.

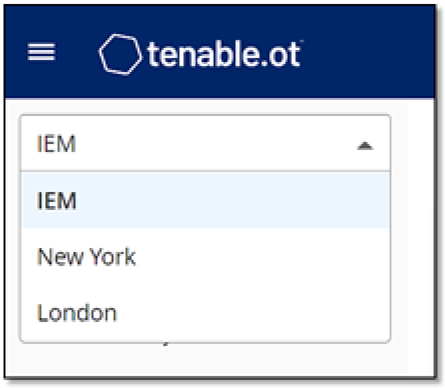
4. Select the desired screen and interact with OT Security in the same manner as you would when using the OT Security Management Console.

Using OT Security Enterprise Manager in Enterprise Mode

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

To use the OT Security Enterprise Manager in Enterprise Mode:

1. Login to the TOT Security Enterprise Manager.
2. Click on the **Mode Selection** title to open a dropdown list of options.

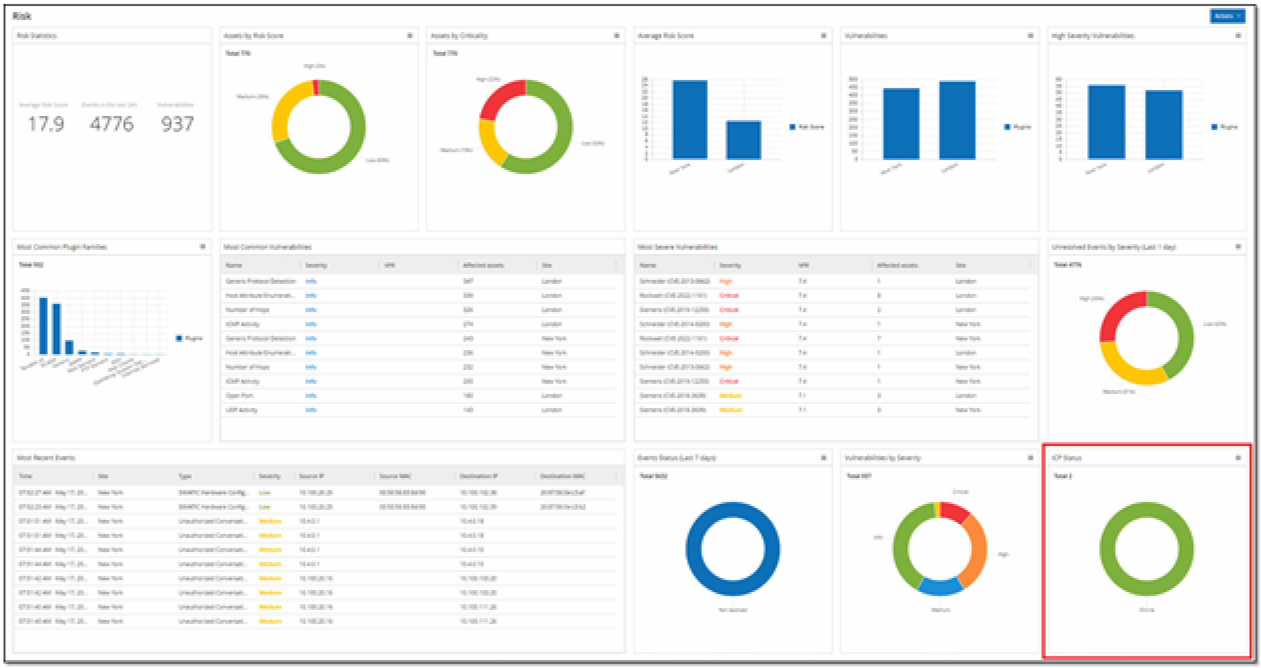


3. Select **EM**.

   The Main Navigation shows the screens available in Enterprise mode.

4. Select the desired screen.

Dashboards



The dashboards contain widgets that offer an at-a-glance view of aggregated information related to your whole enterprise's inventory and security posture based on information collected from all of your Sites. In addition to the standard widgets that are shown for individual Sites, the EM dashboards contain an ICP Status widget that displays the connectivity status of each of your Sites.

The following dashboards can be viewed:

- **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 etc.

- **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 etc.

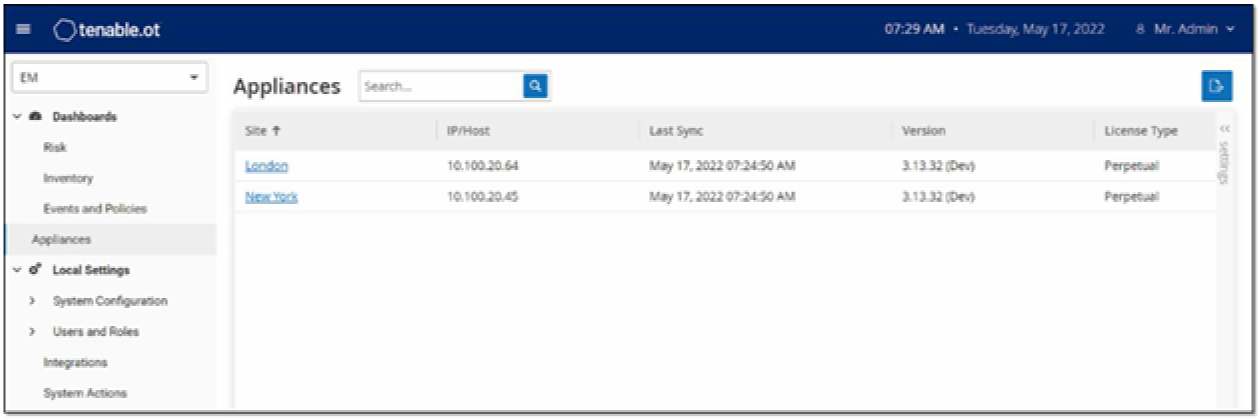
- **Events and Policies** - provides a means to detect threats to the enterprise by monitoring the identified events and the policies violations that they generate. The **Events and Policies** dashboard displays aggregated data in widgets such as: Events and Policies Statistics, Hourly Events Breakdown, High Severity Events, Events Status etc.

