



Tenable OT Security 4.0 Enterprise Manager User Guide

Last Revised: December 19, 2024



Table of Contents

Tenable OT Security 4.0 Enterprise Manager User Guide	1
Welcome to Tenable OT Security Enterprise Manager	4
OT Security Technologies	5
Solution Architecture	6
OT Security Components	6
Network Components	7
System Elements	8
Assets	8
Policies and Events	9
Policy-Based Detection	9
Anomaly Detection	10
Policy Categories	10
Groups	11
Events	12
Deployment Specifications	13
Set Up OT Security EM	14
OT Security EM License Workflow	20
OT Security EM Management Console Elements	32
Main User Interface Elements	32
Other Actions	34
Customize Tables	34
OT Security EM Overview	36
Most Recent Events	38



ICPs	40
Pair ICP with Enterprise Manager	46
Disconnect ICP Pairing with Enterprise Manager	49
Local Settings	50
OT Security EM License	53
Users Management	53
User Settings	54
Local Users	55
User Groups	60
Authentication Servers	62
SAML	65
Integrations	69
Syslog Servers	74
System Actions	76
System Log	77
Send System Log to a Syslog Server	78
API Keys	78
Certificates	79
Revision History	82



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

OT Security offers comprehensive security tools and reports for IT security personnel and OT engineers. It provides visibility into converged IT/OT segments and ICS activity, and makes you aware of situations across all sites and their respective OT assets—from Windows Servers to PLC backplanes—in a single pane of glass.

OT Security has the following key features:

- **360-Degree Visibility** – Attacks can easily propagate in an IT/OT infrastructure. With a single platform to manage and measure cyber risk across your OT and IT systems, you have complete visibility into your converged attack surface. OT Security also natively integrates with IT security and operational tools, such as your Security Information and Event Management (SIEM) solution, log management tools, next-generation firewalls, and ticketing systems. Together, this builds an ecosystem where all of your security products can work together as one to keep your environment secure.
- **Threat Detection and Mitigation** – OT Security leverages a multi-detection engine to find high-risk events and behaviors that can impact OT operations. These engines include policy, behavioral and signature-based detection.
- **Asset Inventory and Active Detection** – Leveraging patented technology, OT Security provides visibility into your infrastructure—not only at the network level, but down to the device level. It uses native communication protocols to query both IT and OT devices in your ICS environment in order to identify all of the activities and actions occurring across your network.



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

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

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

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

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

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

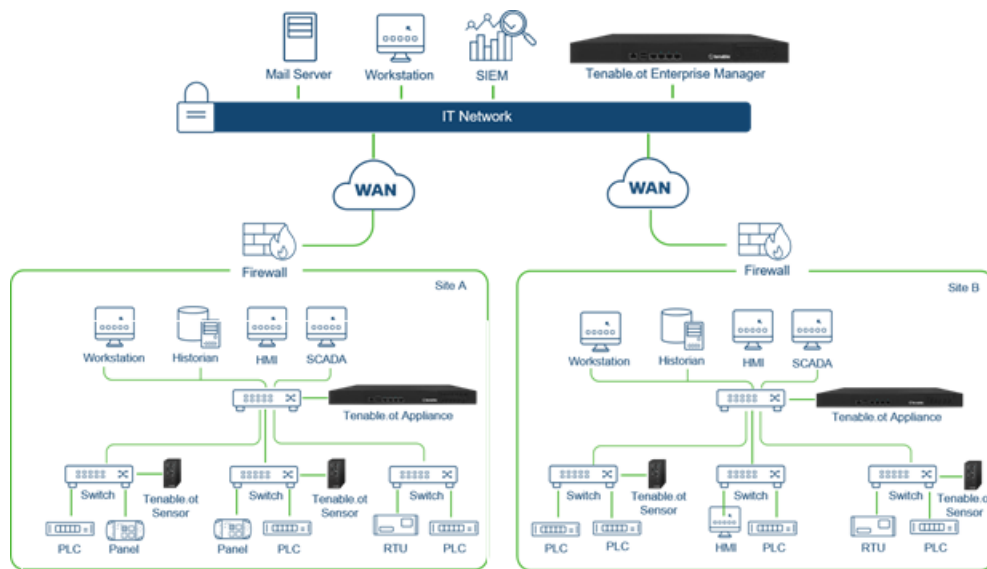
The OT Security solution is composed of these components:

- **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.
- **ICP (OT Security Appliance)**– This component collects and analyzes the network traffic directly from the network (via a span port or network tap) and/or using a data feed from the



Tenable OT Security Sensor (OT Security Sensor). The ICP appliance executes both the Network Detection and Active Query functions.

- **OT Security Sensors** – These are small devices deployed on network segments that are of interest, up to one sensor per managed switch. OT Security sensors provide full visibility into these network segments by capturing all the traffic, compressing the data and then communicating the information to the OT Security appliance. You can configure Sensors version 3.14 and later to send out active queries to the network segments on which they are deployed.



Network Components

OT Security supports interaction with the following network components:

- **OT Security user (management)** – You can create user accounts to control access to the OT Security Management Console. You can access the Management Console through a browser (Google Chrome) via a secure socket-layer authentication (HTTPS).

Note: You can only access OT Security user interface from the latest version of Chrome.

- **SIEM**– Send OT Security Event logs to a SIEM using Syslog protocol.
- **SMTP Server** – OT Security sends event notifications by email to specific groups of employees via an SMTP server.



- **DNS Server** – Integrate DNS servers into OT Security to help in resolving asset names.
- **Third-party applications** – External applications can interact with OT Security using its REST API or access data using other specific integrations¹.

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

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 OT Security EM specifications are the same as that for a t3.xlarge instance:

- CPU: 4
- Memory: 16 GB
- Disk: 205 GB



Set Up OT Security EM

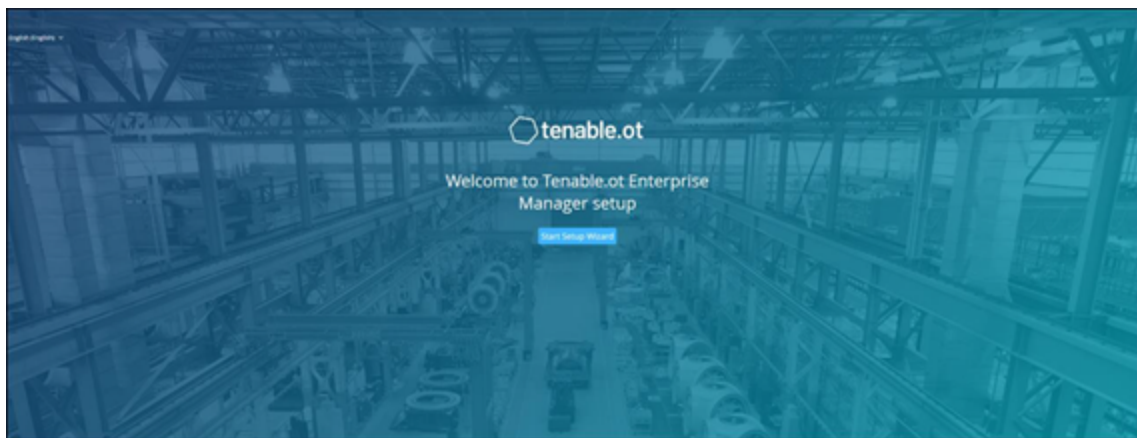
The Initial setup of OT Security EM involves two steps:

1. Run the Setup Wizard and provide relevant configuration information.
2. [Pair ICP with OT Security EM.](#)

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.

IEM Setup Wizard

User Info Device System Time

USERNAME *

RETYPE USERNAME *

FULL NAME *

PASSWORD *

RETYPE PASSWORD *

Next >

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

User Info Device System Time

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.

IEM Setup Wizard

User Info Device System Time

TIME ZONE *
Etc/UTC

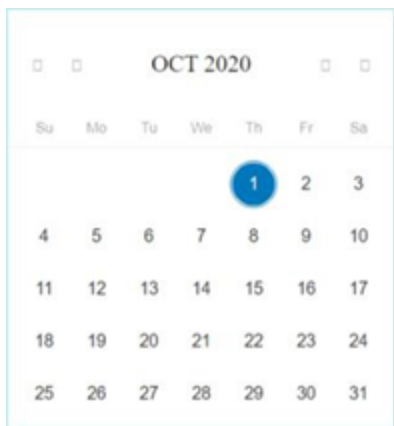
DATE *
05/18/2022

TIME *
11:23:04

< Back 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 License Workflow

Licenses for Tenable accounts are calculated based on the number of unique IPs in the system. Each IP requires a separate license. For example, even if more than one device shares the same IP address, multiple devices connected to the same backplane that share the same three IPs, the licenses can still be based on the number of IPs. In this case, you need three licenses, regardless of the number of devices.

After you install OT Security EM, the next step is to activate your license.

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

Before you Begin

- [Install the OT Security EM Appliance.](#)
- Make sure that you have the license code (20 characters letter/numbers), which you received from Tenable when you ordered your device.
- Make sure you have access to the internet. If your OT Security EM device is not connected to the Internet, you can register the license from any PC.
- Make sure you have access to the [Tenable Provisioning](#) portal. For access, contact your Tenable Customer Success Manager.

Activate your OT Security license

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

To activate your OT Security EM license:

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

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

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

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



3. From the **Code** column, copy the 20-digit OT Security license code.
4. Generate activation certificate in OT Security EM:
 - a. Go to the OT Security EM **License Activation** page.
 - b. In step 1, click **Enter new license code**.

The **Enter new license code** panel appears on the right.
 - c. In the **License code** box, paste the code that you copied from the provisioning portal.
 - d. Click **Verify**.

OT Security EM enables the **Generate activation certificate** section.
 - e. Click **Generate Certificate**.

The **Generate Certificate** panel appears on the right.
 - f. Click **Copy text to clipboard**, then click **Done**.

OT Security EM generates the certificate, which you must provide in the Tenable Provisioning Portal to add your sites.
5. In step **3 Enter activation code**, click the **Self-service** link to open the [Tenable Provisioning](#) portal.

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

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

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

- a. (Optional) In the **Label** box, type a name for the site.
- b. In the **Activation Certificate** box, paste the certificate that you copied from OT Security EM. See [step f](#).
- c. Click **Create**.

A dialog box appears with an activation code. This is a one-time generated code that



you must copy to the OT Security instance.

d. Click the  button, then click **Confirm**.

7. Navigate back to the OT Security EM instance and in the step **3 Enter activation code** section, click **Enter Activation Code**.

