MXsecurity User Manual

Version 5.0, July 2025

www.moxa.com/product

MXsecurity User Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Trademarks

Disclaimer

- Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.
- Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.
- Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.
- This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. Introduction

MXsecurity is a management platform that provides centralized visibility and security management to easily monitor and identify cyberthreats and prevent security misconfigurations to create a robust threat defense. This industrial network security management suite translates complex network activity and threat intelligence into real-time visibility of cybersecurity statuses and actionable management for better detection and reaction against cyberthreats. With real-time dashboards, MXsecurity helps users track and react to OT network security events more efficiently.

Key Features

Centralized Management

Manage and monitor your secure router from one central location for better administration and maintenance. Devices can also be managed in groups based on geographic location, function, or responsibility to increase management efficiency.

Unified, Error-free Mass Deployment

Human error can lead to costly security breaches. Unified deployment of firewall policies, firmware upgrades, configuration files, and IPS signature updates prevents configuration errors and ensures your network is protected with the latest security intelligence.

Real-time Visibility and Monitoring

MXsecurity provides at-a-glance visibility, showing real-time network activity and threat analysis through highly customizable interactive widgets and a flexible dashboard.

Event Logs and Alert Notifications

MXsecurity automatically aggregates and monitors security logs at the appliance level and supports customizable instant real-time alerts for more efficient monitoring and faster troubleshooting.

Interactive Map View

MXsecurity features a map view which shows the real-time GPS location of the secure router. The map function is particularly useful to locate the secure router when it is used in mobile applications where the device is installed on moving equipment.

Comprehensive Reports

MXsecurity supports comprehensive reports for the OnCell Series, making it easier for administrators to conduct device audits and manage cellular signal and data usage. Additionally, the scheduling feature enables users to set up periodical reports that are automatically generated and sent to specified recipients.

System Requirements

The computer that MXsecurity is installed on must satisfy the following system requirements. The system requirements depend on the number of nodes that will be managed through MXsecurity.

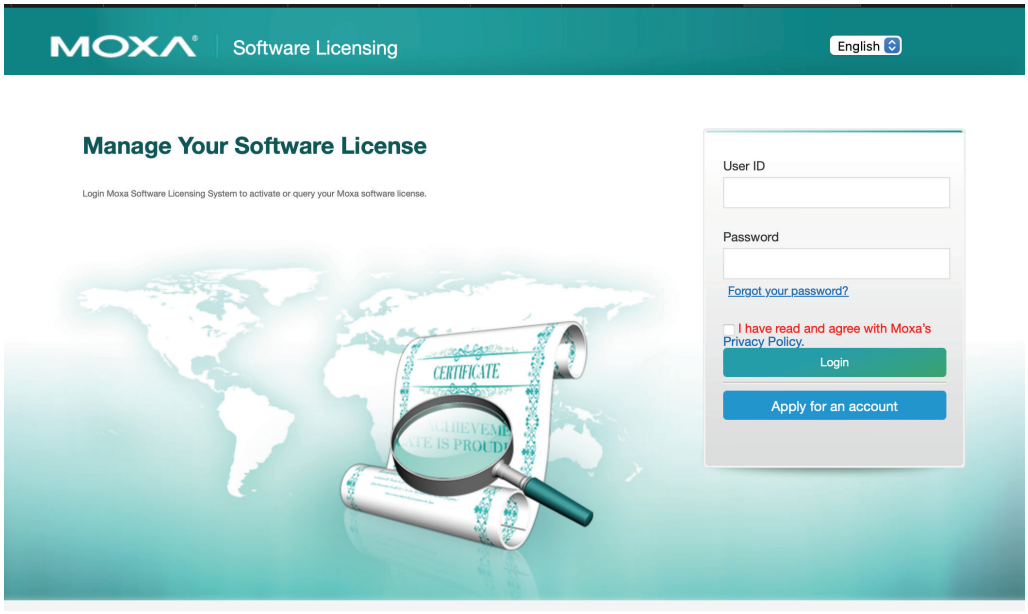
CPU (virtual cores)	4
RAM	8 GB
Hard Disk Space	64 GB
Supported Virtual Machines	VMWare ESXi 6.x or above, VM Workstation 14 or above

Downloading MXsecurity

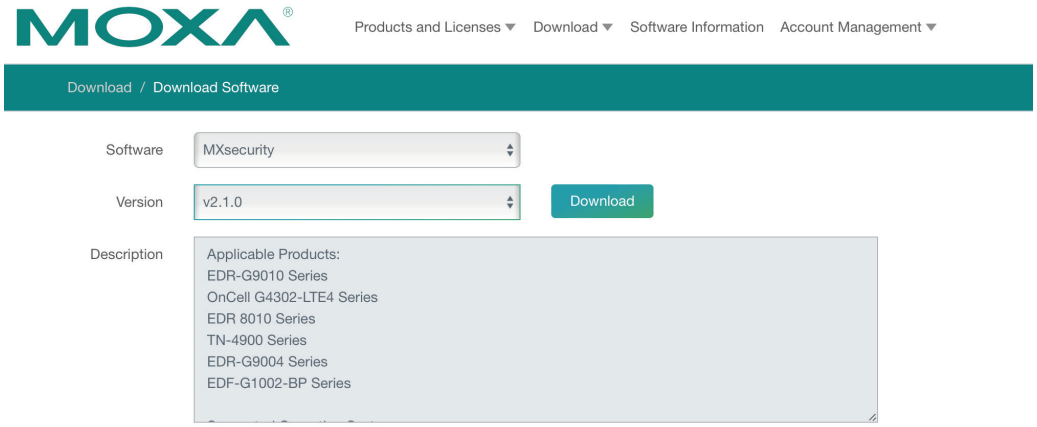
This section describes how to download the MXsecurity image file from the Moxa Software License site.

Steps:

1. Open a web browser and go to https://netsecuritylicense.moxa.com.
2. Log in to the Software License site using your Moxa account.



3. In the top toolbar, navigate to **Download > Download Software**.
4. Select **MXsecurity** and the image version.
   A changelog for each version is provided in the Description field.



5. Click **Download**.

Setting Up the Virtual Machine

Installing MXsecurity on a VMware Workstation

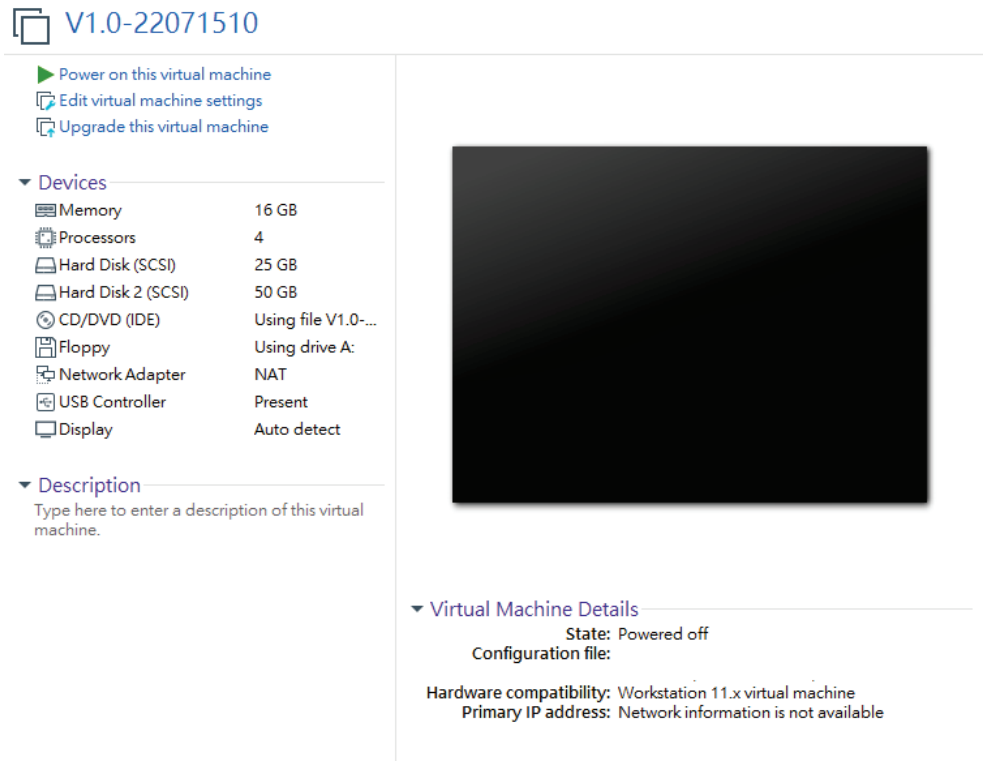
This section describes how to deploy MXsecurity to a VMware Workstation system.

Prerequisites

- The OVA packages provided by Moxa must be available and accessible to the VMware Workstation.
- VMware Workstation 14 or later is required.

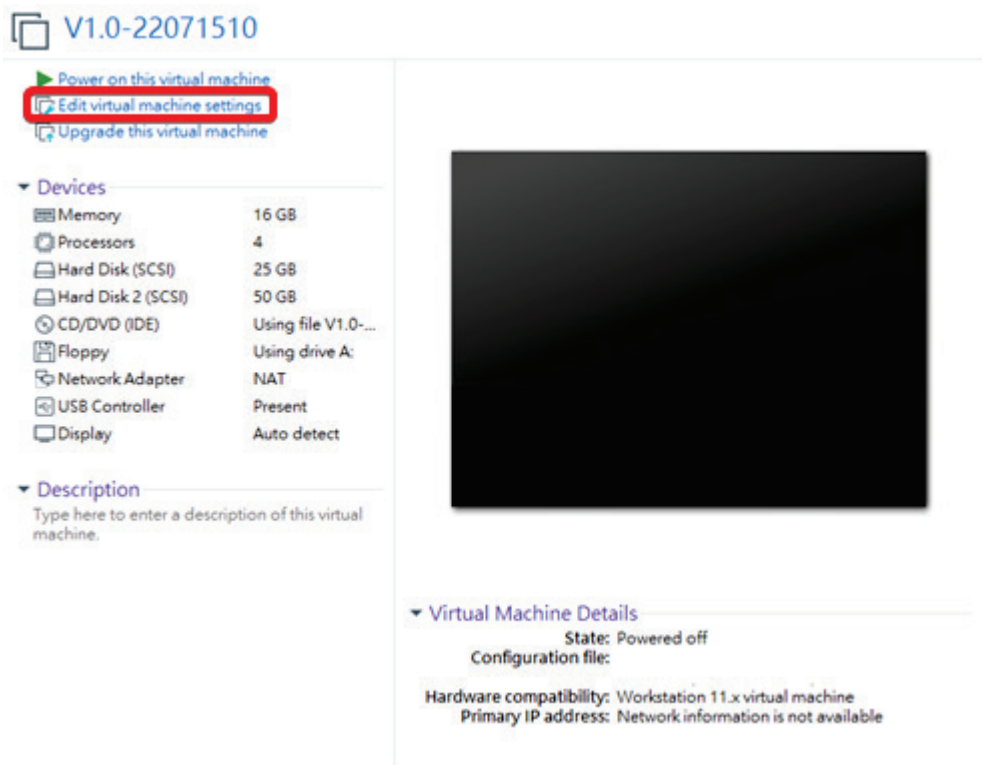
Steps:

1. Start the VMware Workstation.
2. Go to **File > Open** in the menu bar.
3. Select the MXsecurity VM image file (*.ova) from your localhost file path and click **Open**.
4. Specify the name and the storage path for the new virtual machine and click **Import**.
5. Check the detailed VM information of the imported MXsecurity VM.

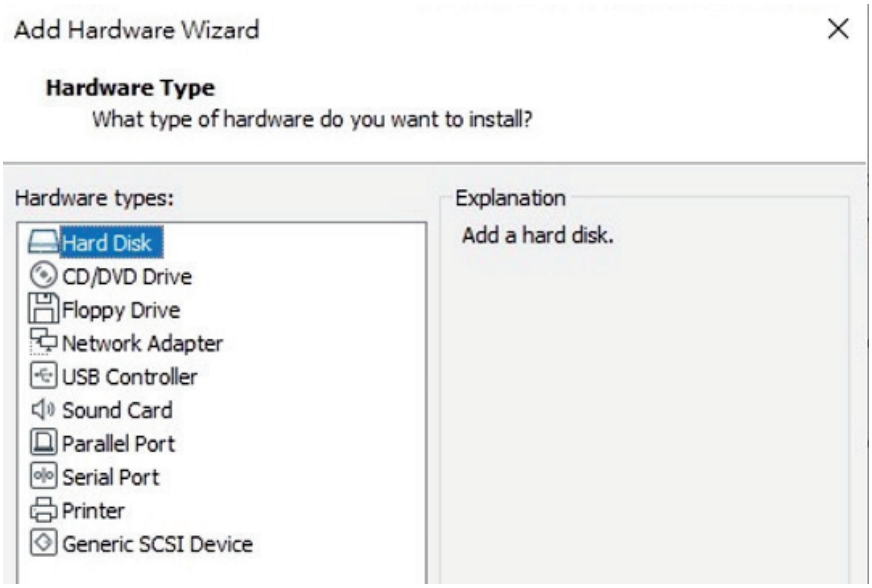


6. Add an external disk. MXsecurity requires one external disk with at least 20 GB of available storage, otherwise MXsecurity will not be able to finish initialization and the boot process will not be completed. The external disk is used to store the system configurations and event logs. You may attach the external disk of a terminated MXsecurity instance here instead of adding a new disk if you want to migrate the configurations and logs of the terminated instance to the new MXsecurity instance.

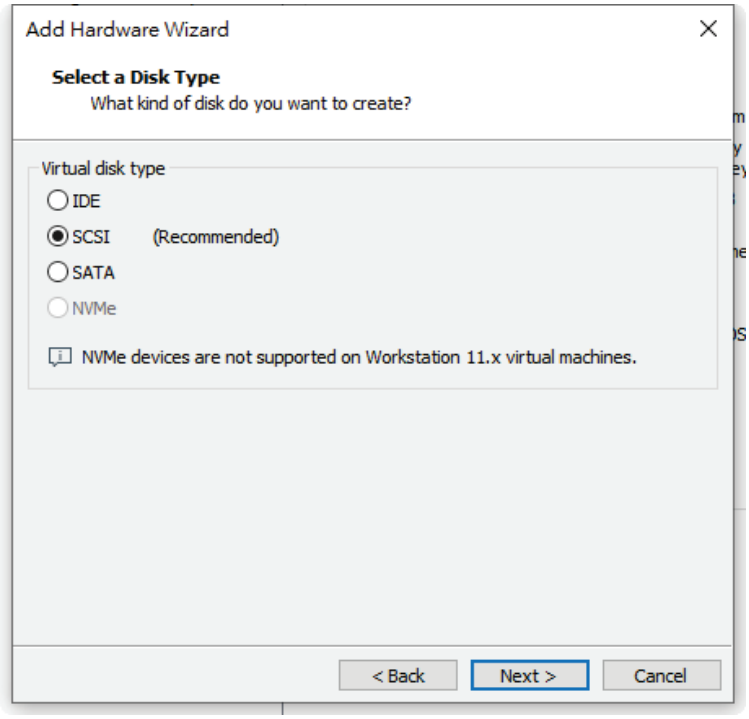
   a. Click **Edit virtual machine settings**.