The Risk dashboard is the initial default view; however, you can change the default view to a different dashboard by clicking on 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 OT Security User Guide.

Appliances Screen

All of your appliances associated with the OT Security Enterprise Manager are listed on the **Appliances** screen. You can customize the display settings by adjusting which columns are displayed and where each column is positioned. You can download a CSV file with the appliance info by clicking on the **Export** button in the top right. You can also sort and filter the Appliances list as well as search for text in the Search box. For an explanation of the customization features, see the chapter on Working with Lists in the OT Security User Guide.



Site ↑	IP/Host	Last Sync	Version	License Type
London	10.100.20.64	May 17, 2022 07:24:50 AM	3.13.32 (Dev)	Perpetual
New York	10.100.20.45	May 17, 2022 07:24:50 AM	3.13.32 (Dev)	Perpetual

The following table describes the information shown on the **Appliances** screen.

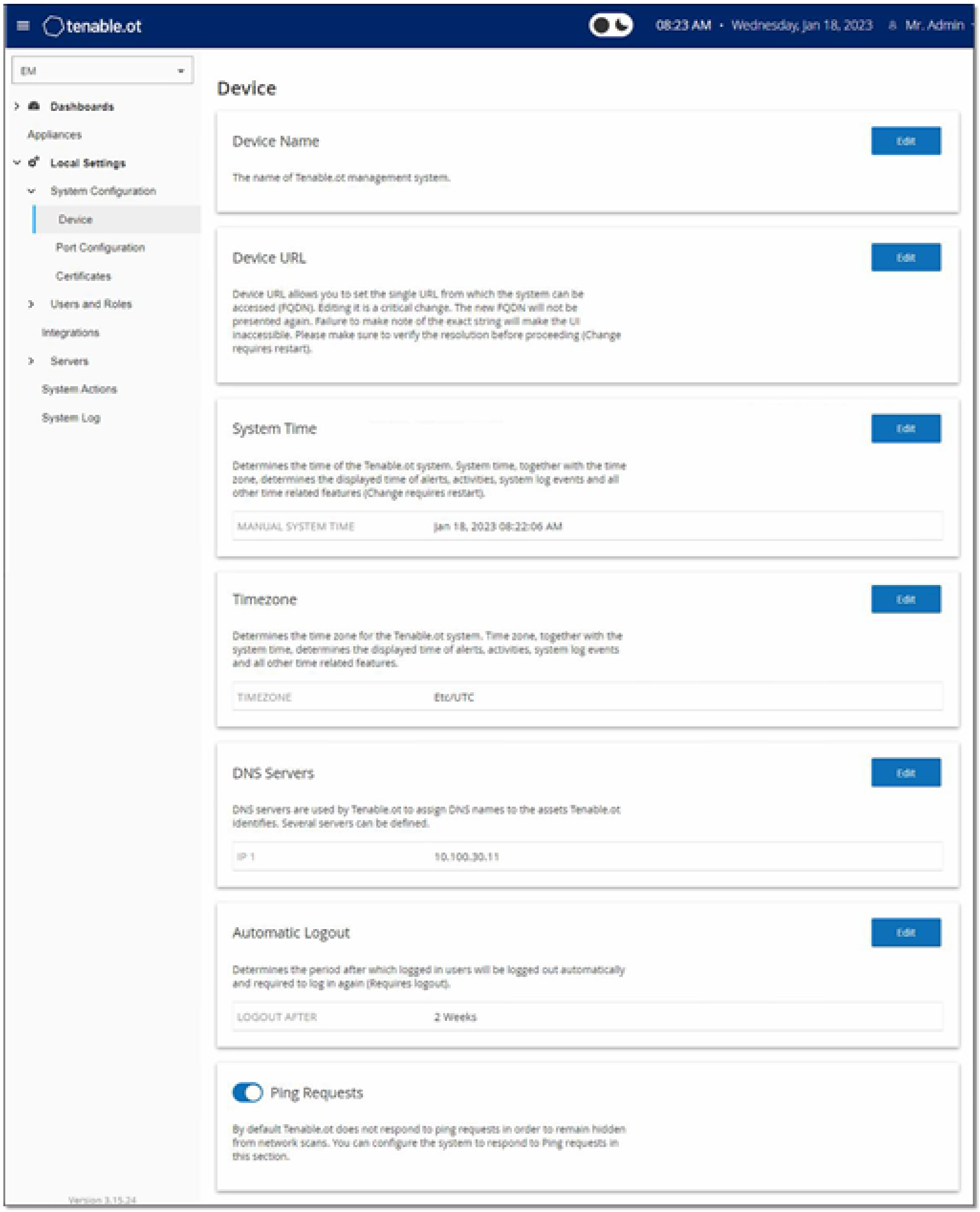
Parameter	Description
Site	The site where the OT Security instance is deployed. The site name is a link to open the EM in Site mode for that site.
IP/Host	The IP or Hostname of the OT Security instance.
Last Sync	The date and time that the site data was synchronized with the OT Security Enterprise Manager.
Version	The OT Security software version.
License Type	The license type associated with this appliance. Options are: subscription or perpetual.
License Expires	The date and time that the license expires.
Licensed	Options are:

Assets	- The number of assets that you are using out of the total number that you are licensed for, and the percentage of licenses used (e.g. 464/500 (93%)). - Unlimited.
Computer ID	The unique ID of the site computer.

Local Settings

The **Local Settings** section is where you can view and configure the EM settings. These controls are split between two screens: **Device** and **Certificate**. On the Device screen you can view and edit device details and network information (e.g. port configuration and system time, automatic logout (i.e. inactivity timeout)). On the Certificate screen you can view info about your HTTPS certificate and generate a new certificate for secure HTTPS connections for the EM.

Device Screen



Device

Device Name — Edit

The name of Tenable.ot management system.

Device URL — Edit

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).