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

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

9. Click **Activate**.

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

10. Click **Enable**.

OT Security EM is now enabled and ready to use.

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

12. Click **Confirm**.

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

Update your license

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

Before you Begin

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

To update your license:



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

The **License** window appears.

License Actions ▾

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

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

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

License

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

Follow these steps in order to update your license

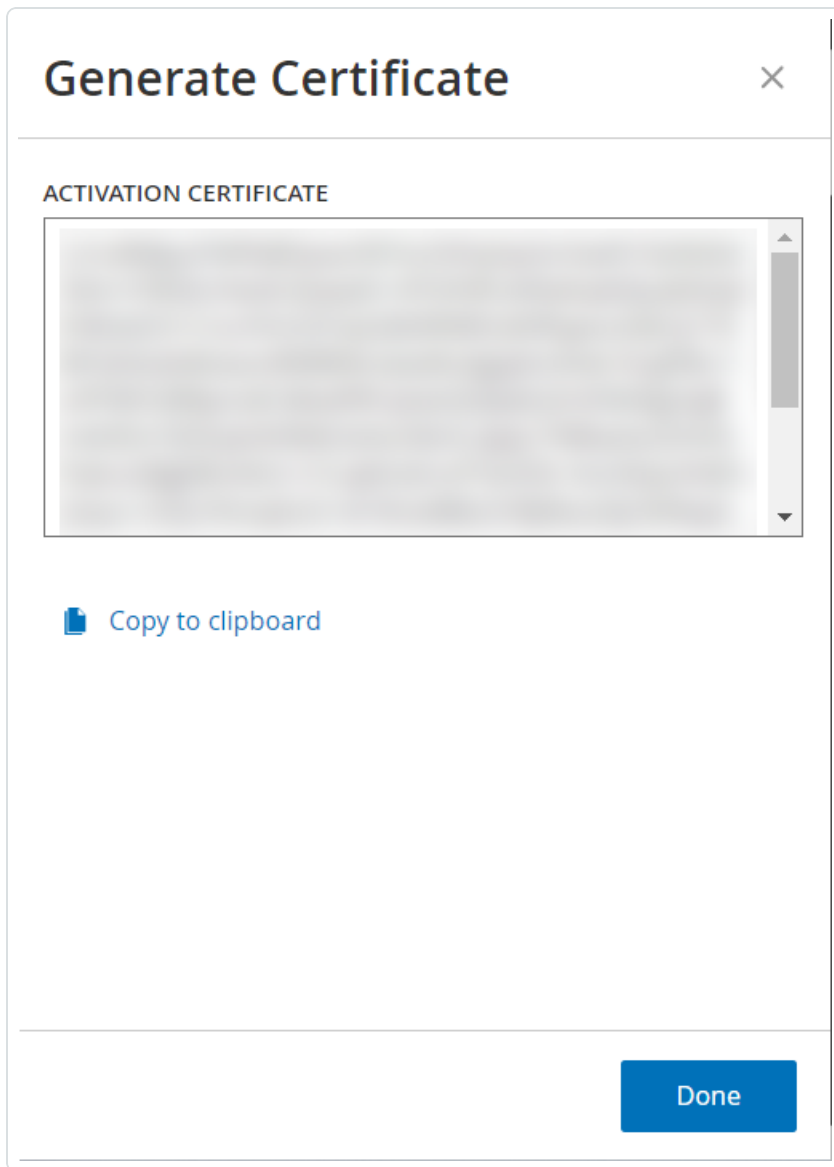
1 Certificate was generated successfully Generate certificate

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

Cancel

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


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



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

The side panel closes.

5. Edit the site details in the Tenable Provisioning portal:

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

A menu appears.

- b. Click **Edit Site**.



The edit window for the site appears.

Edit [Close]

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

Label (optional) ⓘ
HQICS

IPs
1426 - +

1 4949


Activation Certificate

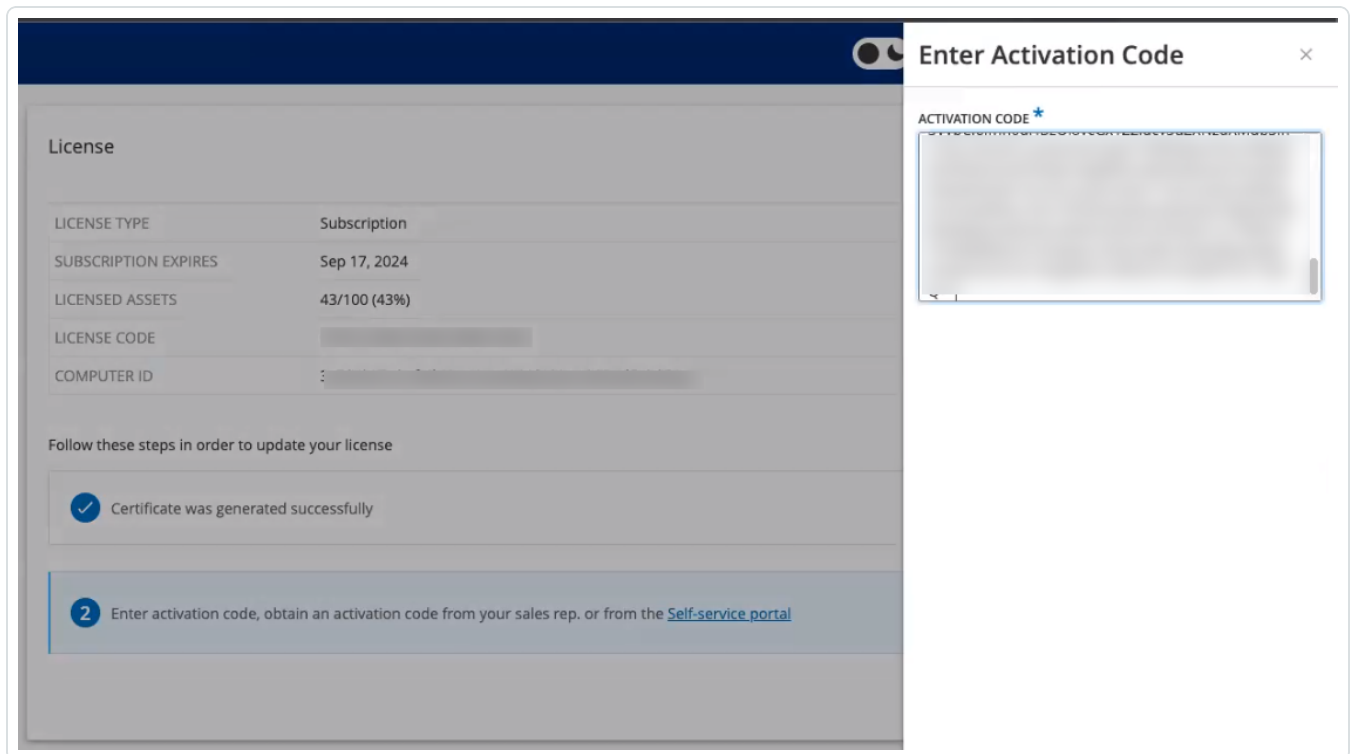
Submit Cancel

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



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

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



9. Click **Activate**.

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

Update your license in offline mode

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



License

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

Follow these steps in order to update your license

Certificate was generated successfully Generate certificate

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

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

Activate Tenable OT Security Offline

1 Activation Info

Offline Activation Details

Tenable OT Security

Activation Certificate

License Code

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

2 Confirmation

Information

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

[How Do I Generate a Tenable OT Security Activation Certificate?](#)

[Tenable Security Center Offline Activation](#)

[Tenable Nessus Professional Offline Activation](#)



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

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

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

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

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

6. Click **Generate Activation Code**.

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

Activate Tenable OT Security Offline



Offline Activation Code Successfully Created!

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




7. Click the  button.

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

License

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

Follow these steps in order to update your license

 Certificate was generated successfully

[Generate certificate](#)

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

[Enter Activation Code](#)

[Cancel](#)

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



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

The screenshot shows a dialog box titled "Enter Activation Code". It features a close button (X) in the top right corner. Below the title bar, there is a label "ACTIVATION CODE *" and a large, empty text input field. At the bottom of the dialog, there are two buttons: "Cancel" and "Activate".

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

Reinitialize your license

Reinitializing your license removes your current license from the system and activates a new license, similar to the license activation during your system startup. If you need to reinitialize your license (that is, if you are issued a new license), use the following procedure.

Before you Begin

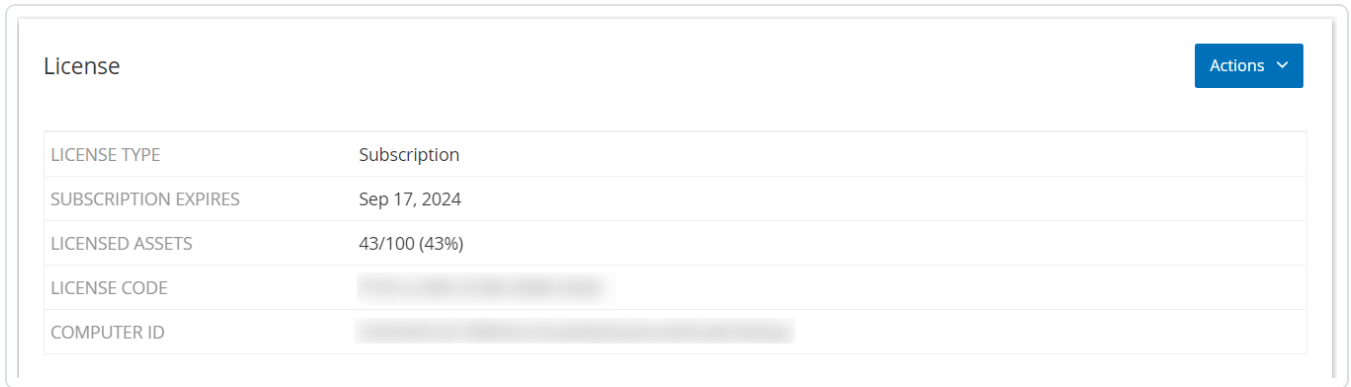
- Your Tenable account manager must have already issued your new license in their system and provided you with a License Code (20 characters letter/numbers).



- You need access to the Internet. If your OT Security EM device is not connected to the Internet, you can register the license from any PC.