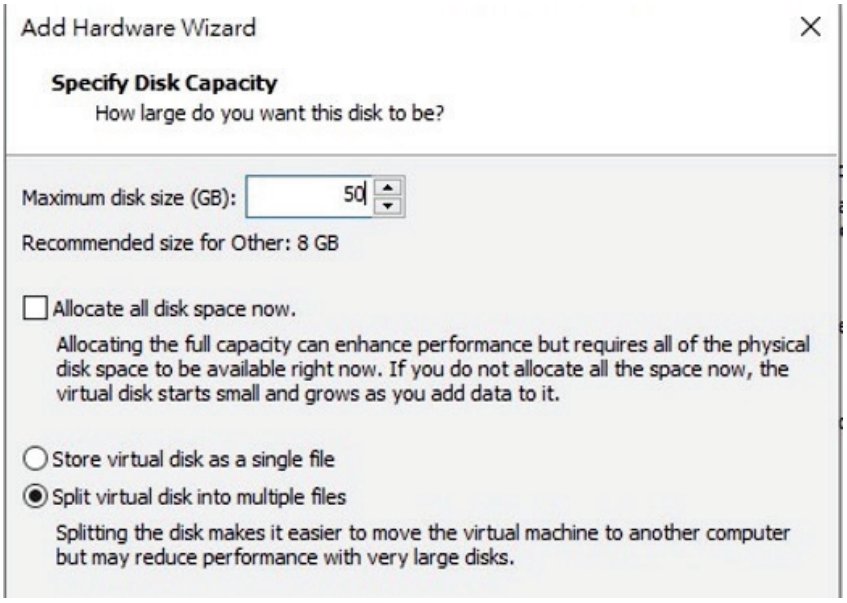
b. Click **Add**, then choose **Hard Disk**.



c. Select a disk type and click **Next**.



d. Set the disk space of the new hard disk. You can configure the external disk size depending on the number of logs to be stored.



e. Select the path to store the disk.

f. Click **Finish**.

g. **(Optional)** If necessary, you can increase the disk size to hold a larger number of MXsecurity logs:

   i. Power off the MXsecurity instance.

   ii. Increase the external disk size based on your requirements.

   iii. Power the MXsecurity instance back on.

7. **(Optional)** Adjust your MX MXsecurity instance to use proper resource configurations (Minimum: 4 CPU cores, 8 GB of memory).

   a. Click **Edit virtual machine settings**.

   b. Configure the amount of memory.

   c. Configure the number of CPU cores.

8. **(Optional)** Depending on your network environment, change the network adapter setting from 'NAT' to 'Bridged' if necessary.
   a. Right-click the MXsecurity VM icon and select **Settings**.
   b. Select **Network Adapter** and change the default setting from **NAT** to **Bridged**.
9. Boot the MXsecurity VM. The MXsecurity instance will initialize.

Installing MXsecurity on a VMware ESXi System

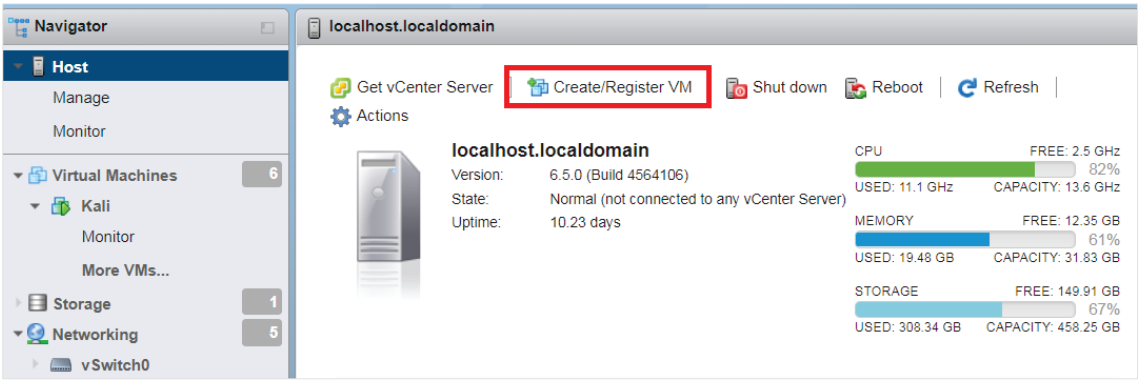
This section describes how to deploy MXsecurity to a VMware ESXi system.

Prerequisites

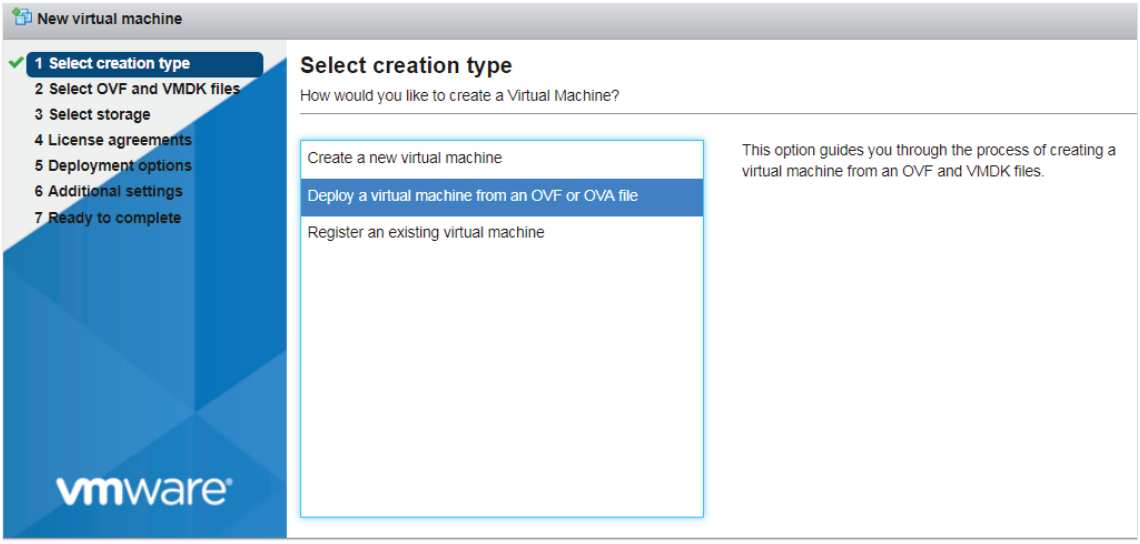
- The OVA packages provided by Moxa must be available and accessible to VMware ESXi.
- ESXi version 6 or above with the required specifications.
- The necessary networks have been properly created in ESXi.

Steps:

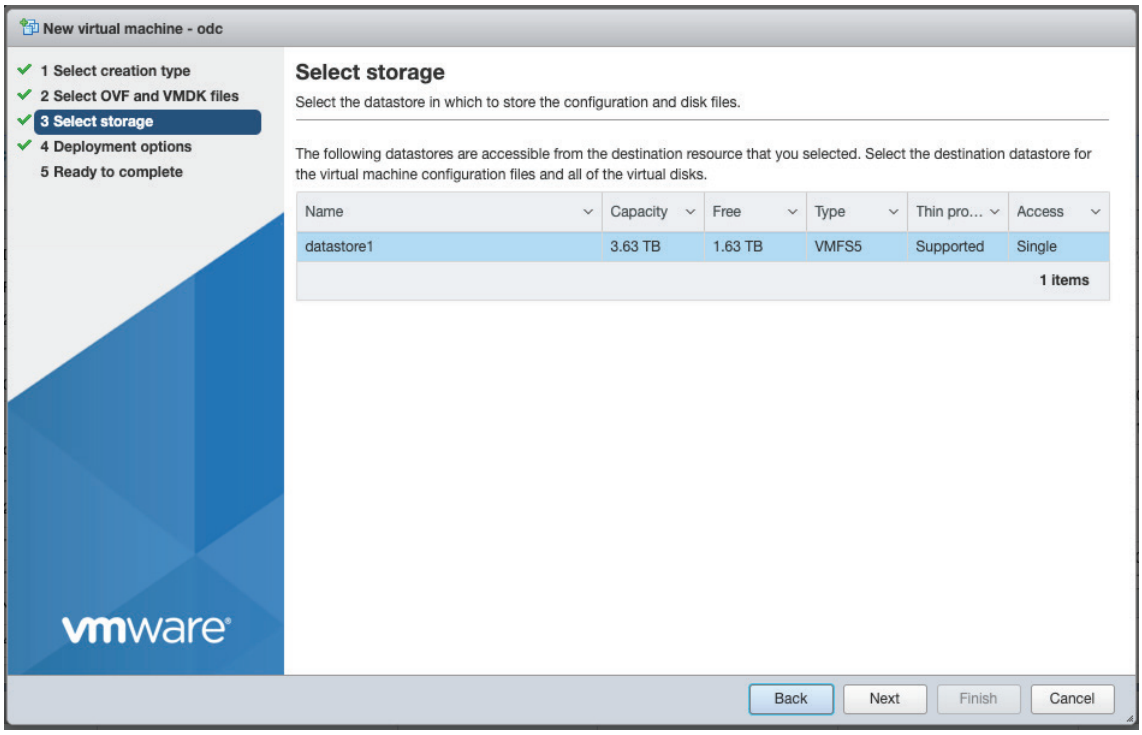
1. Log in to the VMware vSphere web client.
2. Under **Navigator**, click **Host** and then click **Create/Register VM**.



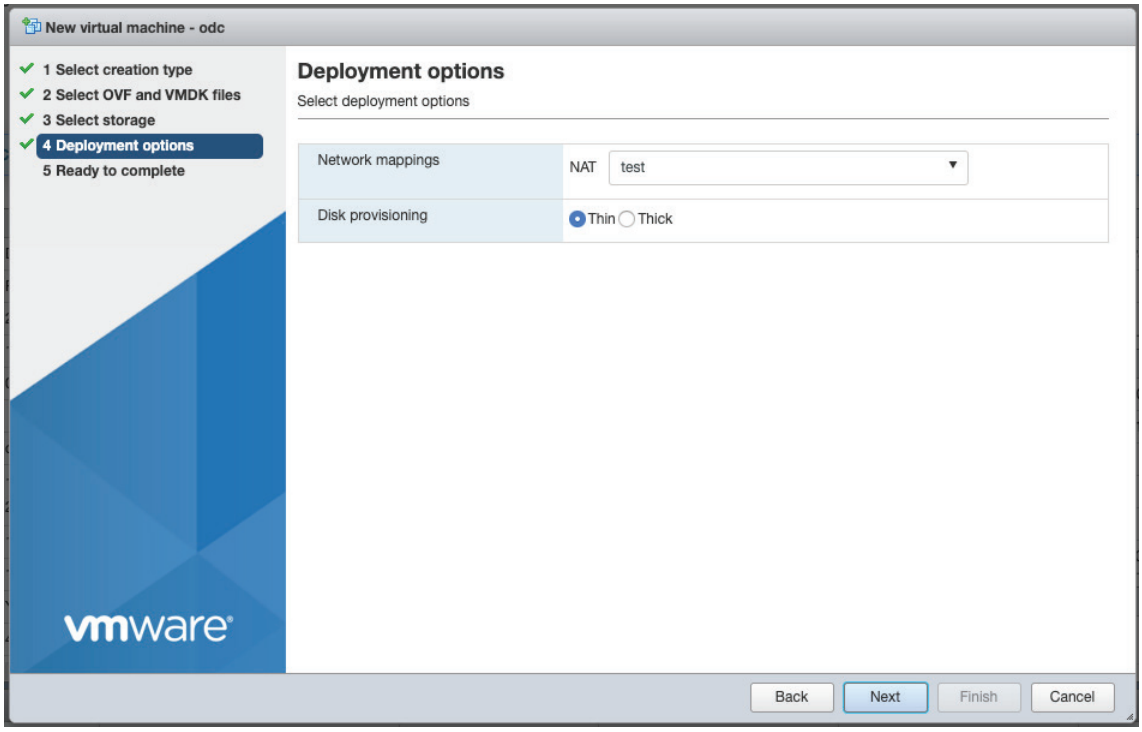
3. Select **Deploy a virtual machine from an OVF or OVA file**.



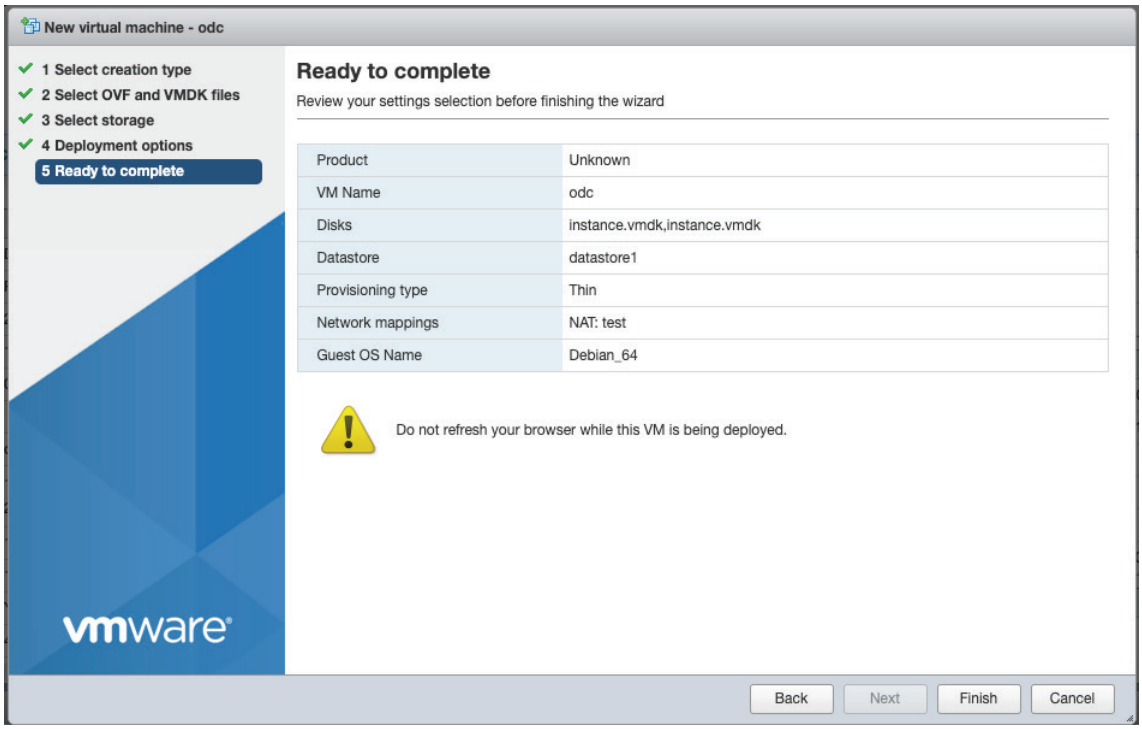
4. Enter a name for your MXsecurity instance and then select an MXsecurity image to upload.
5. Choose a storage location for the MXsecurity virtual machine.