System Time — Edit

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

Timezone — Edit

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

DNS Servers — Edit

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

Automatic Logout — Edit

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

Ping Requests

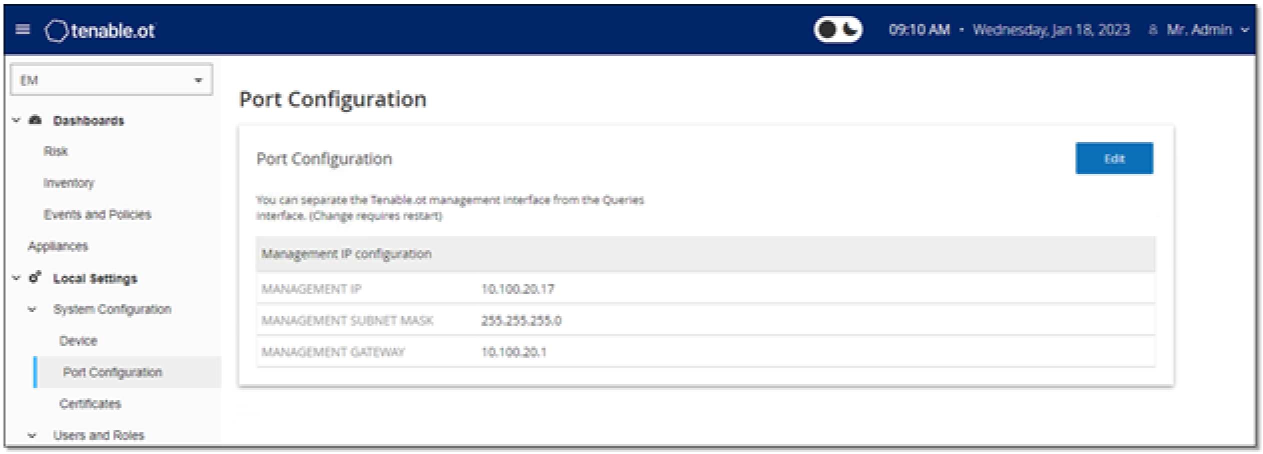
By default Tenable.ot does not respond to ping requests in order to remain hidden from network scans. You can configure the system to respond to Ping requests in this section.

The following table describes the information shown on the **Device** screen.

Parameter	Description
Device Name	The name of the OT Security management system.
Device URL	The URL used to access the OT SecurityEM 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.
Timezone	The time zone of the system.
DNS Servers	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.
Automatic Logout	The period of inactivity that causes the system to automatically log out.
Ping Requests	Set whether or not the OT Security platform responds to ping requests.

Port Configuration Screen



Port Configuration

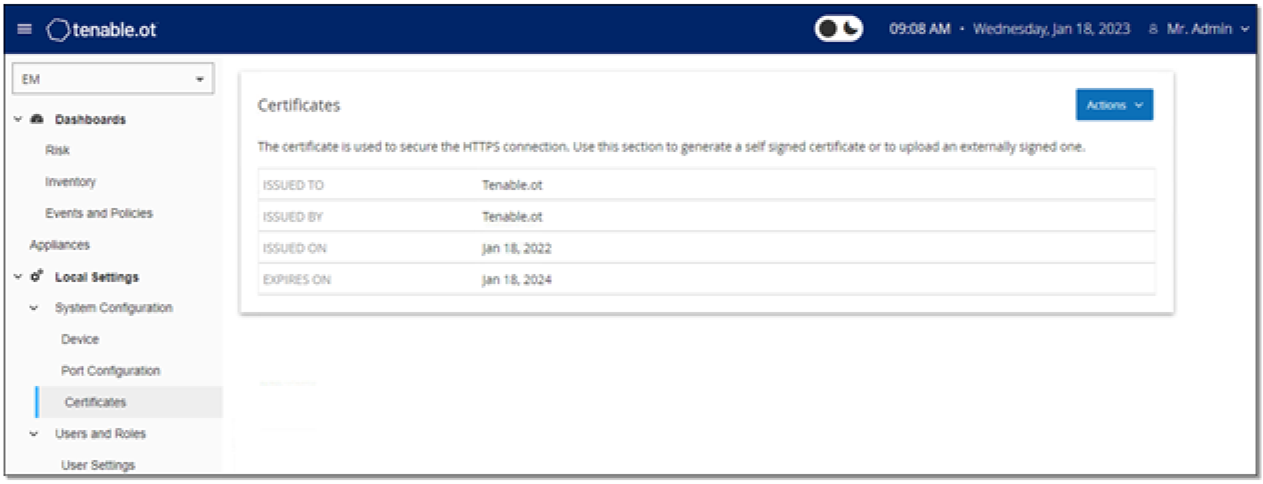
Port Configuration

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

Management IP configuration	
MANAGEMENT IP	10.100.20.17
MANAGEMENT SUBNET MASK	255.255.255.0
MANAGEMENT GATEWAY	10.100.20.1

The Port Configuration screen shows how the ports on the device are configured. For more information on Port Configuration, see Port Configuration in the OT Security User Guide.

Certificate Screen



Certificates

The certificate is used to secure the HTTPS connection. Use this section to generate a self signed certificate or to upload an externally signed one.

ISSUED TO	Tenable.ot
ISSUED BY	Tenable.ot
ISSUED ON	Jan 18, 2022
EXPIRES ON	Jan 18, 2024