To reinitialize your license:

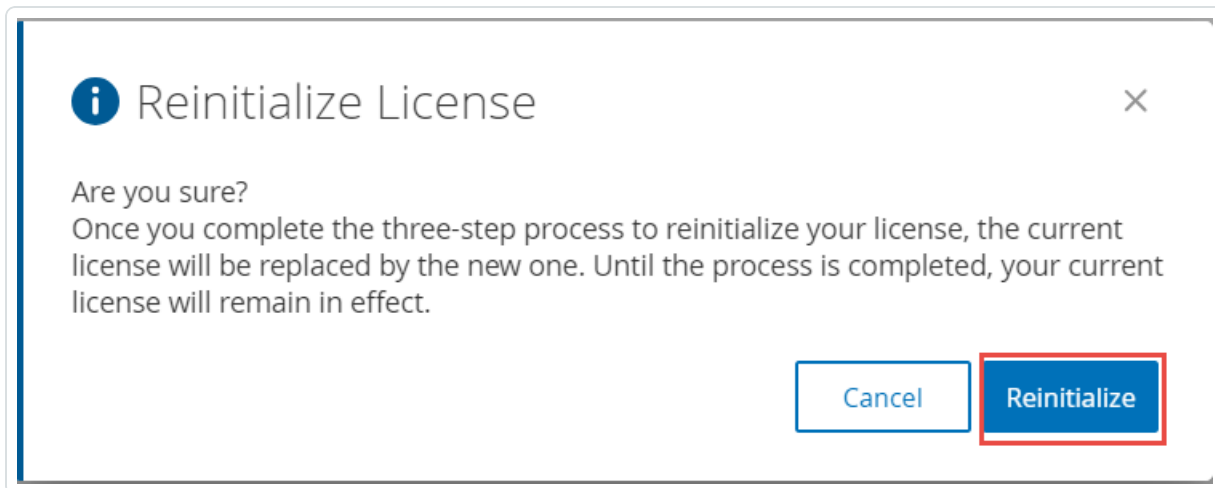
1. Go to **Local Settings > System Configuration > License**.



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

A confirmation window appears.

3. Click **Reinitialize**.



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



License

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

Follow these steps in order to reinitialize your license

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

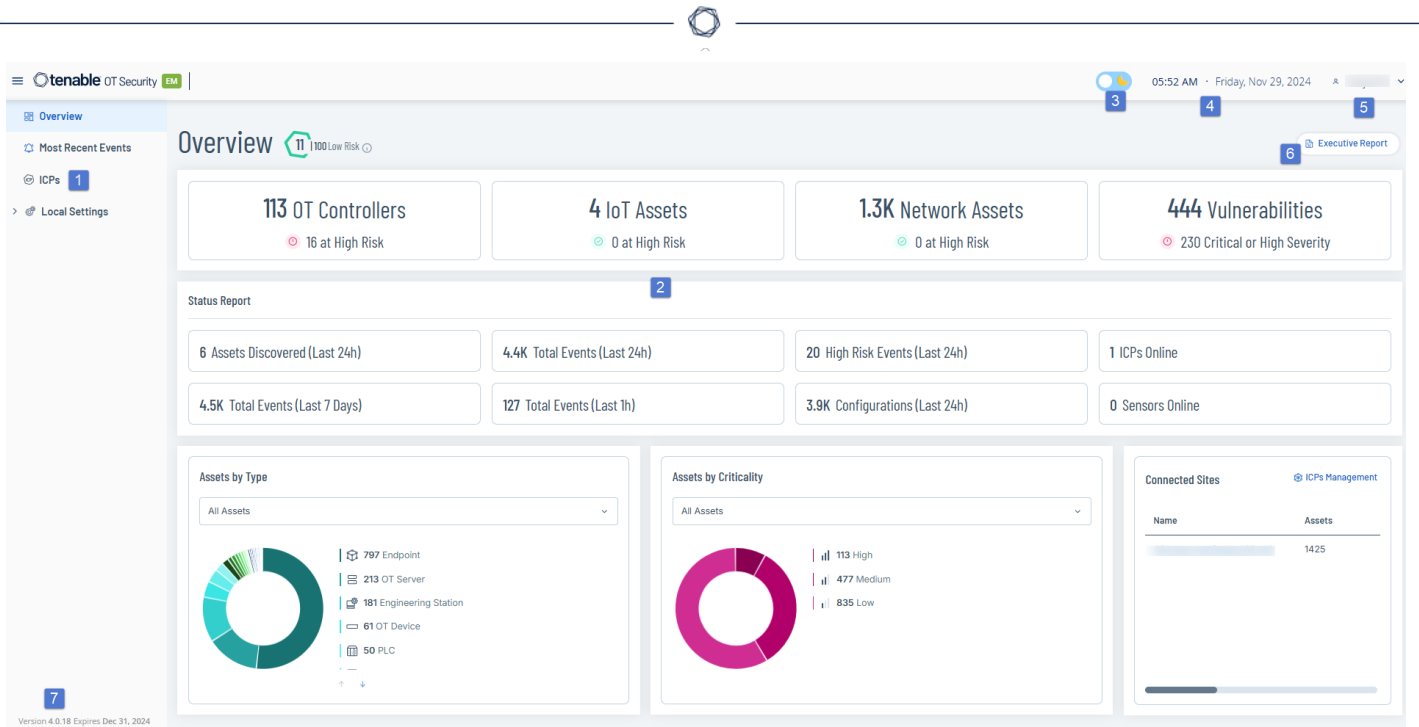
4. Follow the system start-up steps for activating your license. See [Activate your License](#).

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


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.

Main User Interface Elements



The following table describes the main user interface elements:

Sl.No	User interfaceElement	Description
1	Main Navigation	Main navigation menu. Click the  button to show/hide the main navigation menu.
2	Current Date and Time	The current date and time as in the system.
3	Current User	The name of the user currently logged in. Click the down arrow for a selection menu. Options are: About (shows software information) and Logout .
4	Version Info	The version of OT Security EM.
5	Main Screen	The screen that you select in the main navigation.
6	Dark Mode/Daylight Mode	Change the display color scheme to Dark mode or Daylight mode.
7	Executive Report	Generates a risk assessment report in PDF format.



Enterprise Manager Navigation Pages

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

- **Overview** – View widgets that give an at-a-glance view of your entire enterprise’s inventory and security posture based on the aggregated data from your sites. See [OT Security EM Overview](#)
- **Most Recent Events** – Shows the list of events in your EM environment in the last 24 hours. See [Most Recent Events](#).
- **ICPs** – Displays all ICP systems paired with the EM. See [ICPs](#).
- **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](#).

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.

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.



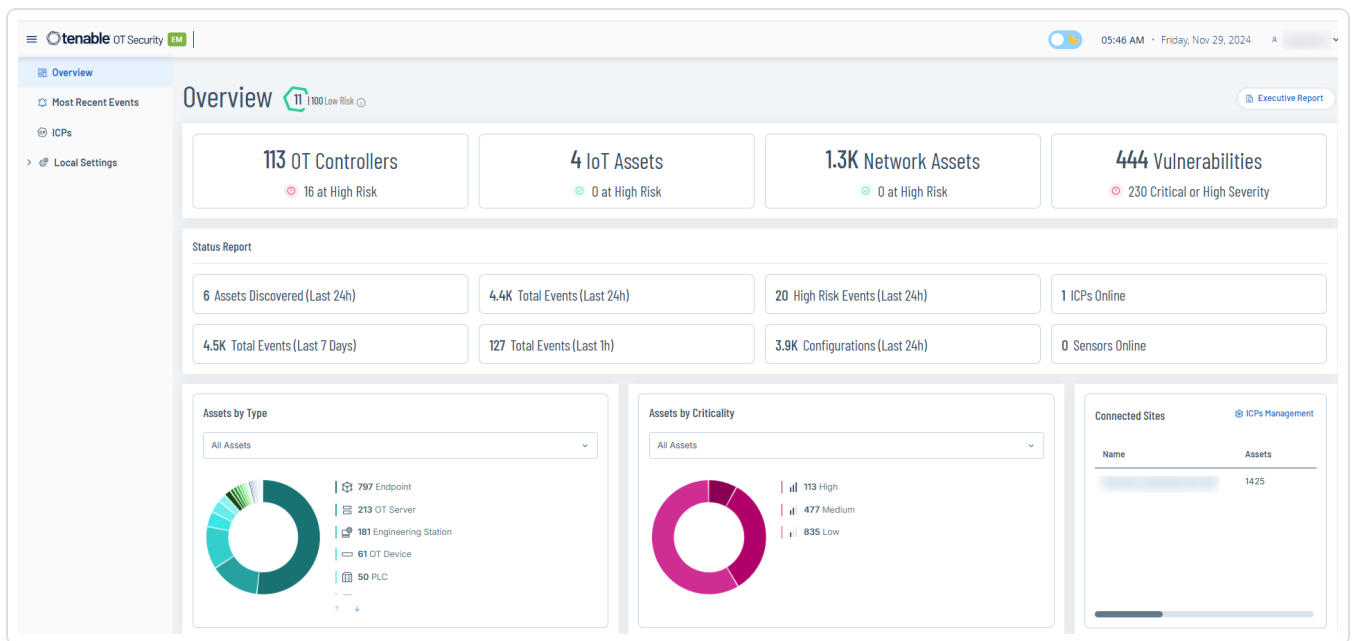
OT Security EM Overview

The **Overview** page features widgets that offer an at-a-glance view of your complete enterprise inventory and security posture. OT Security EM aggregates data from all sites and displays it in widgets. Along with the standard widgets for individual sites, the EM Overview page includes an ICP Status widget showing each site's the connectivity status.

To access the **Overview** page:

1. In the left hand navigation bar, click **Overview**.

The OT Security EM **Overview** page appears.