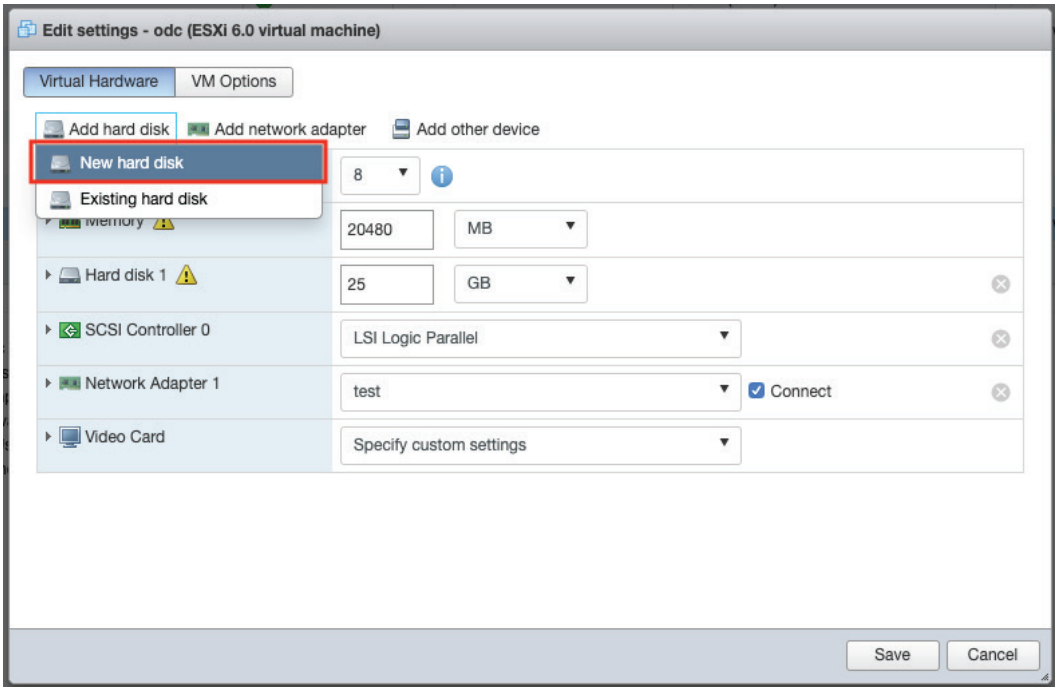
6. Select the deployment options.



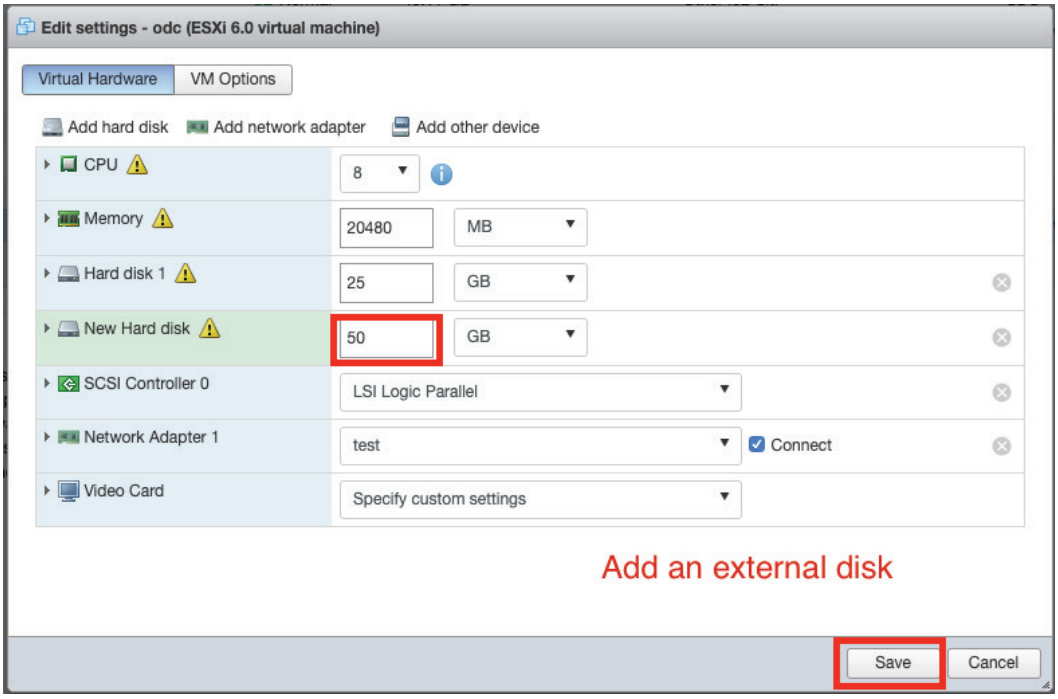
When you see the **Ready to complete** screen, click **Finish** to start the deployment.



7. Under the **Recent tasks** pane, you will see a progress bar indicating that the MXsecurity image is being uploaded. Wait until the upload has finished.
8. Add an external disk with at least 20 GB of available space to the MXsecurity instance:
   a. Power off the MXsecurity instance if it is powered on.
   b. Navigate to **Actions > Edit settings > Add hard disk > New hard disk**.



c. Set the disk space of the new hard disk and click **Save**.
You can configure the external disk size depending on the number of logs to be stored.

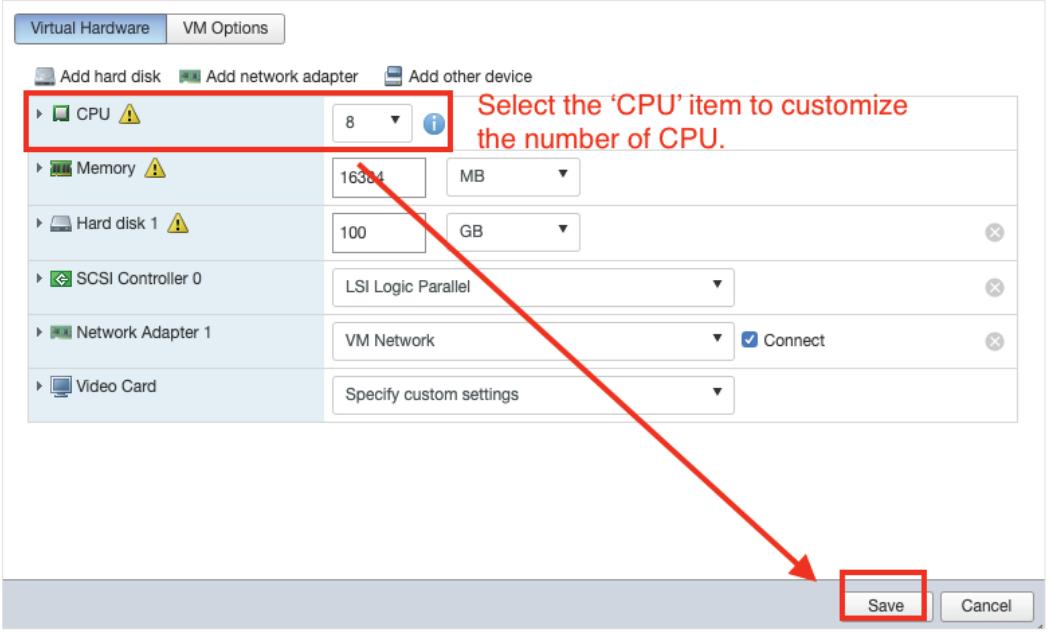


a. **(Optional)** If necessary, you can increase the disk size to hold a larger number of MXsecurity logs:
   i. Power off the MXsecurity instance.
   ii. Increase the external disk size based on your requirements.
   iii. Power the MXsecurity instance back on.

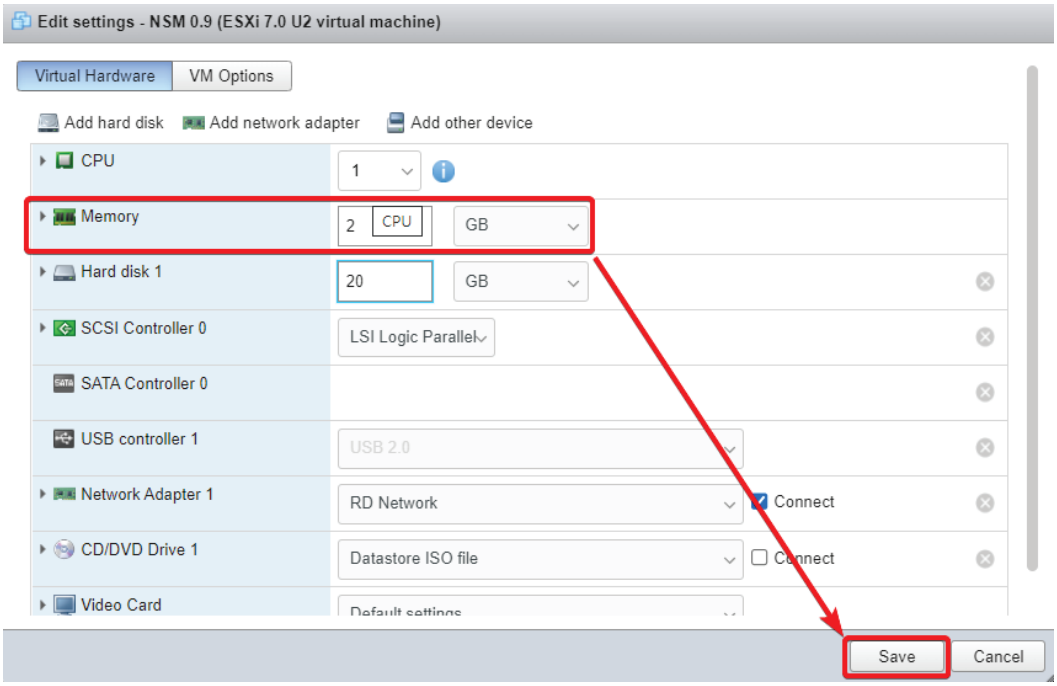
If you want to migrate the existing MXsecurity settings to the newly launched VM, please refer to Migration.

> **NOTE**
>
> The external disk is used to store the system configurations and event logs. You may attach the external disk of a terminated MXsecurity instance instead of adding a new disk if you want to migrate the configurations and logs of the terminated instance to the new MXsecurity instance.

9. Power on the VM.
10. **(Optional)** Adjust your MXsecurity instance to use proper resource configurations (Minimum: 8 core CPU, 8 GB memory).
    a. Shut down the instance of MXsecurity and click **Edit**.
       The **Edit settings** window appears.
    b. Configure the number of CPU cores.



c. Configure the amount of memory.



d. Click **Save**.

e. Boot the MXsecurity instance.

Configuring the MXsecurity system

Accessing the MXsecurity CLI

Steps:

1. Open the MXsecurity VM console.
2. Log in with username **admin** and password **moxa**.
3. Change the default password:

```
MXsecurity login: admin
Password:
You are required to change your password immediately (root enforced)
Changing password for admin.
(current) UNIX password:
New password:
```

The password must meet the following requirements:

- Minimum 8 characters long
- The new password cannot be the same as the old password
- The new password cannot contain the old password
- The password cannot be too simplistic or contain simple character sequences such as “abc”, “123456”, etc

b. Log in to the MXsecurity again with your new password.

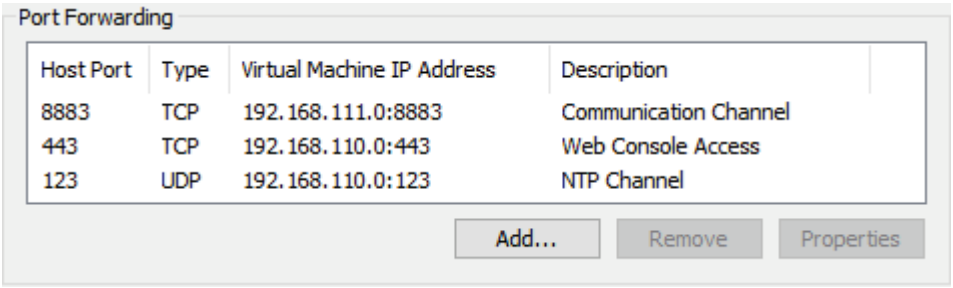
4. **(Optional)** After logging in to the MXsecurity, type the “help” command to see a list of available commands.

```
MXsecurity# help
  interface - Network operation
  resolve   - DNS operation
  ping      - Ping a host IP address
  reboot    - Reboot the MXsecurity
  poweroff  - Power off the MXsecurity
  version   - The version and default value of MXsecurity
  help      - Command line help
  exit      - Exit the terminal
```

Getting the IP Address of the MXsecurity Instance

Steps:

1. Enter the **interface ls** command to get the IP address of the MXsecurity instance.
2. If your VMware network adapter setting is using NAT, you will need to create port forwarding rules to allow traffic to pass from connected devices to MXsecurity.
   a. Navigate to **Edit > Virtual Network Editor**, select the right network subnet and click **NAT Settings**.
      i. To allow users to configure the devices through MXsecurity including all configuration settings and commands and upload logs, forward packets from the host TCP port 8883 to the MXsecurity server IP TCP port 8883.
      ii. To allow devices to synchronize their system time with MXsecurity, forward packets from the host UDP port 123 to the MXsecurity server IP UDP port 123.
      iii. To access the web management console, forward packets from host TCP port 443 to the MXsecurity server IP TCP port 443.



> **NOTE**
>
> Port 8883, 123, and 443 are the default port numbers. If you change the port numbers, make sure to use the correct port numbers in the NAT settings.

Configuring the IP Address Settings

You can manually configure the IP address if necessary.

Steps:

1. Use the **interface --update** command to update the settings of an existing network interface. For example, the following command sets the interface "eth0" to the static IP address 192.0.2.4/24 with the gateway IP address 192.0.2.254.