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

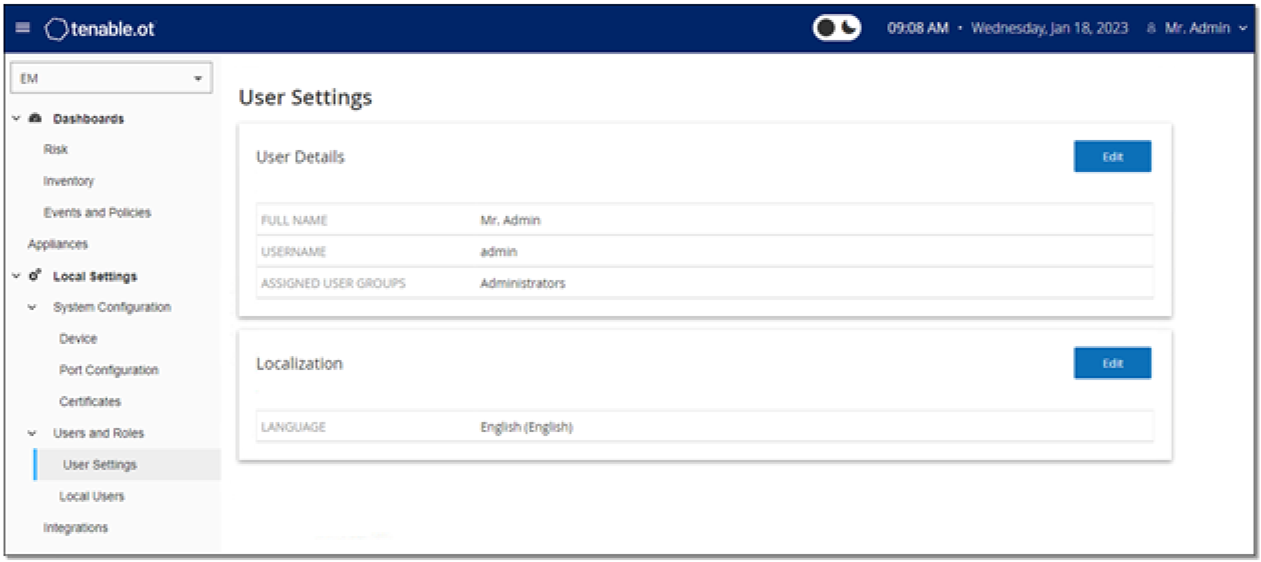
The following table describes the information shown on the **Certificate** screen.

Parameter	Description
Issued to	To what entity the certificate was issued.
Issued by	The entity that issued the certificate.
Issued on	The date the certificate was issued.
Expires on	The date the certificate expires.

Users and Roles

The **Users and Roles** section is where you can view and configure users and user settings. These controls are split between two screens: **User Settings** and **Local Users**. On the User Settings screen you can 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, or Chinese, French or German). On the Local Users screen an Admin user can create new user accounts, reset passwords and edit or delete existing accounts.

User Settings Screen



User Settings

User Details

FULL NAME	Mr. Admin
USERNAME	admin
ASSIGNED USER GROUPS	Administrators

Localization

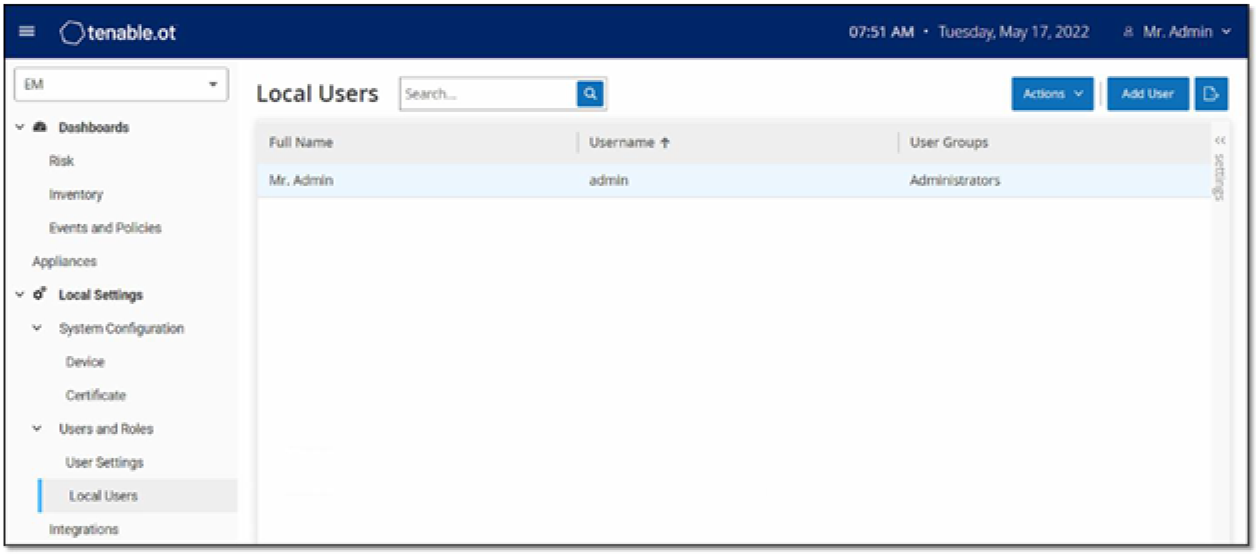
LANGUAGE	English (English)

On the **User Settings** screen you can 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).

The following table describes the information shown on the **User Settings** screen.

Parameter	Description
Full Name	The complete first and last name of the user.
Username	The username of the user.
Assigned User Groups	The User Groups assigned to the user.
Language	The language used in the User Interface (English, Japanese, or Chinese).