The Overview page includes the following widgets:

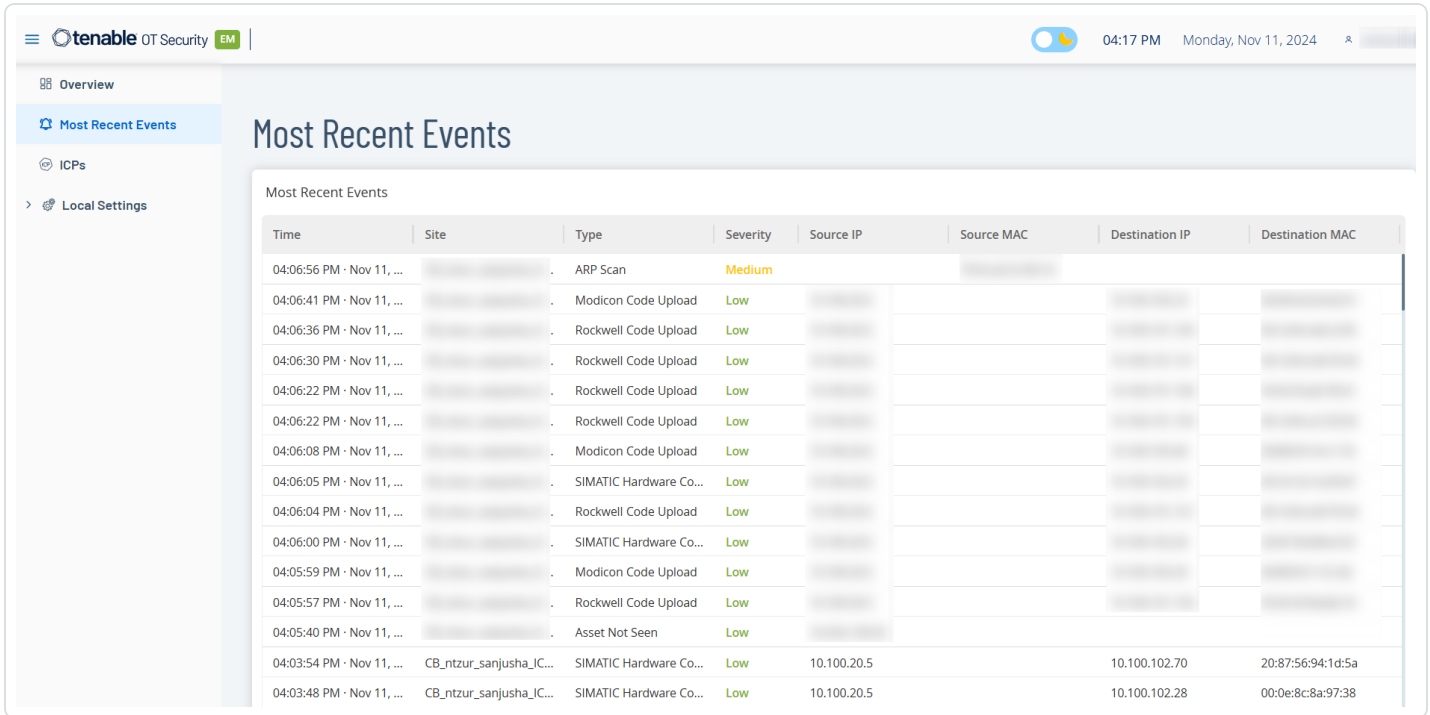
Widget	Description
Risk Score	The average risk score. Hover over the value to get a breakdown of the average risk score.
Executive Report	Click this link to generate a risk assessment report for your environment based on the data from the last 30 days. The report opens on your browser. To download the report as PDF, click Save as PDF at the top of the page.



Assets and Vulnerabilities	The current state of assets and vulnerabilities in your environment. Includes separate widgets for each asset type (OT Controllers, Network Assets, IoT Assets) that show the number of assets in that category and the number of assets that are at high risk.
Status Report	The overall status of your environment, such as assets discovered, total events, number of high risk events, number of configuration events in the last 24 hours. The widget also shows the number of ICPs and sensors that are online. The widget also includes total events in the last 7 days and in the last one hour.
Assets by Type	The number of assets by type, such endpoint, PLC, OT device, and so on.
Assets by Criticality	The number of assets by their criticality: High, Medium, or Low.
Connected Sites	<p>Lists the ICPs connected to the EM. The widget includes the following details:</p> <ul style="list-style-type: none">• Name – The name of the ICP.• Assets – The number of assets within the ICP.• Average Risk Score – The average risk score of the ICP.• Severe Vulnerability – The number of vulnerabilities in the critical state.• Last 24h Events – The number of events recorded in the ICP in the last 24 hours. <p>To open the ICPs page, in the upper-right corner, click ICPs Management.</p>

Most Recent Events

Use the **Most Recent Events** page to view the list of events in your EM environment in the last 24 hours.



Time	Site	Type	Severity	Source IP	Source MAC	Destination IP	Destination MAC
04:06:56 PM · Nov 11, ...		ARP Scan	Medium				
04:06:41 PM · Nov 11, ...		Modicon Code Upload	Low				
04:06:36 PM · Nov 11, ...		Rockwell Code Upload	Low				
04:06:30 PM · Nov 11, ...		Rockwell Code Upload	Low				
04:06:22 PM · Nov 11, ...		Rockwell Code Upload	Low				
04:06:22 PM · Nov 11, ...		Rockwell Code Upload	Low				
04:06:08 PM · Nov 11, ...		Modicon Code Upload	Low				
04:06:05 PM · Nov 11, ...		SIMATIC Hardware Co...	Low				
04:06:04 PM · Nov 11, ...		Rockwell Code Upload	Low				
04:06:00 PM · Nov 11, ...		SIMATIC Hardware Co...	Low				
04:05:59 PM · Nov 11, ...		Modicon Code Upload	Low				
04:05:57 PM · Nov 11, ...		Rockwell Code Upload	Low				
04:05:40 PM · Nov 11, ...		Asset Not Seen	Low				
04:03:54 PM · Nov 11, ...	CB_ntzur_sanjusha_IC...	SIMATIC Hardware Co...	Low	10.100.20.5		10.100.102.70	20:87:56:94:1d:5a
04:03:48 PM · Nov 11, ...	CB_ntzur_sanjusha_IC...	SIMATIC Hardware Co...	Low	10.100.20.5		10.100.102.28	00:0e:8c:8a:97:38

To access the **Most Recent Events** page:

1. In the left navigation bar, click **Most Recent Events**.

The **Most Recent Events** page appears with the following details:

Column	Description
Time	The time stamp of the event.
Site	The name of the site or ICP where the event is recorded.
Type	The type of event.
Severity	The severity of the event: Low, Medium, or High.
Source IP	The IP address of the event source.



Source MAC	The MAC address of the event source.
Destination IP	The IP address of the destination.
Destination MAC	The MAC address of the destination.



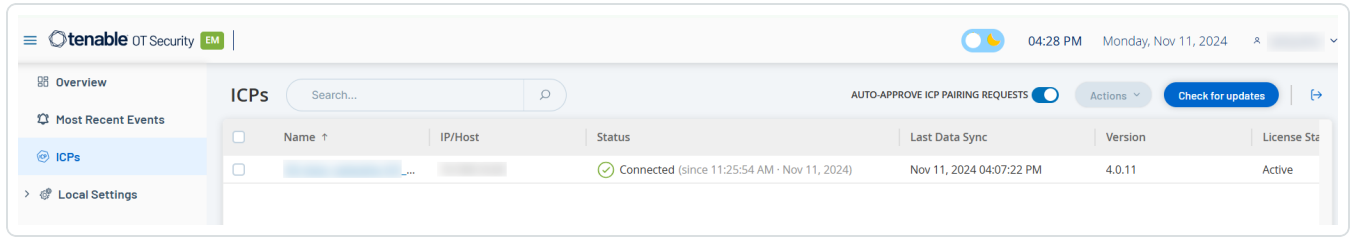
ICPs

Use the **ICPs** page to view all ICP systems paired with the EM in a table format.

To access the **ICPs** page:

1. In the left navigation bar, click **ICPs**.


The **ICPs** page appears with the list of paired ICPs.



The ICP table includes the following columns:

Column	Description
Name	The name of the ICP paired with the EM.
IP/Host	The IP address or the hostname of the ICP.
Status	The status of the ICP: <ul style="list-style-type: none">• Connected• Pending Approval• Disconnected• Update in progress
Last Data Sync	The date of the last data synchronization of the ICP with the EM.
Version	The version of OT Security.
License Status	The status of the license: <ul style="list-style-type: none">• Active• Expired



License Type	The type of license: Perpetual or Subscription .
License Expires	The date when the license ages out for the ICP.
Licensed Assets	The number of licensed assets for the ICP.
Computer ID	The ID of the ICP system.
Sensors Info	<p>The online or offline status of the connected sensors.</p> <p>Click the sensors link to go to the Sensors page in OT Security.</p> <div style="border: 1px solid blue; padding: 5px;"><p>Note: To return to the OT Security EM interface, from the  profile button, click Return to EM.</p></div>
License Usage	The number of licensed assets currently in use.
Last Nessus Plugin Set	The date of the last Nessus plugin update.
Last IDS Engine Ruleset	The date of the last IDS Engine Ruleset.
Memory Usage	The percentage of memory usage of the ICP.
CPU Usage	The percentage of CPU usage of the ICP.

You can do the following actions from the **ICPs** page:

Approve pairing requests automatically

- To approve ICP pairing with EM automatically, enable the **Auto Approve ICP Pairing Requests** toggle.

Approve pairing requests manually

To approve ICP pairing requests manually, do one of the following:



- a. In the row of the ICP you want to approve:
 - Right-click the ICP and select **Approve**.
 - Click the ICP row. This highlights the row and enables the **Actions** button.
- b. Click **Actions** > **Approve**.

Disconnect an ICP pairing

To disconnect an ICP from the EM, do one of the following:

- a. In the row of the ICP you want to disconnect:
 - Right-click and select **Delete**.
 - Click the ICP row. This highlights the row and enables the **Actions** button.
- b. Click **Actions** > **Delete**.

Access the ICP from OT Security EM


To navigate to the ICP from the EM:

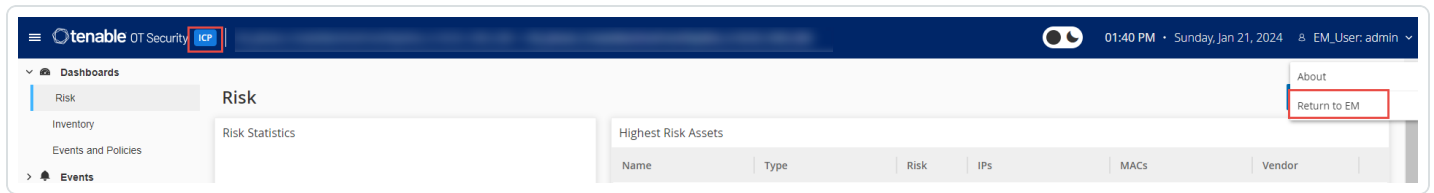
- a. In the row of the ICP that you want to open, click the ICP link in the **Name** column.
OT Security EM opens the OT Security Dashboards page.

When accessing the ICP from **ICPs** page, the OT Security header shows the **ICP** label.