   ```
   $ interface --update eth0 --method static --address 192.0.2.4 --gateway
   192.0.2.254 --netmask 255.255.255.0
   ```

2. Confirm the network interface settings are correct and execute the --**restart [interface]** command to have the new settings take effect.

   ```
   $ interface --restart eth0
   ```

3. Execute the **interface --ls** command to view the network interface settings.

   ```
   $ interface --ls
   ```

4. Use the **resolve --add** command to add a DNS server. For example, the following command adds "8.8.8.8" to the DNS server list.

   ```
   $ resolve --add 8.8.8.8
   ```

5. Execute the **resolve --ls** command to view the DNS server settings.

   ```
   $ resolve --ls
   ```

6. Execute the **reboot** command to reboot the VM.

   ```
   $ reboot
   ```

This chapter provides information and instructions on how to migrate your MXsecurity data to a newer version of MXsecurity.

Migrating to a Newer Version of MXsecurity (VMware Workstation)

This section describes how to migrate to a newer version of MXsecurity with VMware Workstation.

NOTE

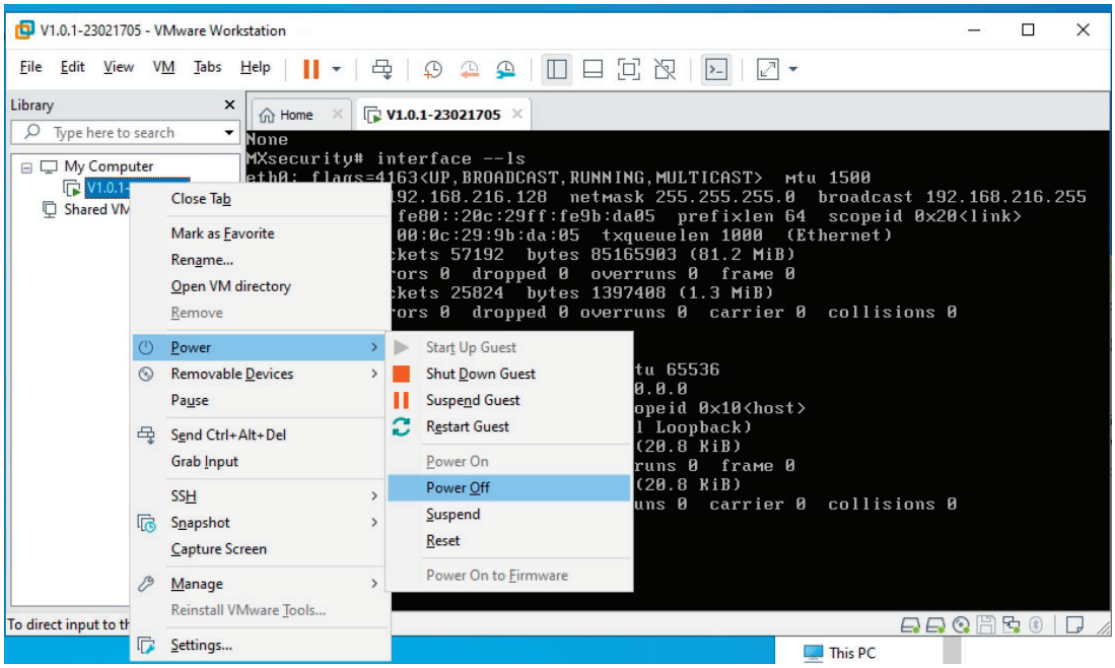
MXsecurity v1.1.0 has implemented enhanced connection security measures. To avoid issues, managed devices should be upgraded to a firmware version and MXsecurity Agent Package which is compatible with MXsecurity v1.1.0. The following device firmware versions are compatible with MXsecurity v1.1.0:

- EDR-G9010 Series FW v3.0 or higher, MXsecurity Agent Package v2.0.13 or higher
- EDR-8010 Series FW v3.0 or higher, MXsecurity Agent Package v2.0.13 or higher
- OnCell G4302 Series FW v3.0 or higher. MXsecurity Agent Package v2.0.13 or higher

If you have an older version of the MXsecurity Agent Package installed, you will need to manually upgrade it to v2.0.13 on the managed device first. To manually upgrade the software package, navigate to **System > System Management > Software Package Management > MXsecurity Agent Package** in the Secure Router's web interface.

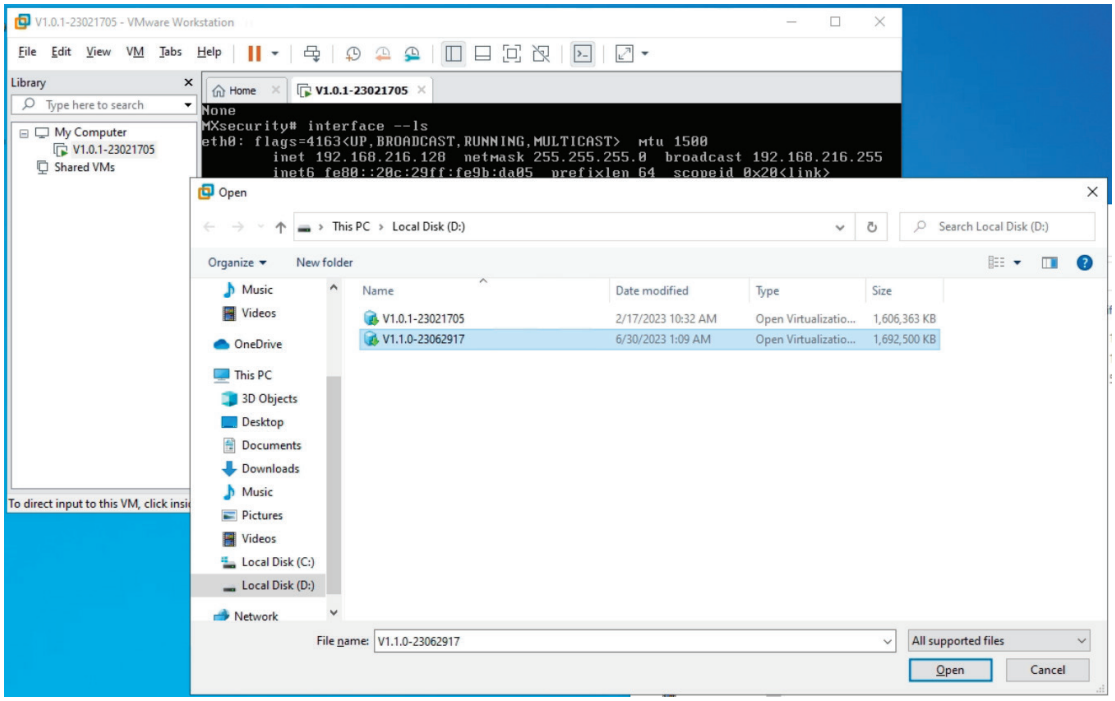
Steps:

1. Start the VMware Workstation.
2. Power off the MXsecurity instance.

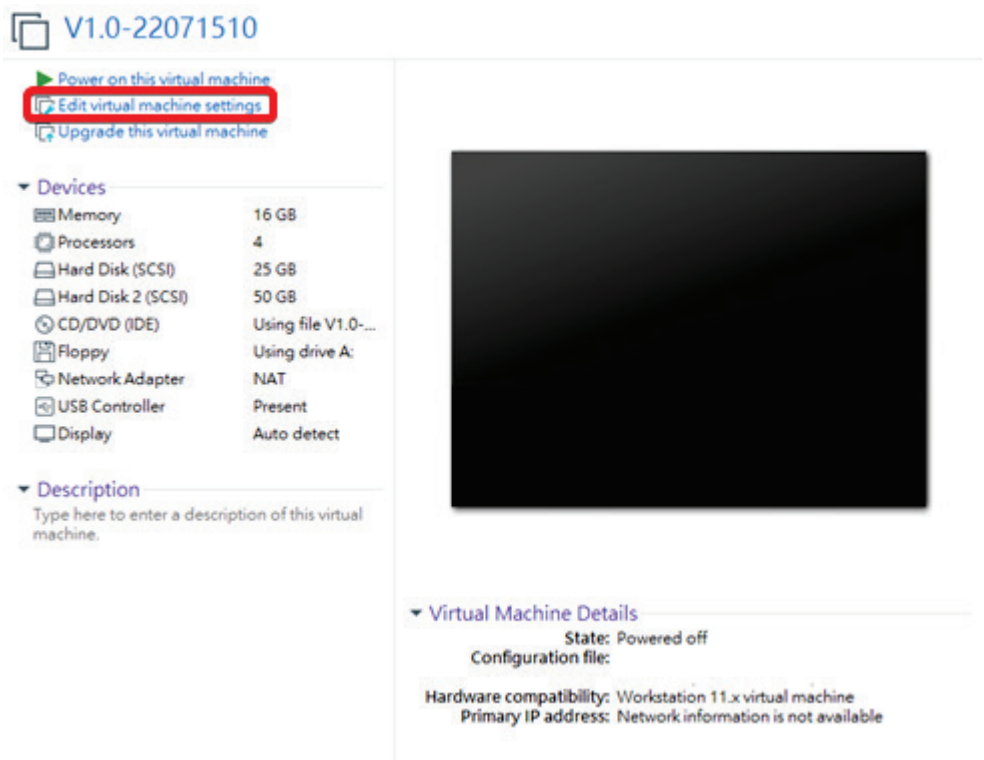


3. Go to **File > Open** in the menu bar.

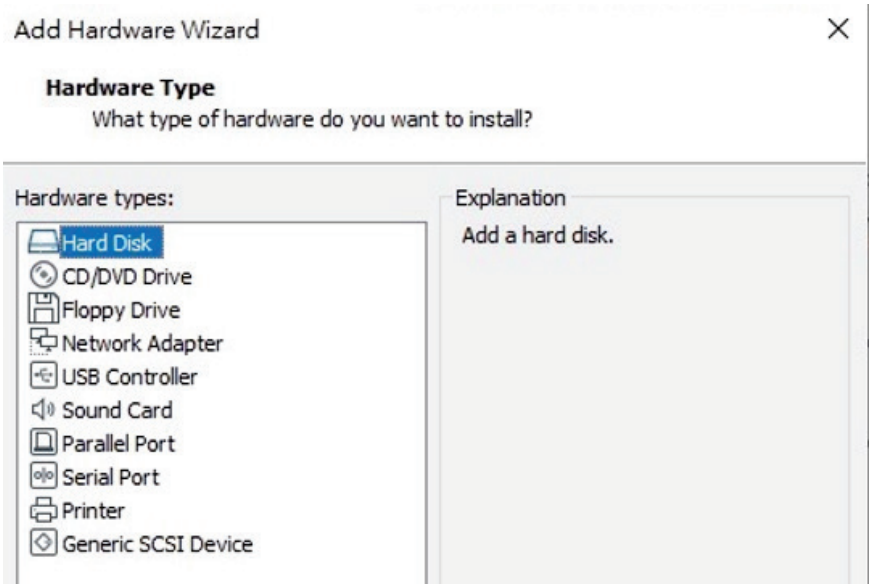
4. Select the VM image file (*.ova) of the new MXsecurity version from your localhost file path and click **Open**.



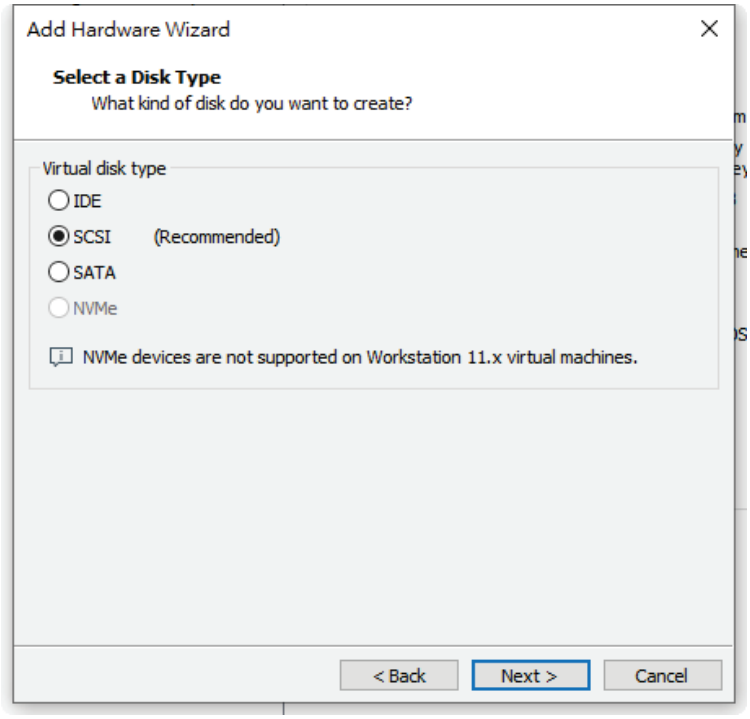
5. Add an existing Hard Disk.
   a. Click **Edit virtual machine settings**.



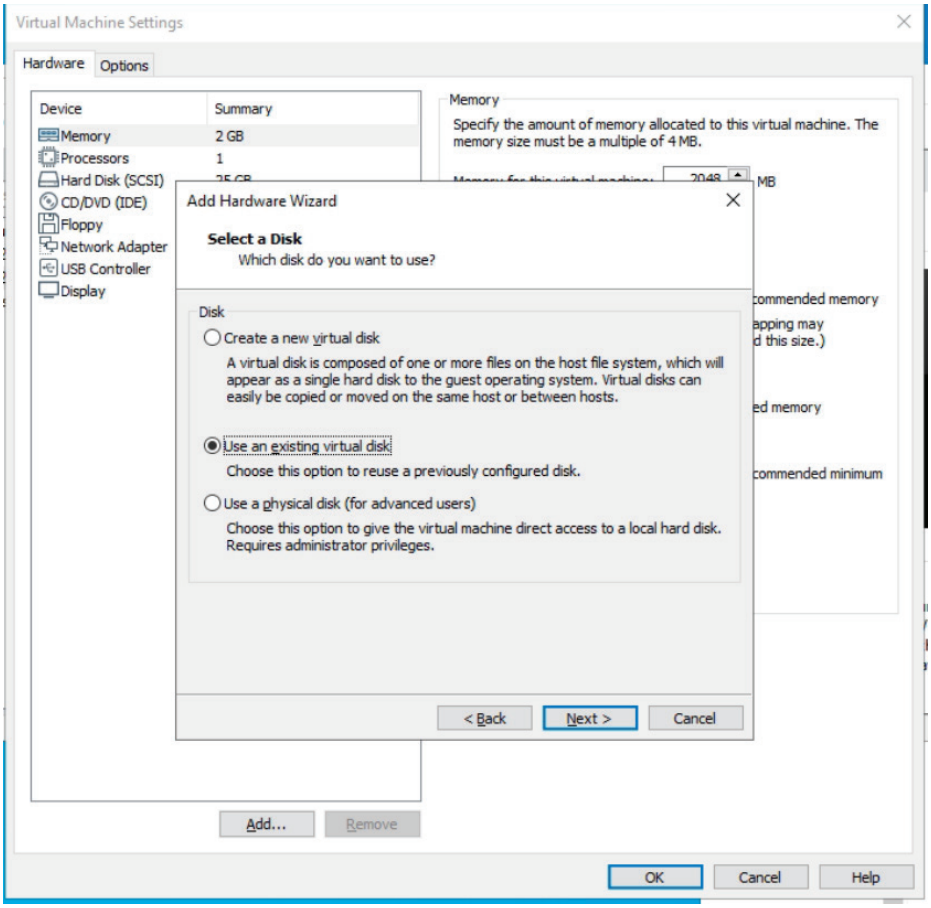
   b. Click **Add**, then choose **Hard Disk**.