Local Users Screen



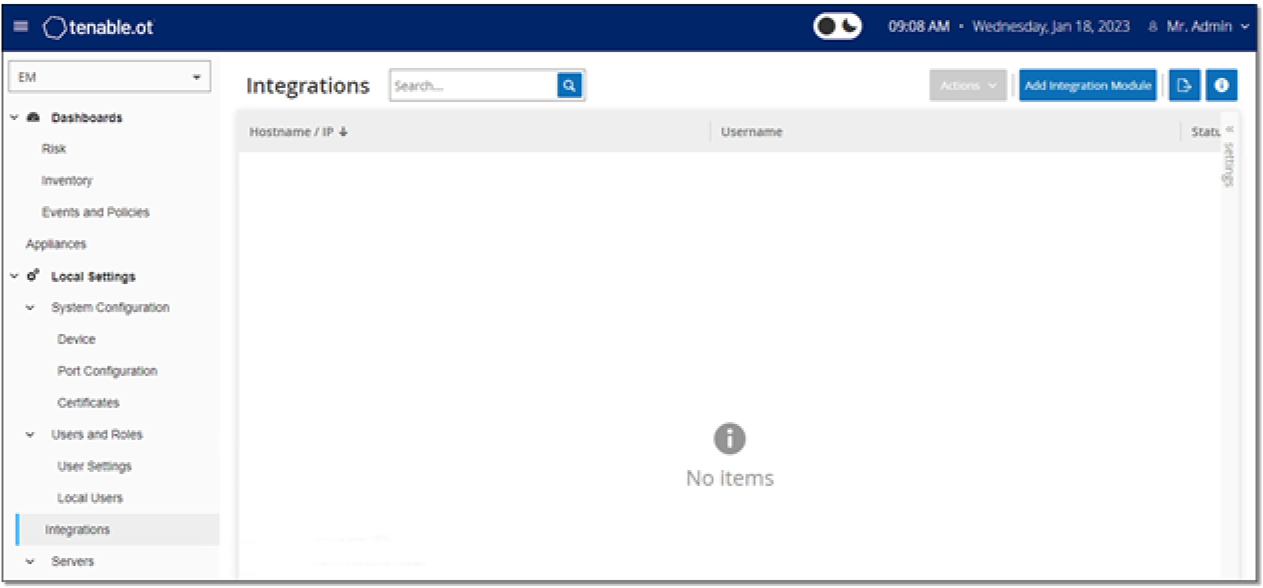
Full Name	Username ↑	User Groups
Mr. Admin	admin	Administrators

The **Local Users** screen lists all of the local users for the EM. You can add new users by clicking the **Add User** button. You can delete a user or change a user's password by clicking the **Actions** button. You can download a CSV file of the users by clicking the **Export** button. 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 users list as well as search for text in the Search box. For an explanation of the customization features, see the chapter on Working with Lists in the OT Security User Guide.

The following table describes the information shown on the **Local Users** screen.

Parameter	Description
Full Name	The complete first and last name of the user.
Username	The username of the user.
User Groups	The User Groups assigned to the user. The only option available to assign is Administrators.

Integrations



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

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

Integration with Tenable Security Center

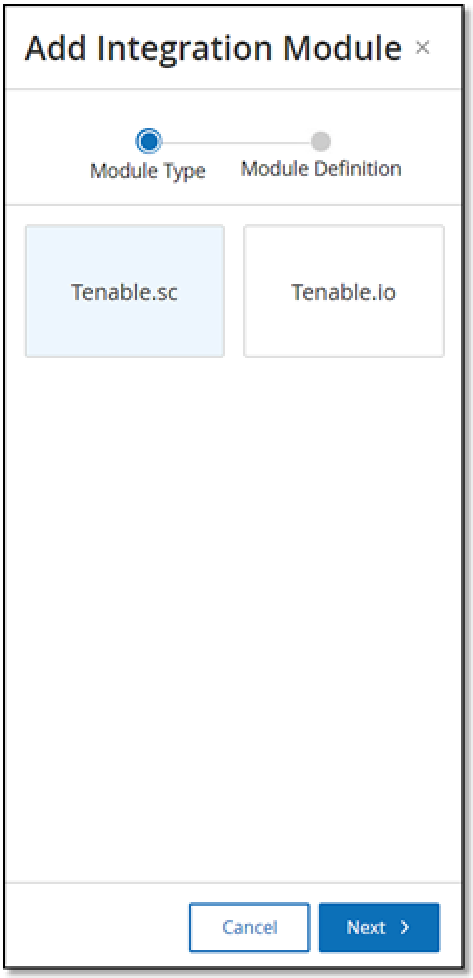
Tenable Security Center can be integrated with OT Security Enterprise Manager so that information from OT Security Enterprise Manager will be sent to designated repositories.

> **Note**: It is recommended to create Tenable Security Center repositories with matching names to OT Security Sites in order to optimize the mapping of Sites to repositories. The exact OT Security Site names should be contained within the Tenable Security Center repository names (e.g. for a site named “London”, a repository name of “OT_London” or “London – OT Security”). Sites without a matching repository will send information to the Default Repository that you designate during the integration setup. For detailed instructions, click on the info button on the Integrations screen.

To integrate Tenable Security Center:

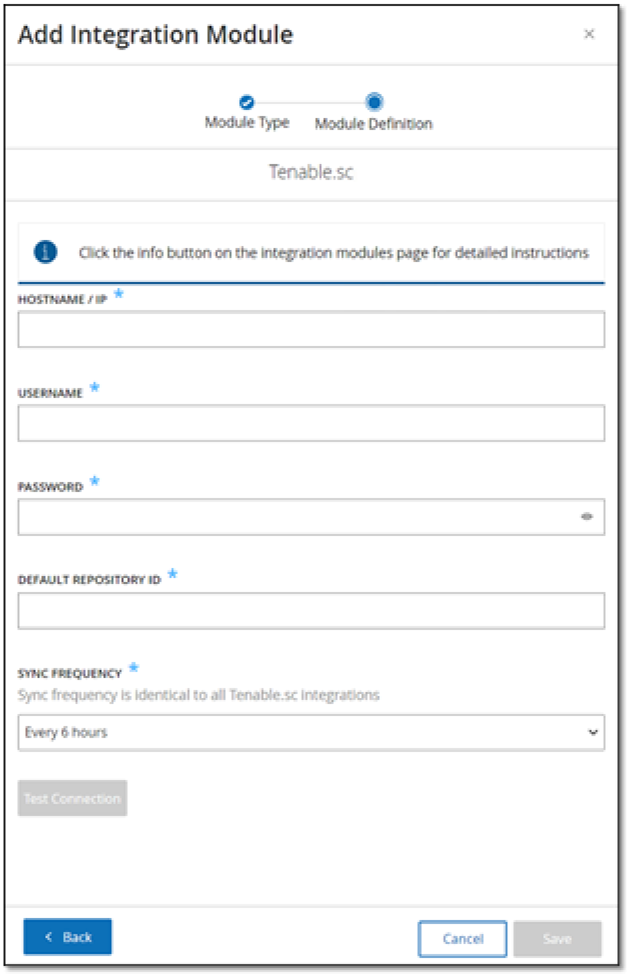
1. Under **Local Settings**, go to the **Integrations** screen.
2. Click on the **Add Integration** button.