To return to the OT Security EM interface from the ICP:

- a. In the upper-right corner, click the  profile button,
A menu appears.
- b. Select **Return to EM**.
OT Security EM interface appears.



Update ICPs

Update your ICP and operating system (OS) to the latest available version. You have the option to update only the OS without the OT Security application. Upgrading only the OS helps reduce system downtime, but Tenable recommends that you update both the application and OS.

Important: You can update ICPs starting from version 4.1 and later. For example, in OT Security EM 4.1, you can update 4.0 ICPs.

To update ICP and OS:

1. In the upper-right corner, click **Check for Updates**.

The **Version** column of the ICPs table displays an **updates available** message.



2. Do one of the following:

Update	Action
A single ICP	<p>To update a single ICP:</p> <ol style="list-style-type: none">In the ICPs table, select the checkbox next to the ICP you want to update. OT Security EM enables the Action button in the header bar.Click Actions > Update ICP Version. The Update ICP Version panel appears.Select one of the following options:<ul style="list-style-type: none">Update ICP Application to version xx.xx.xx, including OS (recommended) – This option is selected by default.Update OS onlyClick Update. The Update ICP Version panel appears with the message that the update process of the selected ICP is about to start.
Multiple ICPs	<p>To update multiple ICPs:</p> <ol style="list-style-type: none">In the ICPs table, select one or more ICPs. OT Security EM enables the Action button in the header bar.Click Actions > Update ICP Version.Select one of the following options:<ul style="list-style-type: none">Update ICP Application to version xx.xx.xx, including OS (recommended) – This option is selected by default.Update OS onlyClick Update.



The **Update ICP Version** panel appears with the message that the update process of the selected ICPs is about to start.

Note: The update process might take up to an hour to complete. During this time, OT Security application is not accessible.

During the update, the **Status** column in the ICPs table shows **Update in progress**. Once the update is complete, the status changes to **Connected**.



Pair ICP with Enterprise Manager

Note: This flow is available for OT Security 3.18 and later.

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

Before you Begin

Make sure that:

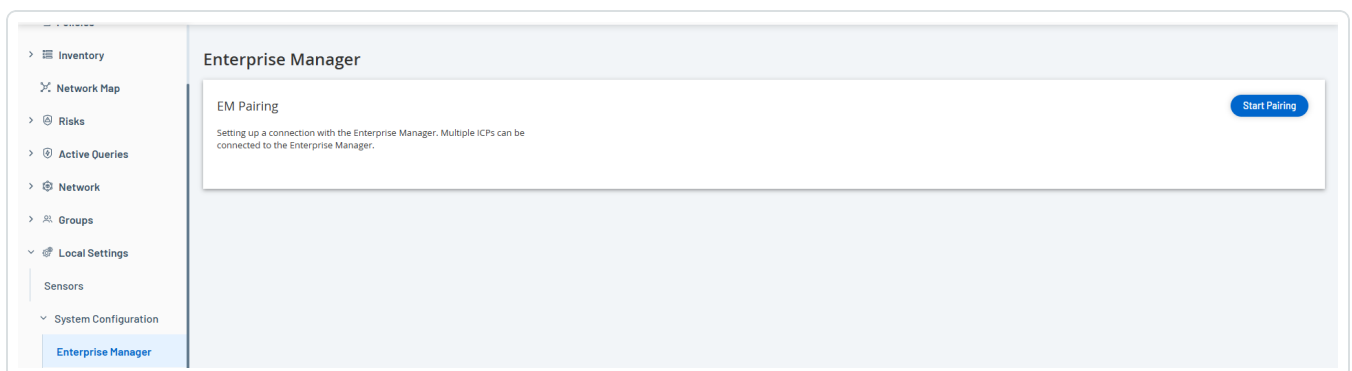
- OT Security EM can connect via API to the ICP.
- Make sure TCP 443 and TCP 28305 are open for communication from ICP to OT Security EM.
- HTTPS connections exist between ICP and OT Security EM.
- (Optional) Generate an API Key in OT Security EM.

Note: This is required only when pairing using the API key option.

To pair ICP with OT Security EM:

1. In OT Security, go to **Local Settings > System Configuration > Enterprise Manager**.

The **Enterprise Manager** page appears.



2. In the **EM Pairing** section, click **Start Pairing**.

The **EM Pairing Configuration** panel appears.

3. Select one of the following:



- **Pair using username and password**
- **Pair using API secret**

If you select...	Action
Pair using username and password	<ol style="list-style-type: none">1. In the Hostname/IP box, type the hostname or the IP address of the EM.2. In the Username box, type the administrator username of the EM.3. In the Password box, type the password of the EM.4. In the EM Certificate Fingerprint, paste the certificate that you copied from the EM Certificates page. <div data-bbox="716 816 1479 932" style="border: 1px solid green; padding: 5px;">Tip: You can skip this step and manually approve the certificate from the EM Pairing page.</div> <div data-bbox="716 957 1479 1073" style="border: 1px solid blue; padding: 5px;">Note: You can access the Certificates page from Local Settings > System Configuration in OT Security EM.</div>
Pair using API Key	<ol style="list-style-type: none">1. In the Hostname/IP box, type the hostname or the IP address of the EM.2. In the API Secret box, paste the API key that you copied from the EM.3. In the EM Certificate Fingerprint, paste the certificate that you copied from the EM Certificates page. <div data-bbox="716 1465 1479 1581" style="border: 1px solid green; padding: 5px;">Tip: You can skip this step and manually approve the certificate from the EM Pairing page.</div> <div data-bbox="716 1606 1479 1722" style="border: 1px solid blue; padding: 5px;">Note: You can access the Certificates page from Local Settings > System Configuration in OT Security EM.</div>

4. Click **Pair**.



OT Security displays the **EM Pairing** page with the pairing status.

Note: The status can show as **Waiting for certificate approval** (if certificate is not provided) or **Pending EM approval** (if automatic approval of pairing requests is disabled).

5. (Optional) If the status shows **Waiting for certificate** approval:

a. Click **Show Certificate**.

The **Approve Certificate** panel appears.

b. Verify if the fingerprint on the panel is the same as that on the EM **Certificates** page.

Click **Approve**.

OT Security approves the certificate and displays the EM pairing page with the status changed to **Pending EM approval**.

6. If the status shows **Pending EM approval**, it indicates that **Auto Approve ICP Pairing Requests** is disabled, then proceed as follows:

Tip: To approve pairing requests automatically in OT Security EM, enable the **Auto Approve ICP Pairing Requests** in the OT Security EM **ICPs** page.

a. In OT Security EM, in the left navigation bar, select **ICPs**.

The **ICPs** page appears.

b. Hover over the row of the system you want to pair, do one of the following:

- Right-click the **Status** column and select **Approve**.
- In the upper-right corner, click **Actions > Approve**.

OT Security EM approves the pairing and shows the status as **Connected**.

Tip: After the pairing is complete, OT Security EM shows the following:

- Shows the data from the ICP on the EM **Dashboards**.
- Newly paired ICP appears on the **ICPs** page.
- Access to the ICP by clicking the ICP name from the **ICPs** page. The ICP instance



accessed from the EM shows the **ICP** label in the header. For more information, see [ICPs](#) in the Tenable OT Security Enterprise Manager User Guide.

In OT Security, the **Enterprise Manager** page shows the status as **Connected**. You can click **Edit** to modify the EM pairing configuration.

Disconnect ICP Pairing with Enterprise Manager

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

To disconnect an ICP pairing from OT Security EM:

1. In OT Security EM, in the left navigation bar, select **ICPs**.

The **ICPs** page appears.

2. Hover over the row of the ICP you want to delete, do one of the following:
 - Right-click the **Status** column and select **Delete**.
 - Click the ICP row. This highlights the row and enables the **Actions** button.
3. Click **Delete**.

OT Security EM disconnects the pairing with OT Security.

To disconnect an ICP pairing from OT Security:

1. In OT Security, go to **Local Settings > System Configuration > Enterprise Manager**.

The **Enterprise Manager** page appears.

2. In the EM Pairing section, click **Edit**.

The **EM Pairing** panel appears.

3. Click **No Pairing**.
4. Click **Pair**.

OT Security disconnects the pairing with OT Security EM.



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](#)
- [API Keys](#)
- [License](#)
- [Users Management](#)
- [User Settings](#)
- [Local Users](#)
- [User Groups](#)
- [Authentication Servers](#)
- [SAML](#)
- [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).

The screenshot shows the Tenable OT Security EM console interface. On the left is a navigation menu with options like Overview, Most Recent Events, ICPs, Local Settings, System Configuration, and User Management. The 'Device' page is active, displaying four configuration sections: Device Name (with value 'CB_ntzur_CreateMachineFromPipeline_3.19.70_4788_JEM_ol8'), Device URLs, System Time (with value 'Nov 12, 2024 04:21:59 AM'), and Timezone. Each section has an 'Edit' button. The top right shows the time '04:22 AM' and date 'Tuesday, Nov 12, 2024'. The bottom left corner indicates 'Version 4.0.11 Expires Dec 31, 2024'.

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.
Timezone	The time zone of the system.
Automatic Logout	The period of inactivity that causes the system to log out automatically.
Ping Requests	Set to detect whether or not the OT Security platform responds to ping requests.
Classification Banner	Add a banner to OT Security EM to indicate the data accessible via the software.



	<p>To add a banner, click Edit. After adding the banner, click to enable the Classification Banner toggle.</p>
Enable Usage Statistics	<p>The Enable Usage Statistics option specifies whether Tenable collects anonymous telemetry data about your OT Security EM deployment.</p> <p>When enabled, Tenable collects telemetry information at the company level and not at an individual level. This information does not include personal data or personally identifiable information (PII). Telemetry information includes, but is not limited to, data about your visited pages, your used reports and dashboards, and your configured features. Tenable uses the data to improve your user experience in future OT Security EM releases and for other reasonable business purposes in accordance with the Tenable Master Agreement. This setting is enabled by default.</p> <p>To enable telemetry collection, click the Enable Usage Statistics toggle.</p> <div style="border: 1px solid #0070C0; padding: 5px;"><p>Note: You can disable sharing of usage statistics at any time by clicking the toggle switch.</p></div>
Auto approve ICP pairing requests	<p>Enable this option to approve all ICP pairing requests automatically. For more information about pairing an ICP, see Pair ICP with Enterprise Manager.</p>

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.