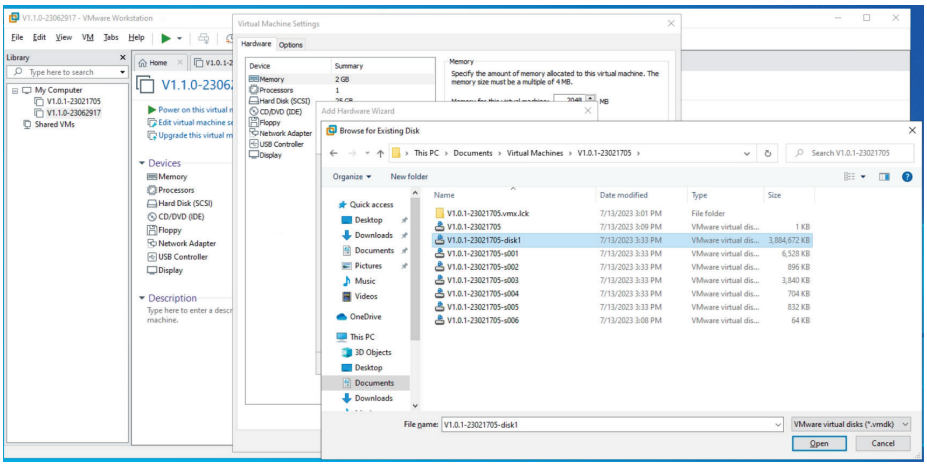
c. Select a disk type and click **Next**.



d. Select **Using an existing virtual disk** and click **Next**.



e. Navigate to the disk of the original MXsecurity instance and click **Open**.



6. Click **Finish**.

> ● **NOTE**
>
> After installing the new MXsecurity instance, you may need to reconfigure the IP address of the MXsecurity server. Refer to Configuring the IP Address Settings for instructions.

7. Log in to the MXsecurity web console and confirm the migration was successful.

Migrating to a Newer Version of MXsecurity (ESXi)

This section describes how to migrate to a newer version of MXsecurity with VMware ESXi.

NOTE

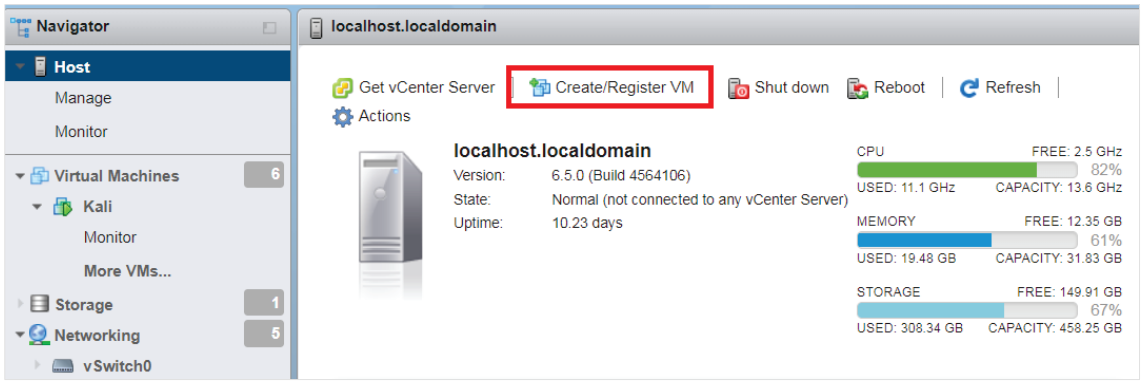
MXsecurity v1.1.0 has implemented enhanced connection security measures. To avoid issues, managed devices should be upgraded to a firmware version and MXsecurity Agent Package which is compatible with MXsecurity v1.1.0. The following device firmware versions are compatible with MXsecurity v1.1.0:

- EDR-G9010 Series FW v3.0 or higher, MXsecurity Agent Package v2.0.13 or higher
- EDR-8010 Series FW v3.0 or higher, MXsecurity Agent Package v2.0.13 or higher
- OnCell G4302 Series FW v3.0 or higher. MXsecurity Agent Package v2.0.13 or higher

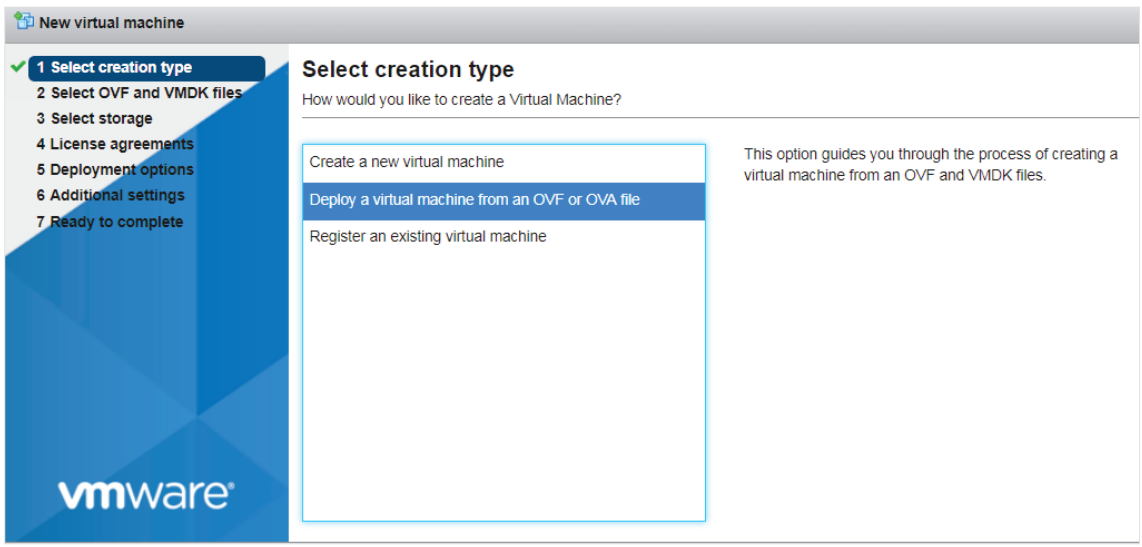
If you have an older version of the MXsecurity Agent Package installed, you will need to manually upgrade it to v2.0.13 on the managed device first. To manually upgrade the software package, navigate to **System > System Management > Software Package Management > MXsecurity Agent Package** in the Secure Router's web interface.

Steps:

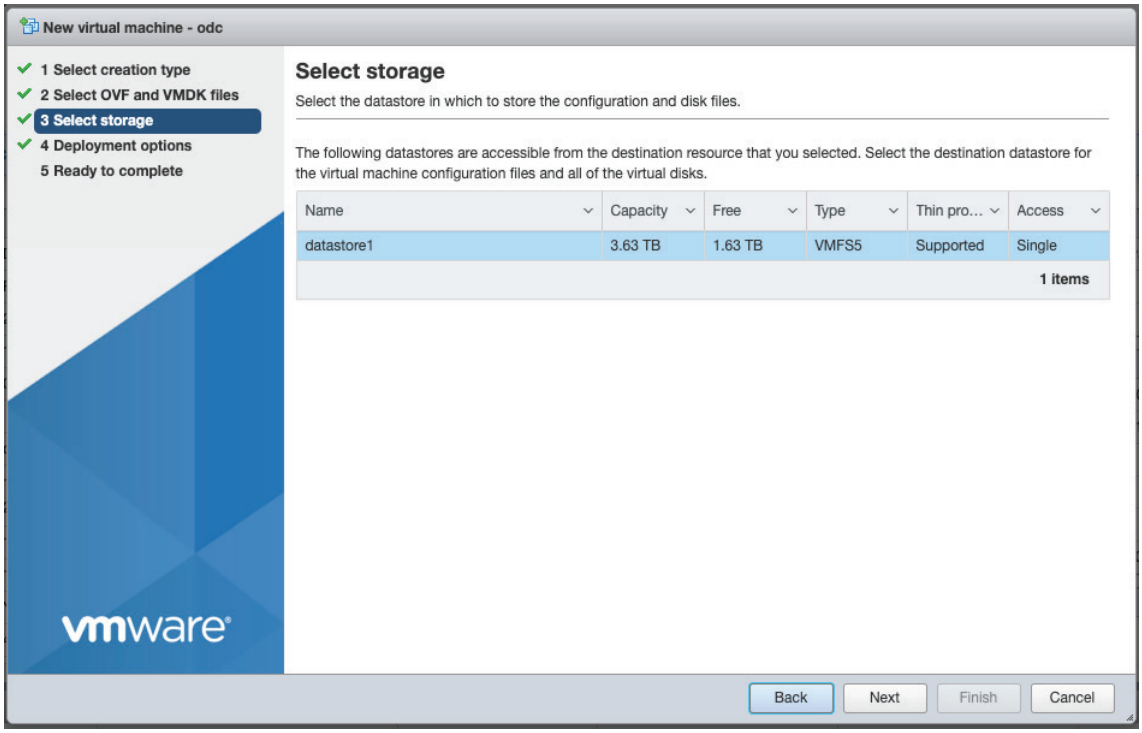
1. Start the VMware ESXi.
2. Power off the MXsecurity instance.
3. Under **Navigator**, click **Host** and then click **Create/Register VM**.



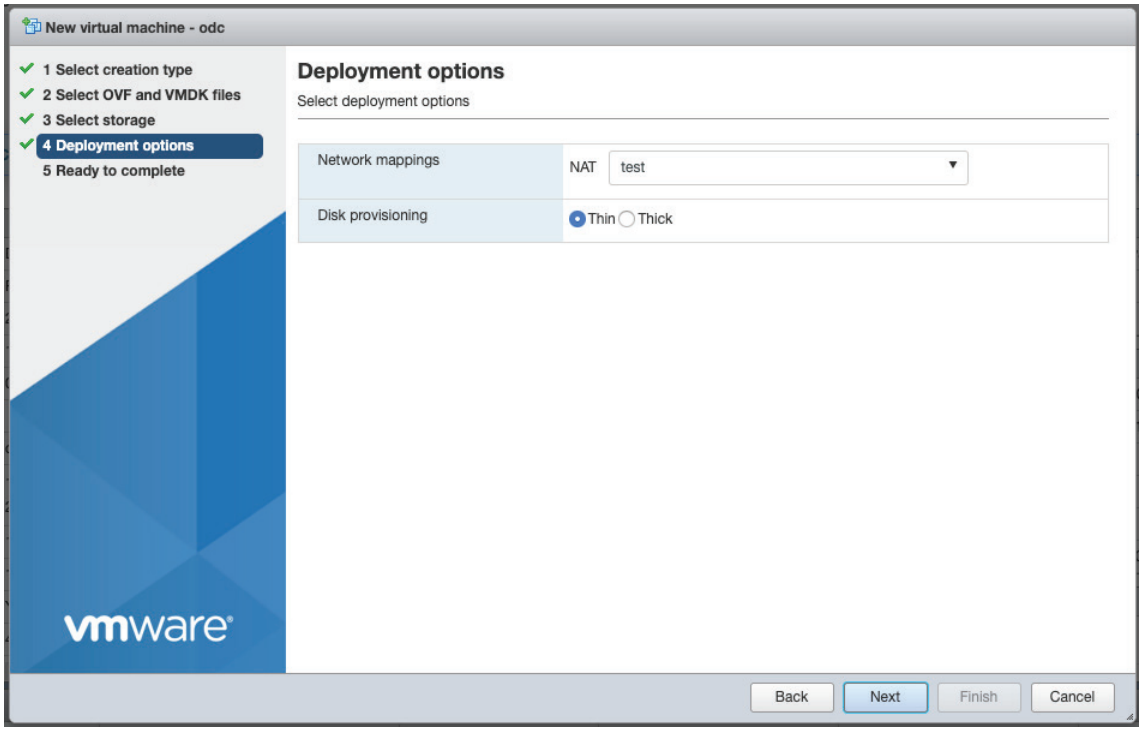
4. Select **Deploy a virtual machine from an OVF or OVA file**.



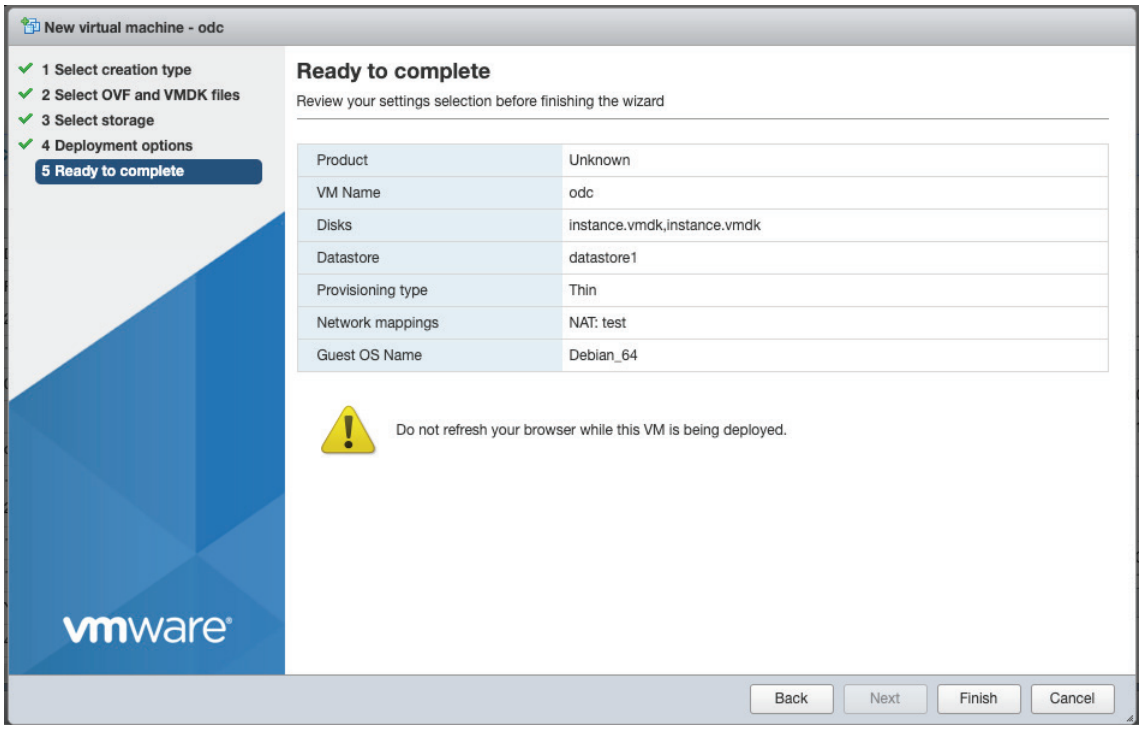
5. Enter a name for your MXsecurity instance and then the image file of the new MXsecurity version to upload.
6. Choose a storage location for the MXsecurity virtual machine.