   The **Add Integration** wizard opens, showing the **Module Type** page.



3. Click on the Tenable Security Center button and click **Next**.

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



Add Integration Module

Tenable.sc

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

SYNC FREQUENCY *

Sync frequency is identical to all Tenable.sc integrations

Every 6 hours

4. In the **Hostname\IP** field, enter a host name or an IP address of the Tenable Security Center system.

5. In the **Username** field, enter the username associated with the Tenable Security Center system.

6. In the **Password** field, enter the password associated with theTenable Security Center system.

7. In the **Default Repository ID** field, enter the ID for the repository that will serve as the default destination for any synced information that does not have a designated repository (see note above).

8. In the **Sync Frequency** field, set the sync frequency for the integration.

9. If you would like to test the connection, click **Test Connection**.

10. Click on the **Save** button.

Note: It is recommended to create a specific user onTenable Security Center that will be used to integrate with OT Security Enterprise Manager. The user should have the role of Security.

Integration with Tenable Vulnerability Management

Tenable Vulnerability Management can be easily integrated with OT Security Enterprise manager after generating an API key in the Tenable Vulnerability Management console.

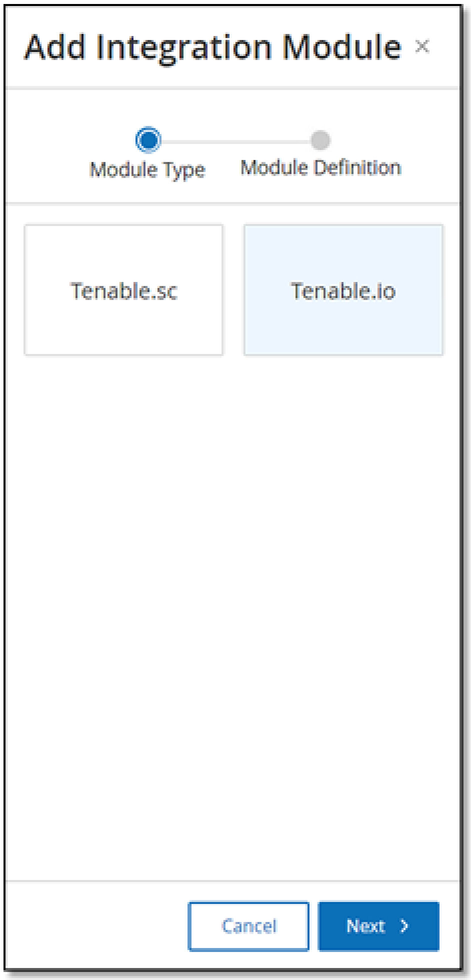
> **Note**: You need to first generate an API key in the Tenable Vulnerability Management console (Settings > My Account > API Keys > Generate). You will be given an Access Key and a Secret Key which you enter in the OT Security console when configuring the integration.

To integrate Tenable Vulnerability Management:

1. Under Local Settings, go to the **Integrations** screen.

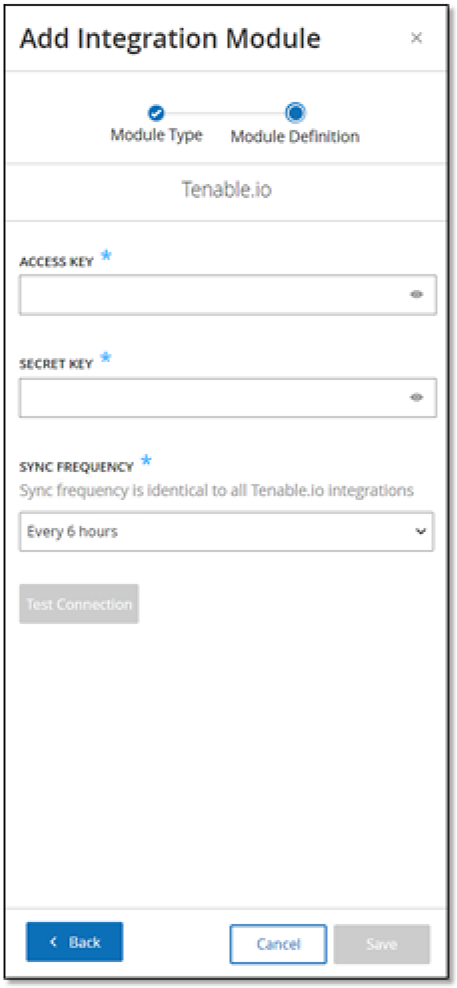
2. Click on the **Add Integration** button.

   The **Add Integration** wizard opens, showing the **Module Type** page.