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 Security
ISSUED BY	Tenable OT Security
ISSUED ON	Nov 8, 2023
EXPIRES ON	Nov 7, 2025
CERTIFICATE FINGERPRINT	[REDACTED]

Actions

- Generate Self-Signed Certificate
- Upload Certificate
- Download Certificate

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

Parameter	Description
Issued to	The entity to which the certificate was issued.
Issued by	The entity that issued the certificate.
Issued on	The issue date of the certificate.
Expires on	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**.

License

LICENSE TYPE	Subscription
SUBSCRIPTION EXPIRES	Dec 31, 2024
LICENSE CODE	[REDACTED]
COMPUTER ID	[REDACTED]

Follow these steps in order to update your license

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

Cancel

Users Management

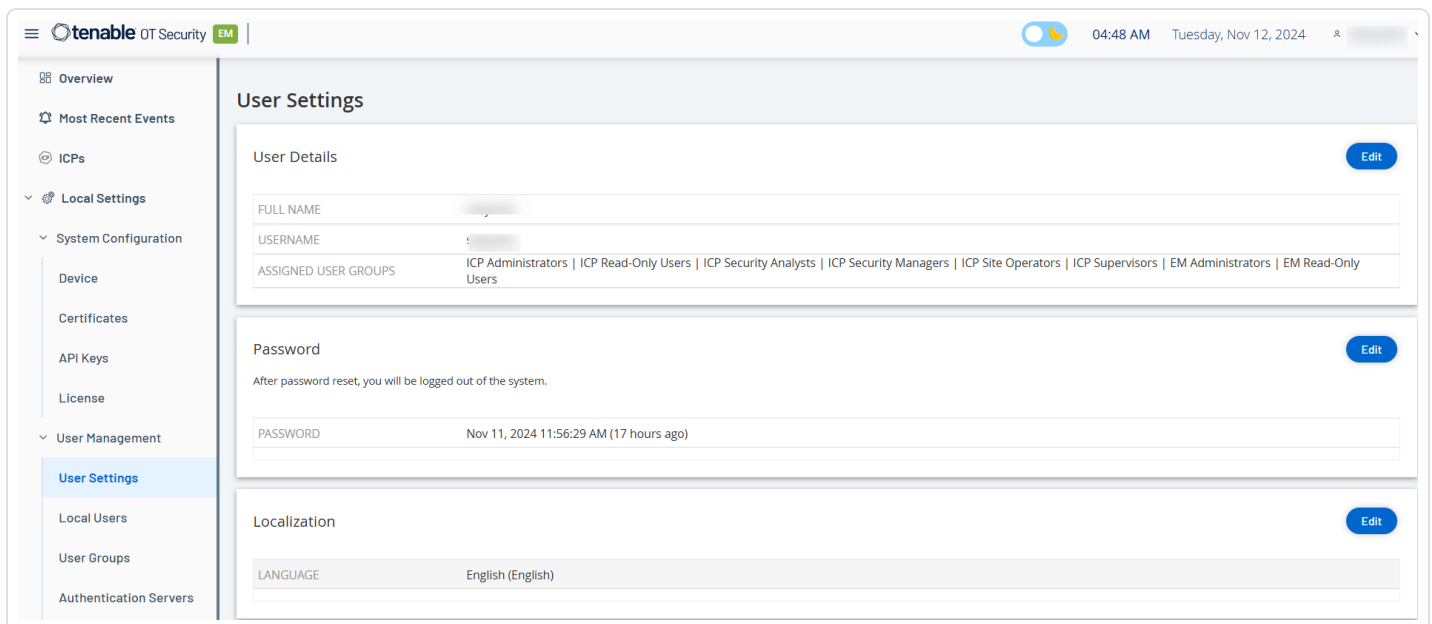


The **Users Management** section includes these pages:

- [User Settings](#)
- [Local Users](#)
- [User Groups](#)
- [Authentication Servers](#)
- [SAML](#)

User Settings

The User Settings page allows you to view and edit information about the user who is currently logged into the system (Full Name, Username, and Password) and change the user interface language (English, Japanese, Chinese, French, or German).



The following table describes the information on the **User Settings** page.

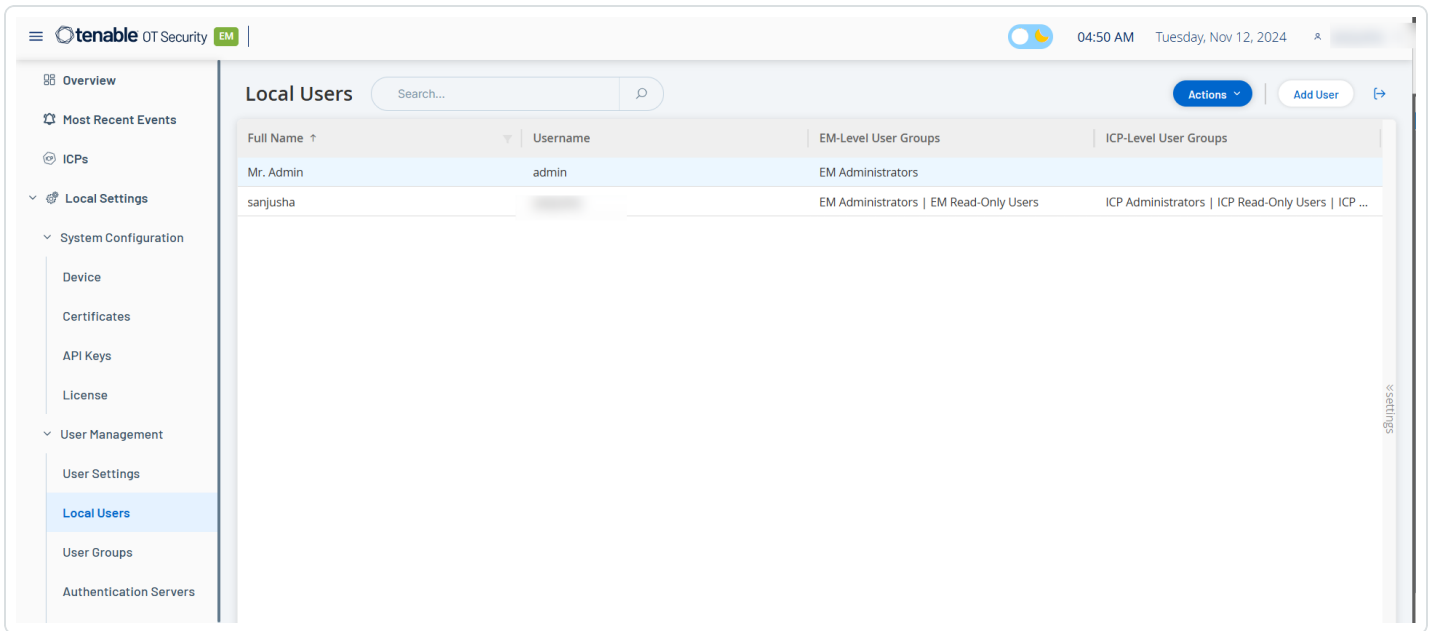
Parameter	Description
Full Name	The first and last name of the user.
Username	The username of the user.
Assigned User	The user groups assigned to the user.



Groups	
Language	The language of the user interface (English, Japanese, Chinese, French, or German).

Local Users

The **Local Users** page lists the local users for the OT Security EM. On this page, an administrator user can create new user accounts, reset passwords, and edit or delete existing accounts. Each user belongs to one or more user groups, which determine the roles assigned to the user.



- To add new users, in the upper-right corner, click **Add User**.
- To modify a user, delete a user, or change a user's password, click the **Actions** button.
- To download a CSV file of the users, click the **Export** button.

You can customize the display settings by adjusting the display and position of columns. You can also sort and filter the users list as well as search for text in the **Search** box. For information about customizing features, see [Customize Tables](#) in the Tenable OT Security User Guide.

The **Local Users** page shows the following details:

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



Full Name	The first and last name of the user.
Username	The username of the user.
EM Level User Groups	The EM user groups assigned to the user. The options available are: EM Administrators and EM Read-Only Users .
ICP Level User Groups	The ICP user groups assigned to the user. The ICP user groups available are: <ul style="list-style-type: none">• ICP Administrators• ICP Read-Only Users• ICP Security Analysts• ICP Security Managers• ICP Site Operators• ICP Supervisors

You can perform the following actions from the **Local Users** page:

Add a Local User

You can create user accounts to authorize individual users to access the system. Each user must belong to one or more User Groups.

To create a local user account:

1. Go to **Local Settings > Users Management > Local Users**.
2. Click **Add User**.

The **Add User** pane appears.

Add User ✕

FULL NAME *

USERNAME *

PASSWORD *

RETYPE NEW PASSWORD *

EM LEVEL USER GROUPS *

ICP LEVEL USER GROUPS *

3. In the **Full Name** box, type the first and last name.



Note: The name that you enter appears in the header bar when the user signs in.

4. In the **Username** box, type a username to use when logging in to the system.
5. In the **Password** box, type a password.
6. In the **Retype Password** box, retype the password.

Note: This is the password that the user uses for the initial login. The user can change the password in the **Settings** window after logging into the system.

7. In the **EM Level User Groups** drop-down box, select the checkbox for each user group to which you want to assign this user. The EM user groups available are: **EM Administrators** and **EM Read-Only Users**.
8. In the **ICP Level User Groups** drop-down box, select the ICP group to which you want to assign this user. The ICP user groups available are:
 - **ICP Administrators**
 - **ICP Read-Only Users**
 - **ICP Security Analysts**
 - **ICP Security Managers**
 - **ICP Site Operators**
 - **ICP Supervisors**
9. Click **Create**.

OT Security creates the new user account in the system and adds it to the list of users in the **Local Users** page.

Edit a User

You can assign a user to additional user groups or remove the user from a group.

To edit a user group:



1. Go to **Local Settings > Users Management > Local Users**.

The **Local Users** page appears.

2. Do one of the following:

- Select the row of the user you want to edit and click **Actions** in the upper-right corner.

A menu appears.

- Right-click the row of the user you want to edit.

A menu appears.

3. Click **Edit User**.

The **Edit User** panel appears.

4. In the **EM Level User Groups** box, select or clear the user groups to which the user belongs.

5. In the **ICP Level User Groups** box, select or clear the user groups to which the user belongs.

6. Click **Save**.

OT Security EM saves the changes to the user account.

Reset Password

Note: Only an administrator can change the password for any account in the system. Any user can change their own password from **Local Settings > User Settings**.

To change the password of a user:

1. Go to **Local Settings > Users Management > Local Users**.

The **Local Users** page appears.