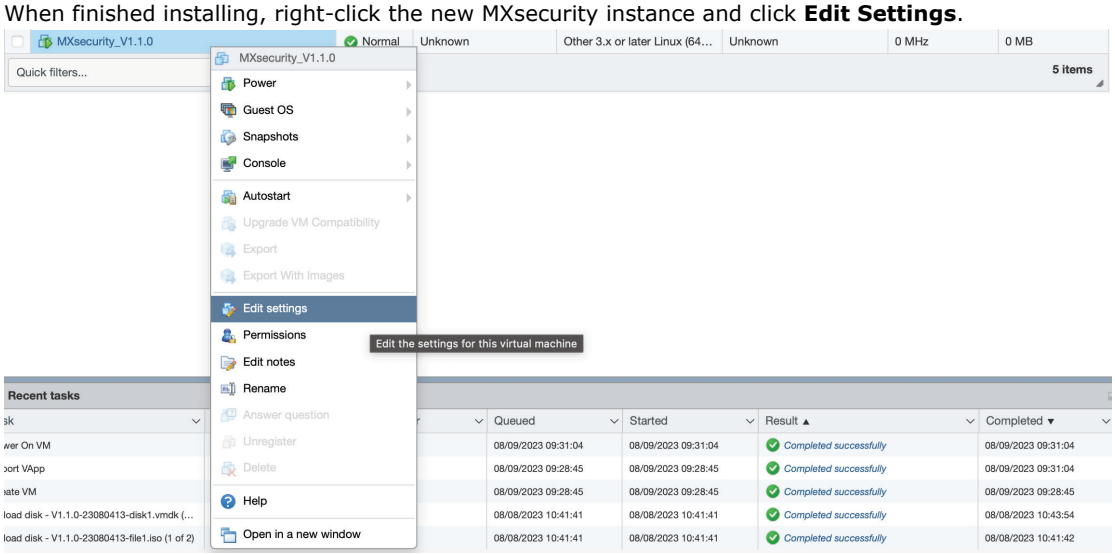
7. Select the deployment options.



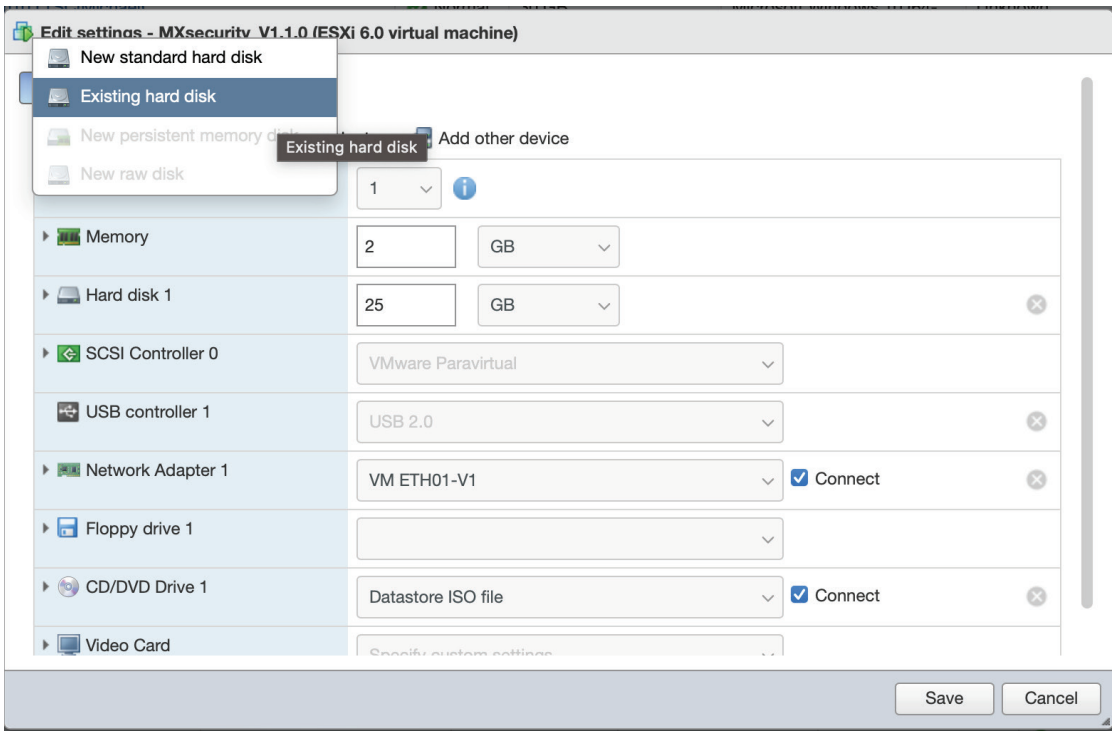
When you see the **Ready to complete** screen, click **Finish** to start the deployment.



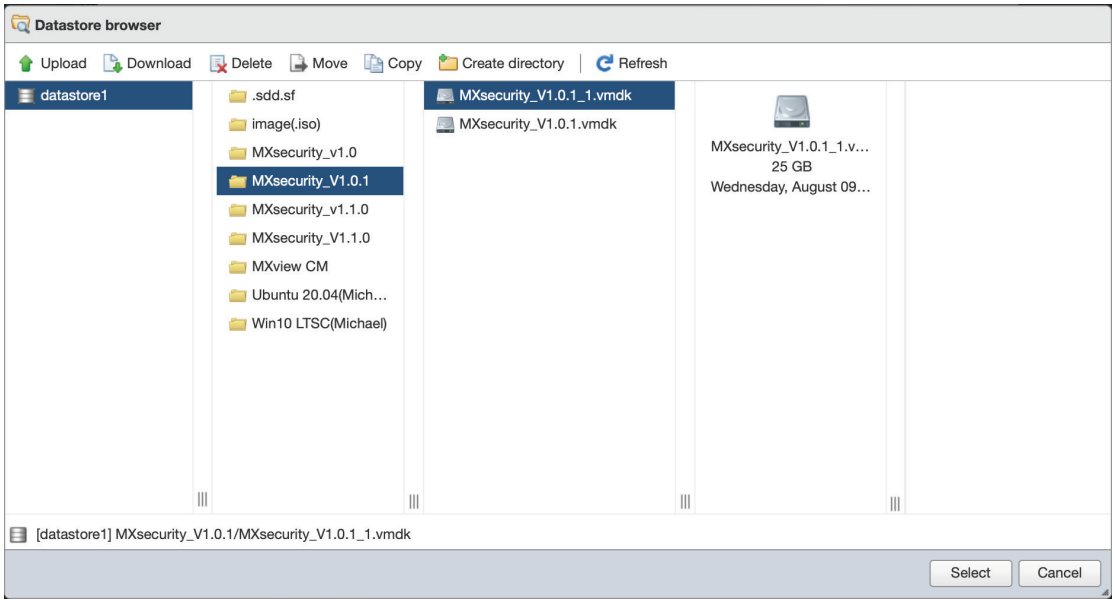
8. Under the **Recent tasks** pane, you will see a progress bar indicating that the MXsecurity image is being uploaded. Wait until the upload has finished.
9. When finished installing, right-click the new MXsecurity instance and click **Edit Settings**.



10. Click **Add Hard Disk > Existing hard disk**.



11. Navigate to the disk of the original MXsecurity instance and click **Select**.



12. Click **Save**.

> **NOTE**
>
> After installing the new MXsecurity instance, you may need to reconfigure the IP address of the MXsecurity server. Refer to Configuring the IP Address Settings for instructions.

13. Log in to the MXsecurity web console and confirm the migration was successful.

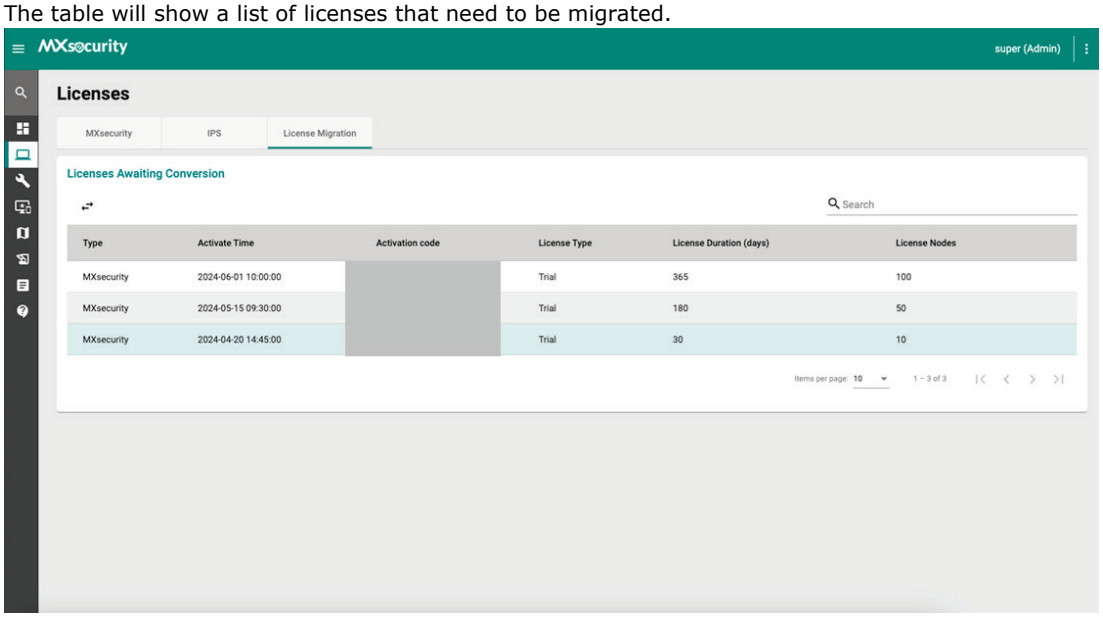
Migrating Licenses

MXsecurity v2.3.0 introduces a new license mechanism. As a result, users operating MXsecurity v2.2.0 or an earlier version must migrate all licenses when upgrading to v2.3.0.

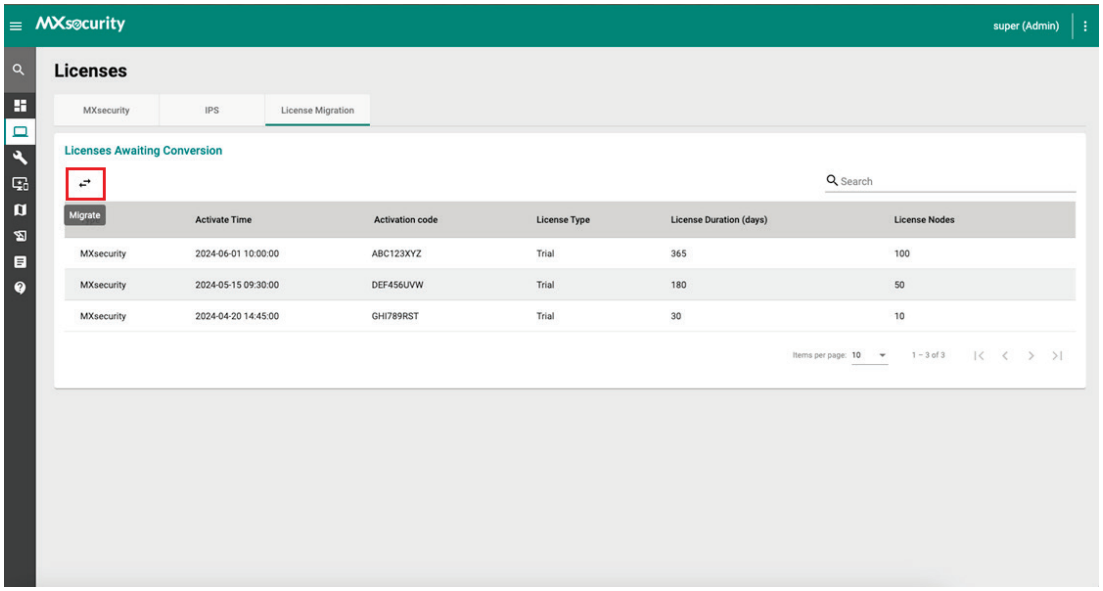
> **NOTE**
>
> To ensure optimal security and avoid compatibility issues, we strongly recommend upgrading MXsecurity to v2.3.0 and the firmware of MXsecurity devices to v3.19.0. Using older versions may lead to security vulnerabilities and limitations to certain functions.

Steps:

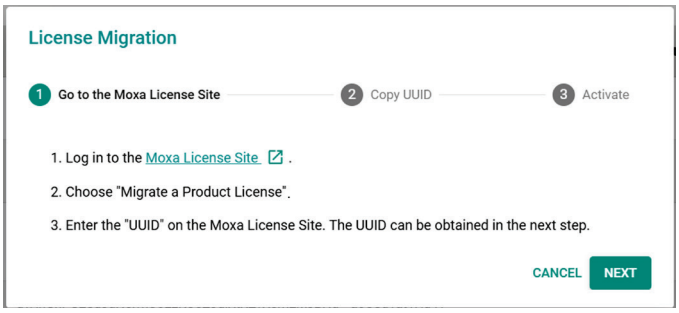
1. Upgrade MXsecurity to v2.3.0.
2. Log in to MXsecurity.
3. Navigate to **System > Licenses > License Migration**.
   The table will show a list of licenses that need to be migrated.



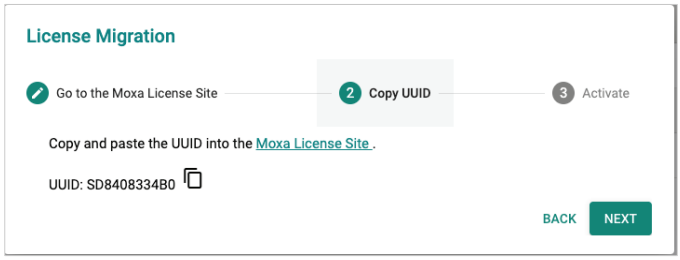
4. Click the ⇄ icon to start the license migration process.