3. Click on the Tenable Vulnerability Management button and click **Next**.

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



Add Integration Module

Tenable.io

ACCESS KEY *

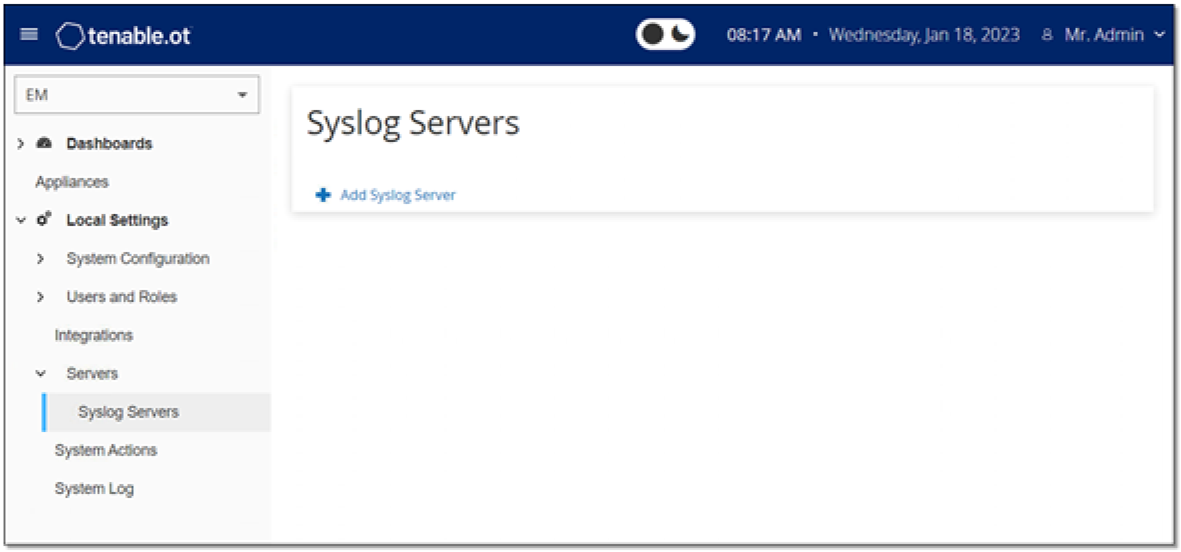
SECRET KEY *

SYNC FREQUENCY *
Sync frequency is identical to all Tenable.io integrations

Every 6 hours

4. In the **Access Key** field, enter the Access Key for the API.
5. In the **Secret Key** field, enter the Secret Key for the API.
6. In the **Sync Frequency** field, set the sync frequency for the integration.
7. If you would like to test the connection, click **Test Connection**.
8. Click on the **Save** button.

Syslog Servers

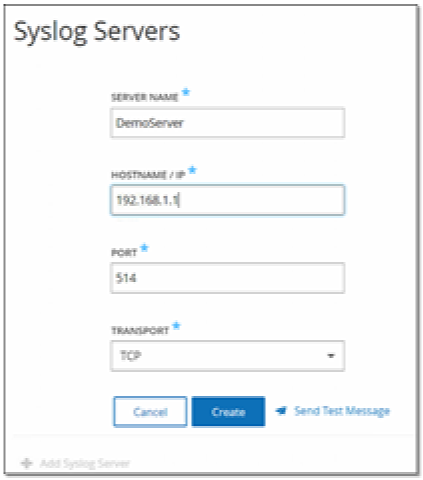


In order to enable collection of log events on an external server you will need to set up a Syslog Server in the system. If you do not want to set up a Syslog Server, then the event logs will only be saved on the OT Security EM platform.

To Set up a Syslog Server:

1. Under Local Settings, go to the **Servers** > **Syslog Servers** screen.
2. Click **+ Add Syslog Server**.

   The **Syslog Servers** configuration window is displayed.