2. Do one of the following:

- Select the row of the user you want to change the password and click **Actions** in the upper-right corner.

A menu appears.



- Right-click the row of the user whose password you want to change.

A menu appears.

3. Click **Reset Password**.

The **Reset Password** panel appears.

4. In the **New Password** box, type a new password.
5. In the **Retype New Password** box, retype the new password.
6. Click **Reset**.

OT Security EM applies the new password to the specified user account.

Delete a User

1. Go to **Local Settings > Users Management > Local Users**.

The **Local Users** page appears.

2. Do one of the following:

- Select the row of the user you want to delete and click **Actions** in the upper-right corner.

A menu appears.

- Right-click the row of the user you want to delete.

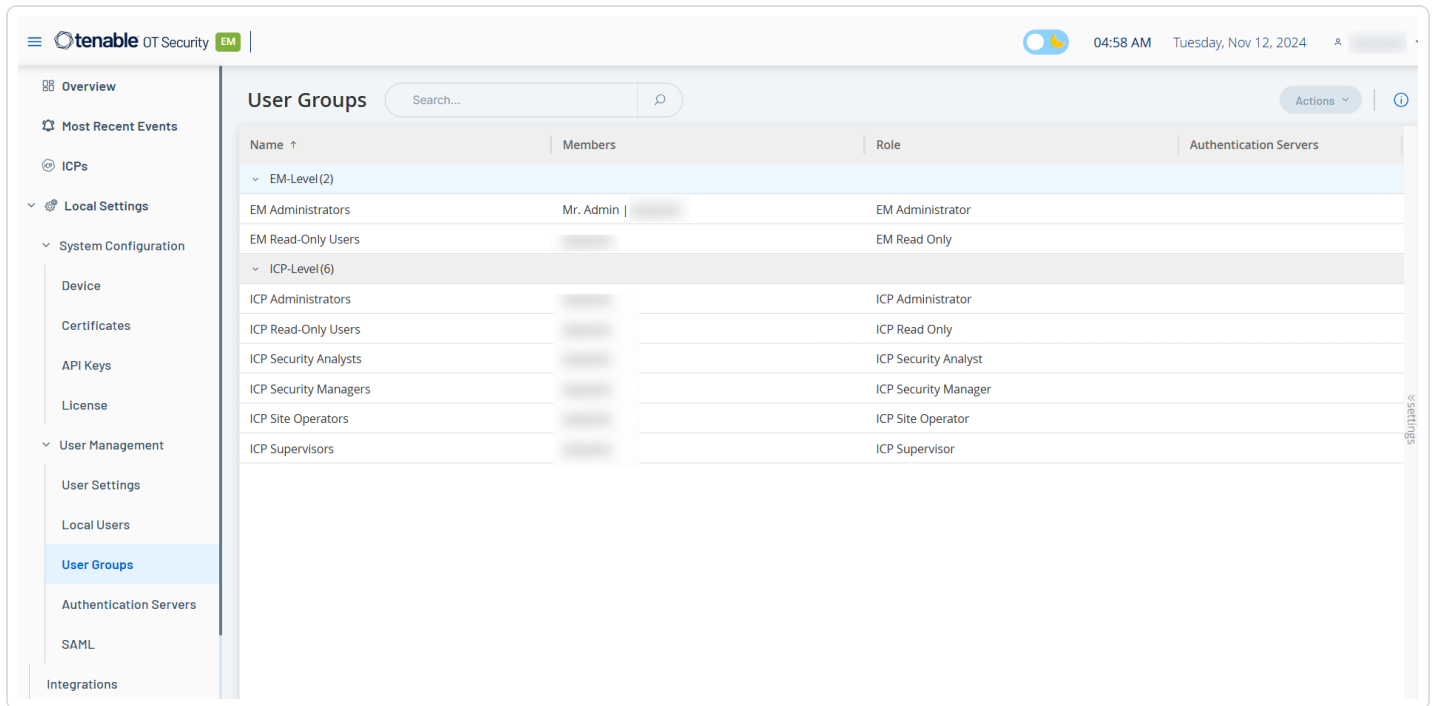
A menu appears.

3. Click **Delete User**.

OT Security EM deletes the user account from the system.

User Groups

Use the User Groups page to view the list of users assigned to the EM Level and ICP Level User Groups. An administrator can create new user groups and edit existing groups. For more information about assigning users to a user group, see [Add a Local User](#).



The User Groups table includes the following:

Column	Description
Name	The type of user group: EM Level and ICP Level .
Members	The user account assigned to the EM level and ICP level user group.
Role	The role assigned to the user account: <ul style="list-style-type: none"> • EM Administrator • EM Read Only • ICP Administrator • ICP Supervisor • ICP Security Manager • ICP Security Analyst

You can perform the following on the **User Groups** page:

Edit a User Group



To change the user groups assigned to a user account, in the upper-right corner, click **Actions > Edit**.

View User Role Descriptions

In the upper-right corner, click the  button to view the user group descriptions.

Authentication Servers

The **Authentication Servers** page shows your existing integrations with authentication servers. You can add a server by clicking the **Add server** button.

You can integrate OT Security EM with the following types of servers:

Active Directory

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

To configure your Active Directory:

1. Go to **Local Settings > Users Management > Authentication Servers**.

The **Authentication Servers** window appears.

2. In the upper-right corner, click **Add server**.

The **Create Authentication Server** panel opens with the **Server Type**.

3. Click **Active Directory**, then click **Next**.

The **Active Directory** configuration pane appears.

4. In the **Name** box, type the username used for logging in to the server.

5. In the **Domain** box, type the FQDN of the organizational domain (for example, company.com).

Note: To find your domain, type the command "set" in the Windows CMD or command line. The value given for the "USERDNSDOMAIN" attribute is the Domain Name.



6. In the **Base DN** box, type the name of the domain. The format for this value is 'DC={second-level domain},DC={top-level domain}' (for example DC=company,DC=com).
7. For each of the groups you want to map from the Active Directory group to an OT Security EM User Group, type the Domain Name of the Active Directory group in the relevant box.

Note: These parameters are optional. However, if a parameter remains empty, no Active Directory users get assigned to that user group. You can set up an integration without mapped groups, but no user can access the system until you add at least one group mapping.

8. (Optional) In the **Trusted CA** section, click **Browse** and navigate to the file that contains your organization's CA Certificate.

Note: You can obtain the certificate from your CA or Network Administrator.

9. Click **Save**.

OT Security EM shows a message prompting you to restart to activate the Active Directory.

10. Click **Restart**.

After the system restarts, OT Security EM activates the Active Directory settings. Any user assigned to the designated group can access the OT Security EM platform using their organizational credentials.

LDAP

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

To configure LDAP:

1. Go to **Local Settings > User Management > Authentication Servers**.

2. Click **Add Server**.

The **Add Authentication Server** panel opens with the **Server Type**.

3. Select **LDAP**, then click **Next**.

The **LDAP Configuration** pane appears.



4. In the **Name** box, type the username that you want to use for logging in.

Note: The login name must be unique and clearly denote its usage for LDAP. If you have both LDAP and Active Directory configured, the username serves as the sole identifier that distinguishes between the various server configurations on the login screen.

5. In the **Server** box, type the FQDN or the login address.

Note: If you use a secure connection, Tenable recommends using the FQDN instead of an IP address to ensure verification of the provided secure certificate.

Note: If you use hostname, it must appear in the list of DNS Servers in the OT Security EM system. See [System Configuration > Device](#).

6. In the **Port** box, type 389 to use a non-secure connection, or 636 to use a secure SSL connection.

Note: If you select 636, you must provide a certificate to complete the integration.

7. In the **User DN** box, type the domain name with parameters in DN format. For example, for a server name of AD_1.qa.com, the user DN can be CN=Administrator,CN=Users,DC=qa,DC=com.
8. In the **Password** box, type the password of the **User DN**.

Note: The OT Security EM configuration with LDAP only continues to work as long as the User DN password is valid. Therefore, when the User DN password changes or ages out, you must update the OT Security EM configuration.

9. In the **User Base DN** box, type the base domain name in DN format. For example, DC=qa,DC=com.
10. In the **Group Base DN** box, type the Group base domain name in DN format.
11. In the **Domain append** box, type the default domain appended to the authentication request if the user did not apply a domain to which they belong.
12. In the relevant group name boxes, type the Tenable group names for the user to use with the LDAP configuration.



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

14. Click **Save**.

OT Security EM starts the Server in the **Disabled** mode.

15. To apply the configuration, click the enable toggle.

The **System Restart** dialog appears.

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

Note: Enabling or disabling LDAP configuration is not complete until the system restarts. If you do not restart the system immediately, click **Restart** on the banner at the top of the page when you are ready to restart.

SAML

You can integrate OT Security EM with your organization's identity provider (for example, Microsoft Entra ID). This enables users to authenticate using their identity provider. The configuration involves setting up the integration by creating an OT Security EM application within your identity provider, by entering information about your created OT Security EM application, and uploading your identity provider's Certificate to the OT Security **SAML** page. Then, map the groups from your identity provider to User Groups in OT Security EM.

To configure SAML:

1. Go to **Local Settings >Users Management > SAML**.
2. Click **Configure**.

The **Configure SAML** panel appears.

Configure SAML

IDP ID *
https://SAML_Host.com

IDP URL *
https://SAML_host/saml-authresponse

CERTIFICATE DATA *
PEM format only
DROP FILE HERE Browse

USERNAME ATTRIBUTE *
NameID

GROUPS ATTRIBUTE *
GroupsID

DESCRIPTION

EM ADMINISTRATORS GROUP OBJECT ID

Cancel Save

3. In the **IDP ID** box, type the Identity Provider's ID for the OT Security EM application.
4. In the **IDP URL** box, type the Identity Provider's URL for the OT Security EM application.



5. In **Certificate Data**, click **Drop File Here**, navigate to and open the Identity Provider's Certificate file you downloaded for use with the OT Security EM application.
6. In the **Username Attribute** box, type the username attribute from the Identity Provider for the OT Security EM application.
7. In the **Groups Attribute** box, type the groups attribute from the Identity Provider for the OT Security EM application.
8. (Optional) In the **Description** box, type a description.
9. For each group mapping that you want to configure, access the Identity Provider's **Group Object ID** for a group of users and enter it into the required **Group Object ID** box to map it to the required OT Security EM User Group.