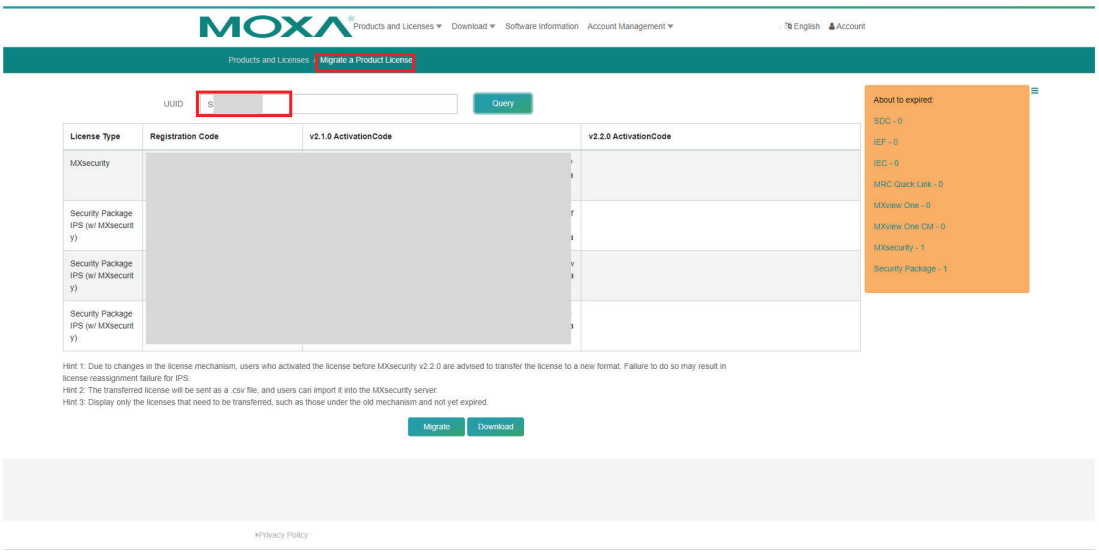
5. In the **License Migration** window, click the link to the **Moxa License Site** and click **NEXT**.
   This will open the Moxa license site in a new browser window.



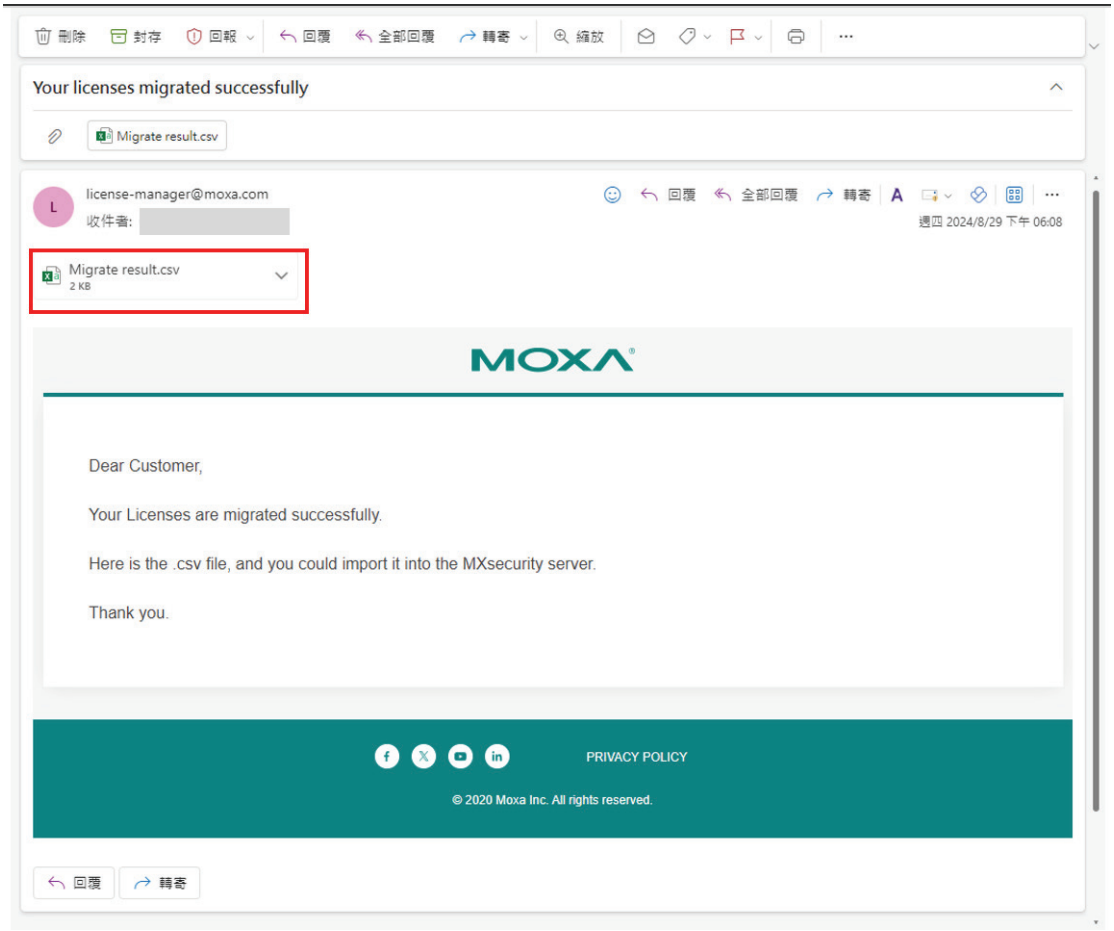
6. When prompted, log in to the Moxa license site using your Moxa account.
7. On the license site, navigate to **Products and Licenses > Migrate a Product License**.
8. In MXsecurity, copy the UUID and click **NEXT**.



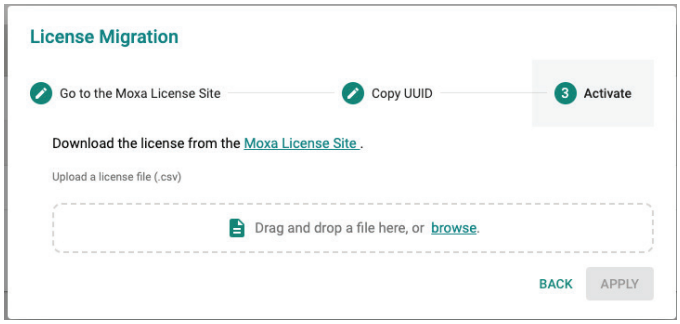
9. On the license site, enter the UUID and click **Query**.
   A list of all licenses that need to be migrated will show.
10. Click **Migrate** to start the migration process.
    When finished, the system will send the license migration results in CSV format to the email registered to your Moxa account.



11. Download the **Migrate result.csv** file from the email you received.



12. In MXsecurity, import the **Migrate result.csv** file and click **APPLY**.



13. Confirm the licenses were migrated successfully by confirming the **License Migration** tab is no longer visible.

4. Getting Started

This chapter describes how to get started with MXsecurity and perform the initial configuration.

Getting Started Task List

The Getting Started task list provides a high-level overview of all procedures required to get MXsecurity (MXsecurity) up and running as quickly as possible. Each step links to more detailed instructions later in the document.

1. Open the management console.
   For more information, see Opening the Management Console.
2. Change the administrator's default login name and password after logging in for the first time.
   For more information, see Changing Your Account Password.
3. Activate your product license.
   For more information, see Licenses.
4. Configure the system time.
   For more information, see Configuring the System Time.
5. Assigning policies to the device groups.
   For more information, see Device Group Management and Policy Profile Management.
6. Creating user accounts.
   For more information, see User Accounts

Opening the Management Console

MXsecurity provides a built-in management console that you can use to configure and manage the product. View the management console using a web browser.

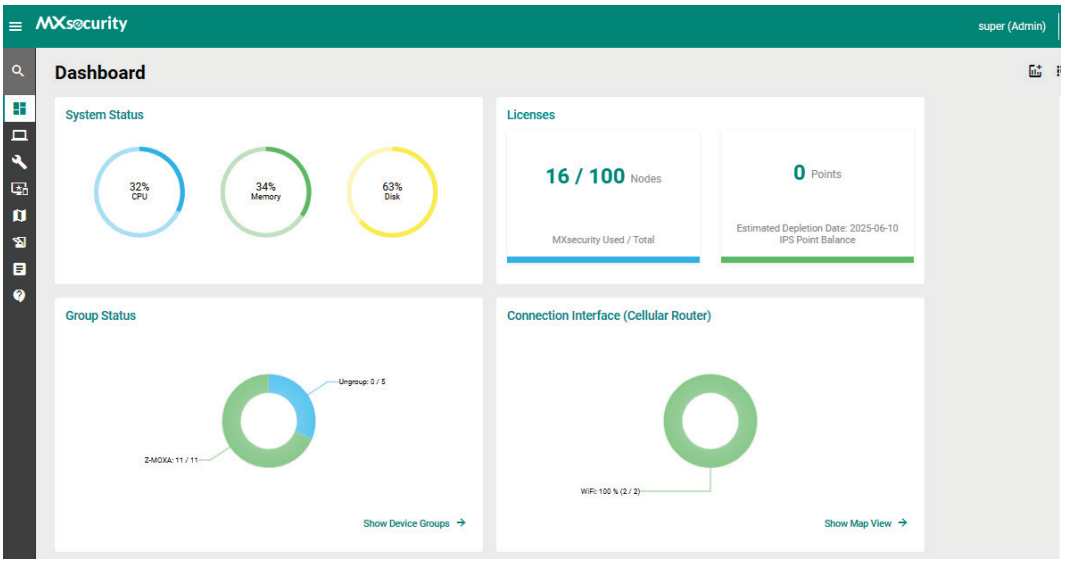
> **NOTE**
>
> View the management console using Google Chrome version 103 or later.

Steps:

1. In a web browser, type the address of the MXsecurity in the following format:
   `https://<target server IP address or FQDN>`
   The login screen will appear.
2. Enter your username and password.
   If you are logging in for the first time, use the default administrator credentials:
   - Username: `admin`
   - Password: `moxa`
3. Click **LOG IN**.
   If this is your first time logging in, the Change Password window will appear.

> **NOTE**
>
> You must change the default login name and password before you can access the management console.

a. Enter your new login details.
   i. Current Password
   ii. New Password
   iii. Confirm New Password
b. Click **Confirm**.
   You will be automatically logged out of the system. The login screen will appear again.
c. Log in again using your new credentials.
   The dashboard screen will appear.

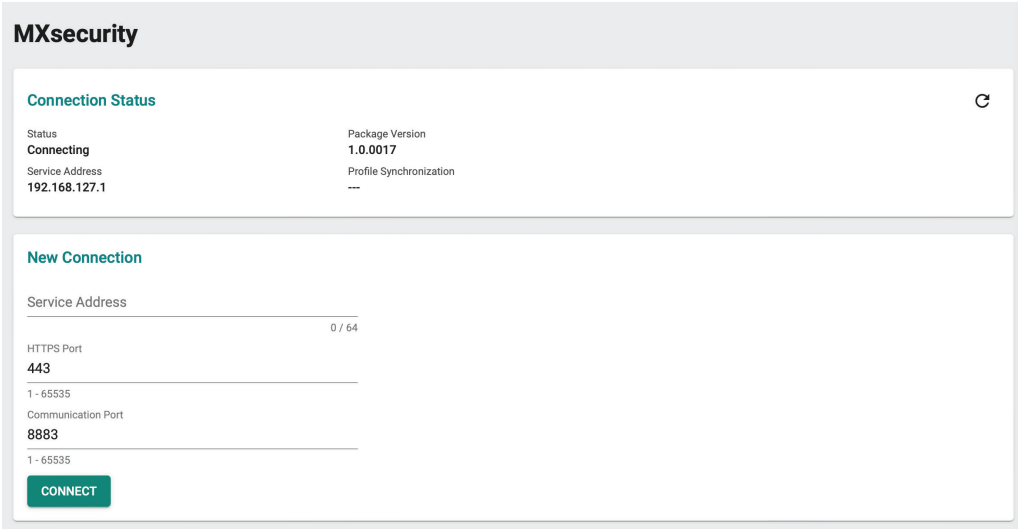


Connecting Secure Routers to MXsecurity

To manage secure routers through MXsecurity, the device needs to be synced to MXsecurity.

Steps:

1. Open a web browser and navigate to the secure router's web management interface by entering its IP address into the address bar.
2. Navigate to **System > Management Interface > MXsecurity**.
3. Enter the MXsecurity IP address field in the **Service Address** field.
4. (**Optional**) Configure the HTTPS port and Communication ports based on the MXsecurity server settings.



5. Click **CONNECT**.

The secure router's MXsecurity page also shows the current connection status. Refer to the table below for more information.

Setting	Description
Status	The status of the connection to MXsecurity. **Disconnected**: The secure router is not connected to MXsecurity. **Connecting**: A connection to MXsecurity is being established. **Connected**: The secure router is connected to MXsecurity.
Package Version	The currently installed MXsecurity Agent Package.
Service Address	The IP address or domain name of the MXsecurity server.
Profile Synchronization	The status of the policy profile synchronization with MXsecurity. **Unsynchronized**: Failed to sync the policy profile settings with MXsecurity. **Synchronized**: The policy profile settings are synced with MXsecurity. **Out of Synchronization**: The policy profile settings were manually modified on the device, causing a mismatch the MXsecurity profile settings.

5. Dashboard and Widgets

Monitor the system status, security assets, and threat detection on the Dashboard page. By default, the Dashboard includes widgets for System Status, Node License Usage, Group Status, Top 5 Layer 3-7 Policy Events, Top 5 Protocol Filter Policy Events, Top 5 ADP Events, and Top 5 IPS Events.

NOTE

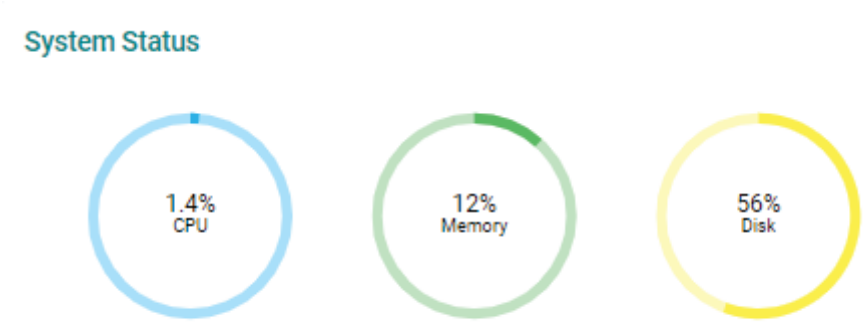
The amount of statistical information shown depends on your user account role and whether permission to manage each device group has been shared with you.