Syslog Servers

SERVER NAME *: DemoServer

HOSTNAME / IP *: 192.168.1.1

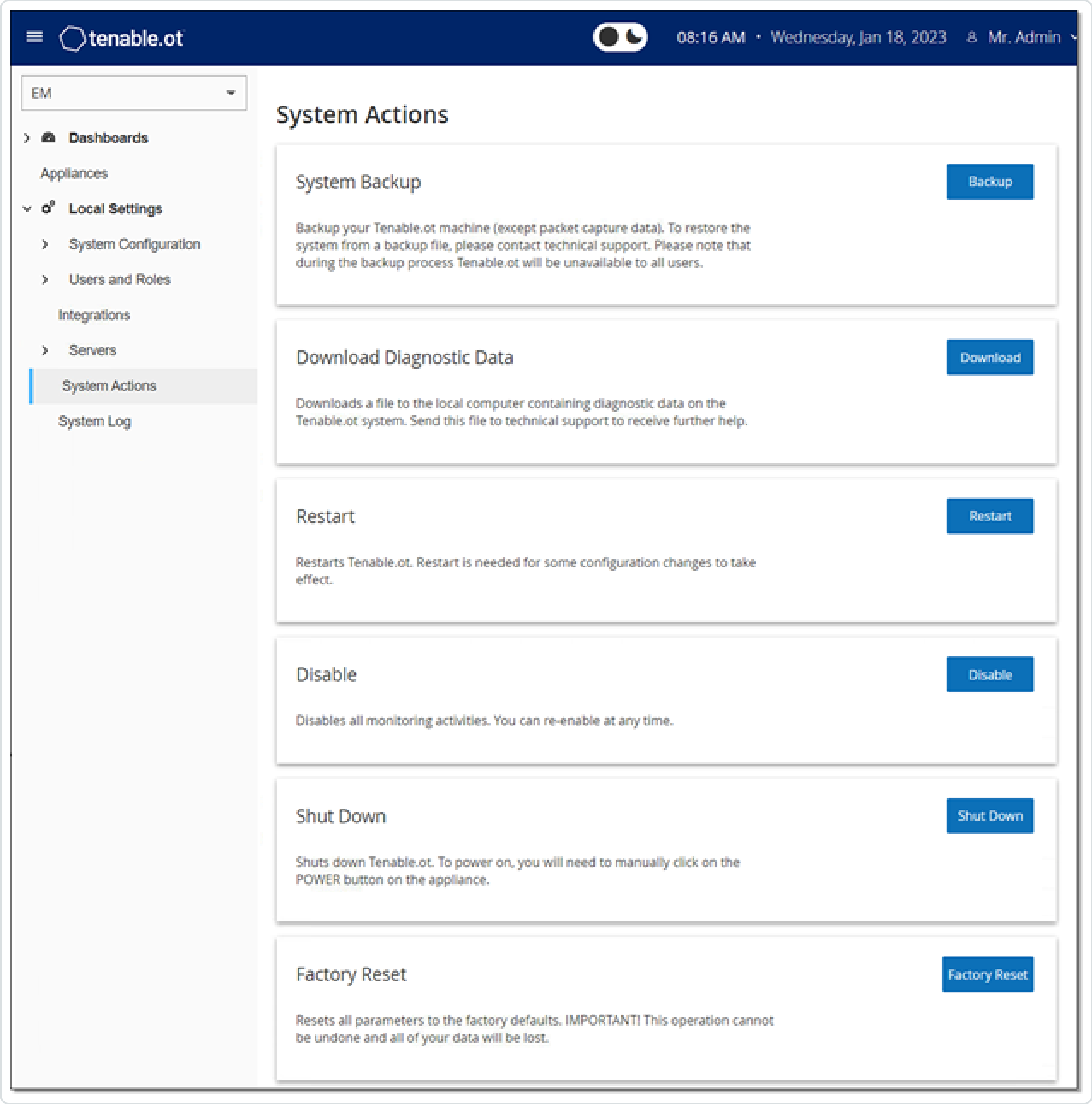
PORT *: 514

TRANSPORT *: TCP

3. In the **Server Name** field, enter the name of a Syslog Server to be used for logging system events.
4. In the **Hostname/IP** field, enter a host name or an IP address of the Syslog server.
5. In the **Port** field, enter the port number on the Syslog server to which the events will be sent. (Default: 514)
6. In the **Transport** field, select from the dropdown list the transport protocol to be used. Options are TCP or UDP.
7. If you would like to send a test message to verify that the configuration was successful, click **Send Test Message** and check if the message has arrived. If the message did not arrive, then troubleshoot to discover the cause of the problem and correct it.
8. Click **Save**.

   You can set up additional Syslog Servers by repeating the procedure described above.

System Actions



System Actions

System Backup

Backup your Tenable.ot machine (except packet capture data). To restore the system from a backup file, please contact technical support. Please note that during the backup process Tenable.ot will be unavailable to all users.

Download Diagnostic Data

Downloads a file to the local computer containing diagnostic data on the Tenable.ot system. Send this file to technical support to receive further help.

Restart

Restarts Tenable.ot. Restart is needed for some configuration changes to take effect.

Disable

Disables all monitoring activities. You can re-enable at any time.

Shut Down

Shuts down Tenable.ot. To power on, you will need to manually click on the POWER button on the appliance.

Factory Reset

Resets all parameters to the factory defaults. IMPORTANT! This operation cannot be undone and all of your data will be lost.

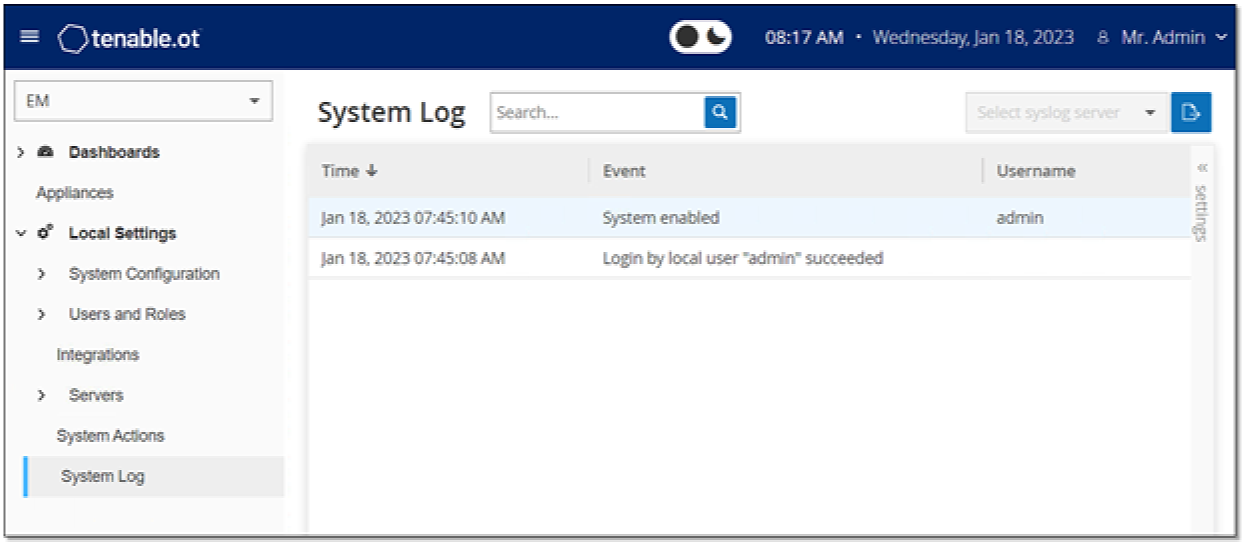
The **System** screen shows a menu of system activities.

The following table describes the information shown on the System screen.

Parameter	Description
System Backup	Backup your OT Security machine (except packet capture data). To restore

	the system from a backup file, please contact technical support. Please note that during the backup process OT Security will be unavailable to all users.
Download Diagnostics Data	Creates a file with diagnostic data on the OT Security system and stores it on the local computer. Send this file to technical support to receive further help.
Restart	Restarts the OT Security EM. This is needed for activation of certain configuration changes.
Disable	Disables all monitoring activities. You can reactivate the monitoring activities at any time.
Shut Down	Shuts down the OT Security EM. To power on, press the Power button on the OT Security EM.
Factory Reset	Returns all setting to the factory default settings. **Warning**: this operation can’t be undone and all data in the system will be lost.

System Log



Time	Event	Username
Jan 18, 2023 07:45:10 AM	System enabled	admin
Jan 18, 2023 07:45:08 AM	Login by local user "admin" succeeded	

The **System Log** screen shows a list of all system events (e.g. Policy turned on, Policy edited, Event Resolved etc.) that occurred in the system. This log includes both user-initiated events as well as automatically occurring system events (e.g. Policy turned off automatically because of too many hits). This log does **not** include Policy generated Events (which are shown on the Events screen). The logs can be exported as a CSV file. You can also configure the system to send the System Log events to a Syslog server.

The information shown for each logged event is described in the following table:

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

Sending System Log to a Syslog Server

To configure the system to send System Events to a Syslog server:

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

   A dropdown list of servers is displayed.

   > **Note**: To add a Syslog server, seeSyslog Servers.

3. Select the desired server.

   The System Log events will be sent to the specified Syslog server.

Revision History

Product version: 3.15

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