The image shows a configuration window with a vertical scrollbar on the right side. It contains eight text input fields, each with a label above it:

- EM ADMINISTRATORS GROUP OBJECT ID
- EM READ-ONLY USERS GROUP OBJECT ID
- ICP ADMINISTRATORS GROUP OBJECT ID
- ICP READ-ONLY USERS GROUP OBJECT ID
- ICP SECURITY ANALYSTS GROUP OBJECT ID
- ICP SECURITY MANAGERS GROUP OBJECT ID
- ICP SITE OPERATORS GROUP OBJECT ID
- ICP SUPERVISORS GROUP OBJECT ID

At the bottom of the window, there are two buttons: "Cancel" (with a blue border) and "Save" (with a grey background).

10. Click **Save** to save and close the side panel.
11. On the **SAML** window, click the **SAML single sign-on login** toggle to enable single sign-on login.

The **System Restart** notification window appears.



- Click **Restart Now** to restart the system and apply the SAML configuration immediately, or click **Restart Later** to delay the application of the SAML configuration at the next system restart.

If you choose to restart later, OT Security EM shows following banner until the next restart:



After the restart, the settings are activated to allow any user belonging to the designated groups access the OT Security EM platform using their Identity Provider credentials.


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.

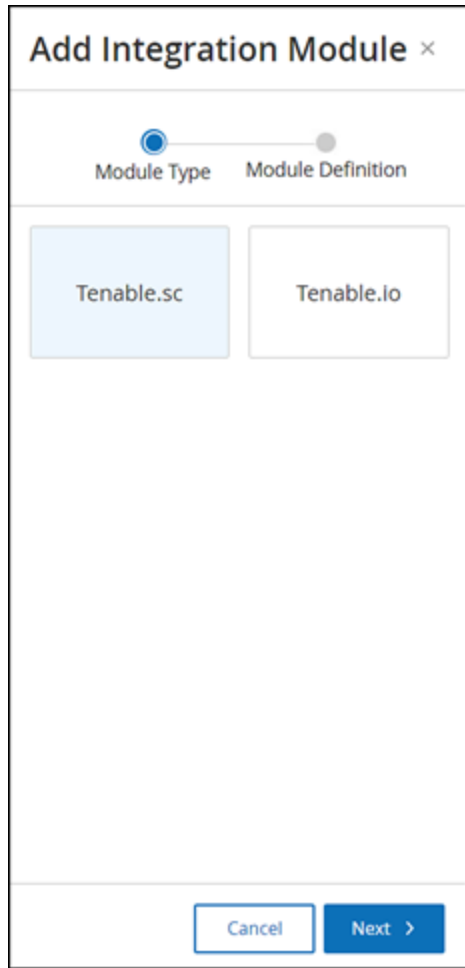
Note: Tenable recommends that you create Tenable Security Center repositories with matching names to OT Security Sites to optimize the mapping of Sites to repositories. The exact OT Security Site names must be contained within the Tenable Security Center repository names. For example, for a site named “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 [Close]

Module Type [Completed] Module Definition [In Progress]

Tenable.sc

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.



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

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



Add Integration Module ×

Module Type Module Definition

Tenable.io

ACCESS KEY *

SECRET KEY *

SYNC FREQUENCY *

Sync frequency is identical to all Tenable.io integrations

Every 6 hours

Test Connection

< Back Cancel Save

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.

Syslog Servers

SERVER NAME *

HOSTNAME / IP *

PORT *

*** Transport**

Send keep-alive message every 10m0s

Allow Syslog message caching

[Cancel](#) [Create](#) [Send Test Message](#)

[Add Syslog Server](#)

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. (Optional) Select the **Send keep alive message every 10m0s** option to check the connection at frequent intervals.
8. (Optional) For TCP syslog, select the **Allow syslog message caching** option to cache events when the connection is disrupted and to send them once the connection is restored.

Note: UDP syslog messages do not have any state awareness and may be lost if the connection is interrupted.

9. To send a test message to verify that the configuration is successful, click **Send Test Message**.

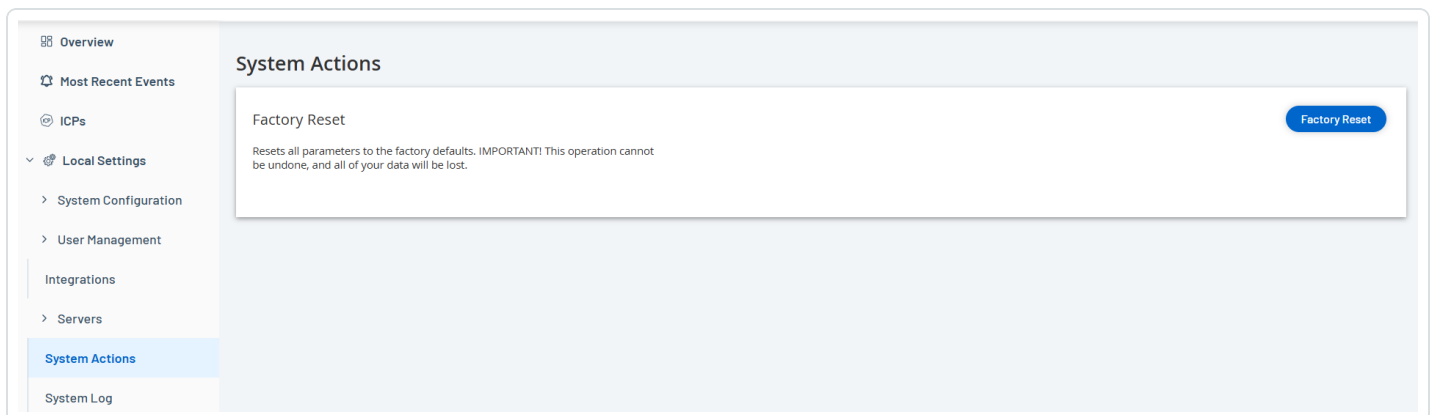
Verify if the message arrived. If the message did not arrive, then troubleshoot to discover the cause of the problem and rectify it.

10. 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
System Backup	<p>Back up your OT Security machine (except packet capture data). To restore the OT Security system from a backup file, contact Technical Support.</p> <p>Note: During the backup process, OT Security is unavailable to all users.</p>
Download Diagnostics Data	<p>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.</p>
Restart	<p>Restarts the OT Security EM. This is needed for activation of certain configuration changes.</p>
Disable	<p>Disables all monitoring activities. You can reactivate the monitoring activities at any time.</p>
Shut Down	<p>Shuts down the OT Security EM. To power on, press the Power button on the OT Security EM.</p>
Factory Reset	<p>Returns all settings to the factory default settings.</p> <p>Warning: You cannot undo this operation and you lose all data in the system.</p>

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 screenshot shows the Tenable OT Security EM System Log interface. The sidebar on the left contains navigation options: Overview, Most Recent Events, ICPs, Local Settings (expanded), System Configuration, User Management, Integrations, Servers, and System Actions. The main content area is titled 'System Log' and features a search bar and a 'Select Syslog server' dropdown. Below this is a table with three columns: Time, Event, and Username. The table lists several events, including successful logins, user creation, ICP connection status changes, and ICP deletion.

Time	Event	Username
Tuesday, Nov 12, 2024, 09:43:41 AM	Login by local user [redacted] succeeded	
Monday, Nov 11, 2024, 05:37:44 PM	Login by local user "[redacted]" succeeded	
Monday, Nov 11, 2024, 05:26:29 PM	New user created. Username: [redacted]	admin
Monday, Nov 11, 2024, 04:55:54 PM	ICP connection is up. Host: [redacted]	System
Monday, Nov 11, 2024, 04:50:06 PM	ICP disconnected, waiting for it to reconnect. [redacted]	System
Monday, Nov 11, 2024, 04:46:20 PM	ICP deleted. Host [redacted], Name: [redacted]	admin
Monday, Nov 11, 2024, 04:45:01 PM	Login by local user "admin" succeeded	
Monday, Nov 11, 2024, 04:43:35 PM	ICP connection is up. Host: [redacted]	System
Monday, Nov 11, 2024, 04:43:35 PM	ICP paired successfully. Host: [redacted]	admin
Monday, Nov 11, 2024, 04:43:33 PM	Em-Icp Pairing Permissive Mode turned on	admin

The following information is available for each logged event:

Parameter	Description
Time	The time and date when the event occurred.
Event	A brief description of the event.
Username	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.

API Keys



You can generate API keys to pair an ICP with the EM. For information about how to pair an ICP, see [Pair ICP with Enterprise Manager](#).

To generate API keys in OT Security EM:

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

The **API Keys** page appears.

2. In the upper-right corner, click **Generate Key**.

The **Generate Key** panel appears.

3. In the **Expiration Period** box, select the number of days after which the API key can age out.
4. In the **Description** box, type a description for the API key.
5. Click **Generate**.

The **Generate Key** panel displays the ID and API Key.

6. Click the copy button to copy the API key.

7. Click **Done**.

OT Security EM displays new API key in the API Keys table.

Certificates

The HTTPS certificate ensures the system uses a secure connection to the OT Security EM appliance and server. The initial certificate ages out after two years. You can generate a new self-signed certificate at any time. The new certificate is valid for one year.

To generate a certificate:

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

The **Certificates** page appears.



Certificates Actions ▾

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 Security
ISSUED BY	Tenable OT Security
ISSUED ON	Nov 8, 2023
EXPIRES ON	Nov 7, 2025
CERTIFICATE FINGERPRINT	

Generate Self-Signed Certificate

Upload Certificate

Download Certificate

- From the **Actions** menu, select **Generate Self-Signed Certificate**.

The **Generate Certificate** confirmation window appears.

- Click **Generate**.

OT Security EM generate the self-signed certificate, which appears on the **Certificates** page.

Actions on Certificates

You can do the following actions on the **Certificates** page:

Upload a Certificate

To upload a certificate:

- Go to **Local Settings > System Configuration > Certificates**.

The **Certificates** window appears.

- From the **Actions** menu, select **Upload Certificate**.

The **Upload Certificate** panel appears.

- In the **Certificate File** section, click **Browse** and navigate to the certificate file you want to upload.
- In the **Private Key File** section, click **Browse** and navigate to the private key file you want to upload.
- In the **Private Key Passphrase** box, type the private key passphrase.
- Click **Upload**.

OT Security EM uploads the certificate.



Download Certificate

- To download the certificate, click **Actions** > **Download Certificate**.

OT Security EM downloads the certificate to your system.



Revision History

Product version: 4.0

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
1.6	January 05, 2024	Updated for version 3.17
1.7	March 15, 2024	Updated for version 3.18
1.8	July 30, 2024	Updated for version 3.19