Dashboard Widgets Overview

This section describes available widgets on the dashboard.

System Status

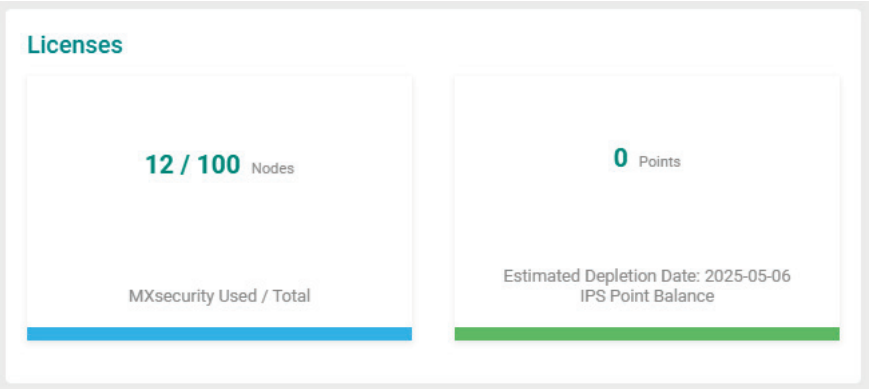
This widget shows the CPU usage, memory usage, and disk usage of the system running the MXsecurity instance.



Licenses

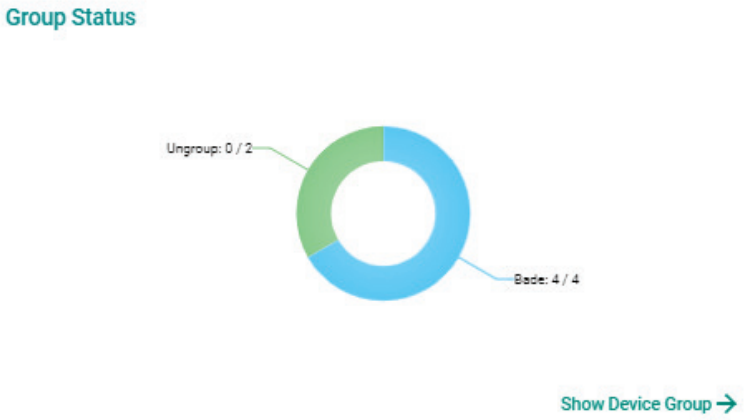
This widget displays the following information about MXsecurity and IPS licenses:

- The number of total and used MXsecurity node licenses.
- The total IPS license point balance and estimated depletion date.



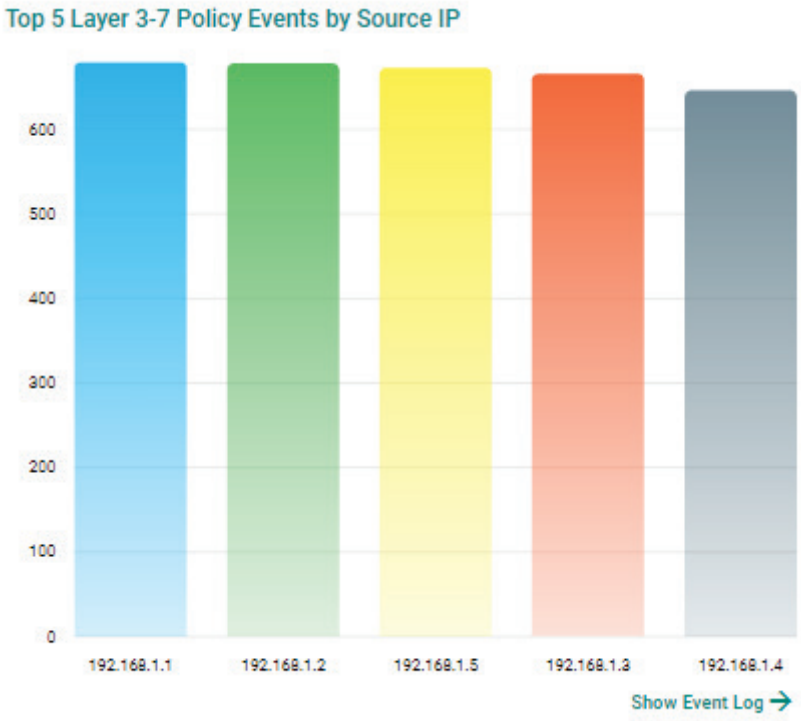
Group Status

This widget lists the information of device groups and device status.



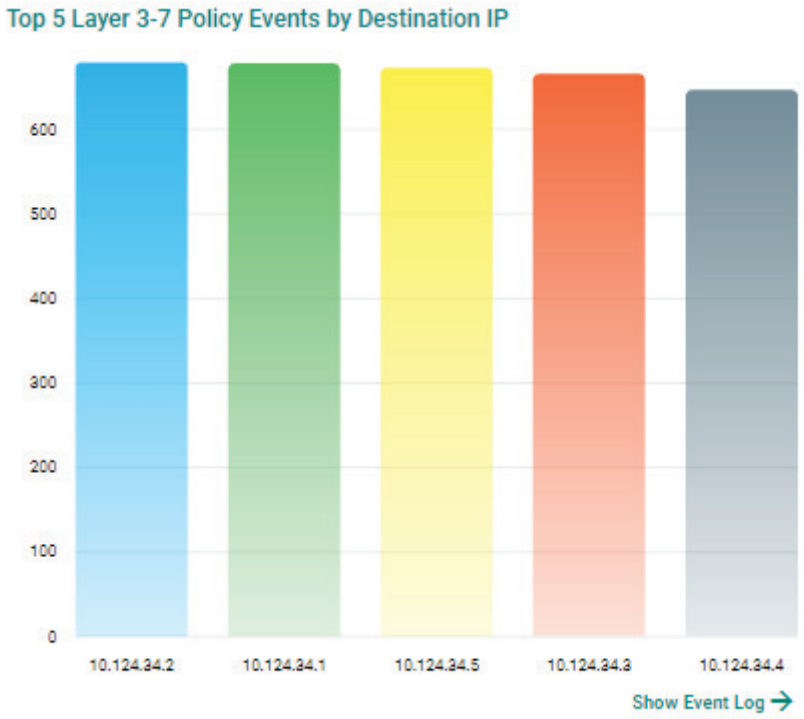
Top 5 Layer 3-7 Policy Events by Source IP

This widget displays the top 5 source IP addresses in the selected device group(s) where the most Layer 3-7 Policy Events were detected within the last 24 hours.



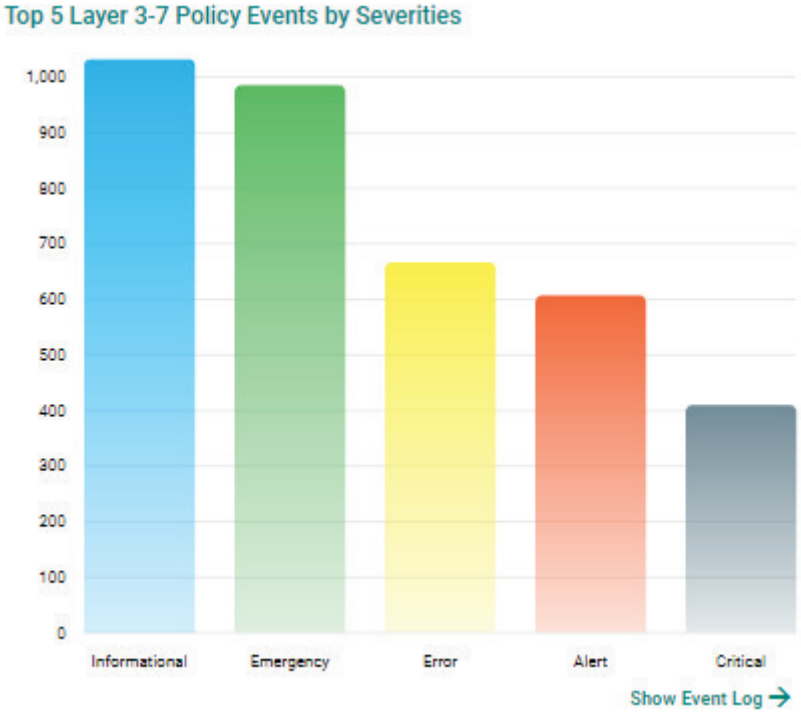
Top 5 Layer 3-7 Policy Events by Destination IP

This widget displays the top 5 destination IP addresses in the selected device group(s) where the most Layer 3-7 Policy Events were detected within the last 24 hours.



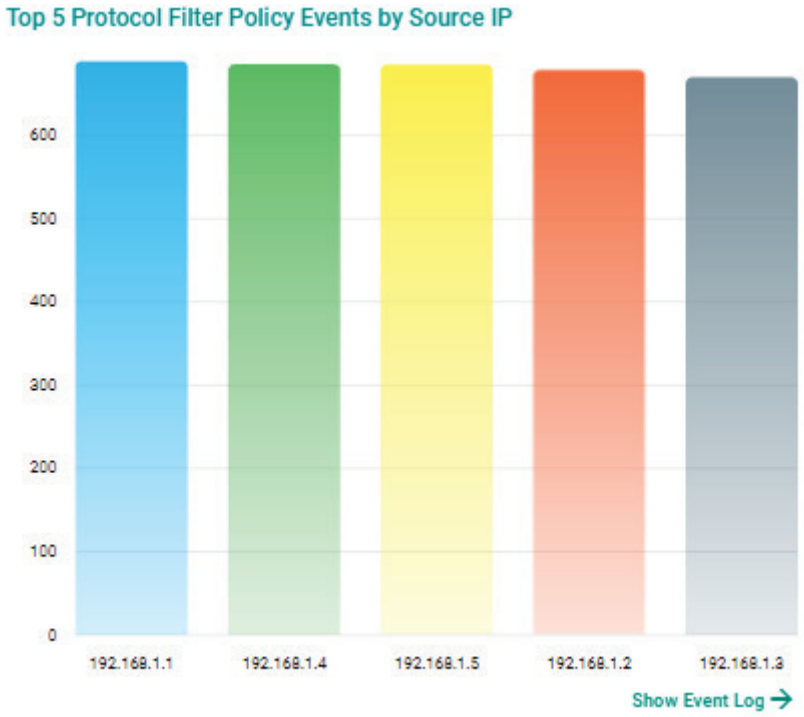
Top 5 Layer 3-7 Policy Events by Severity

This widget displays the number of Layer 3-7 Policy Events in the selected device group(s) within the last 24 hours categorized by severity level.



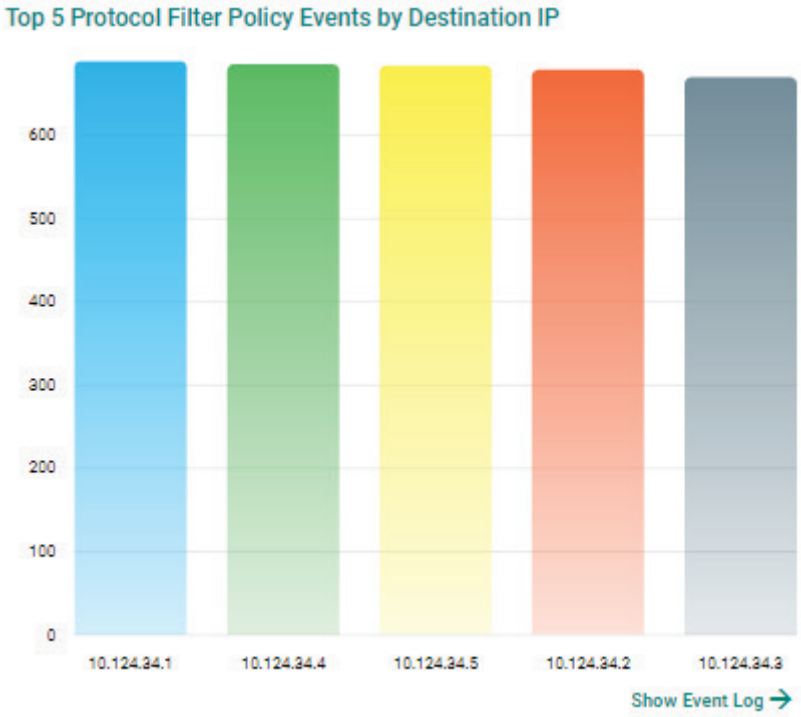
Top 5 Protocol Filter Policy Events by Source IP

This widget displays the top 5 source IP addresses in the selected device group(s) where the most Protocol Filter Policy Events were detected within the last 24 hours



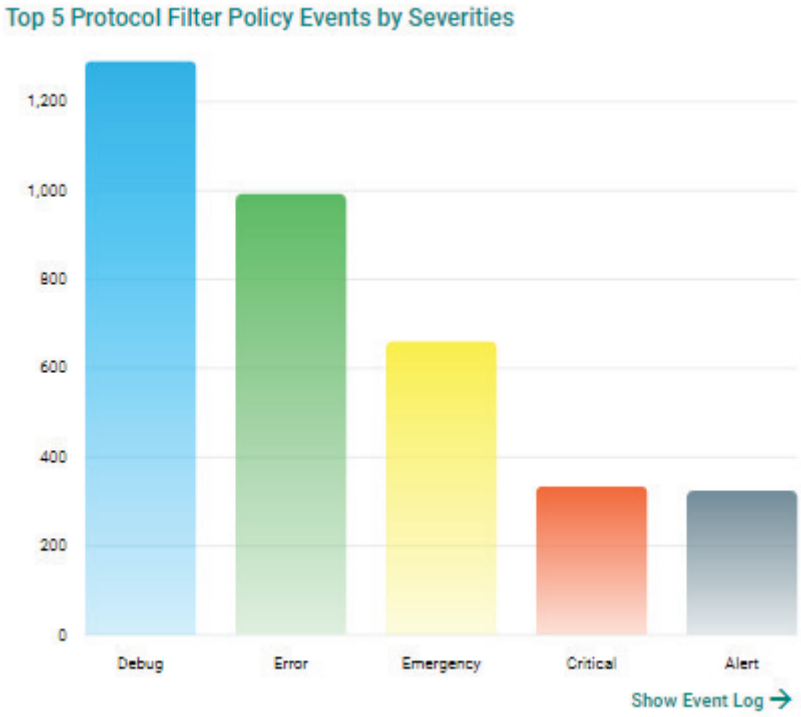
Top 5 Protocol Filter Policy Events by Destination IP

This widget displays the top 5 destination IP addresses in the selected device group(s) where the most Protocol Filter Policy Events were detected within the last 24 hours.



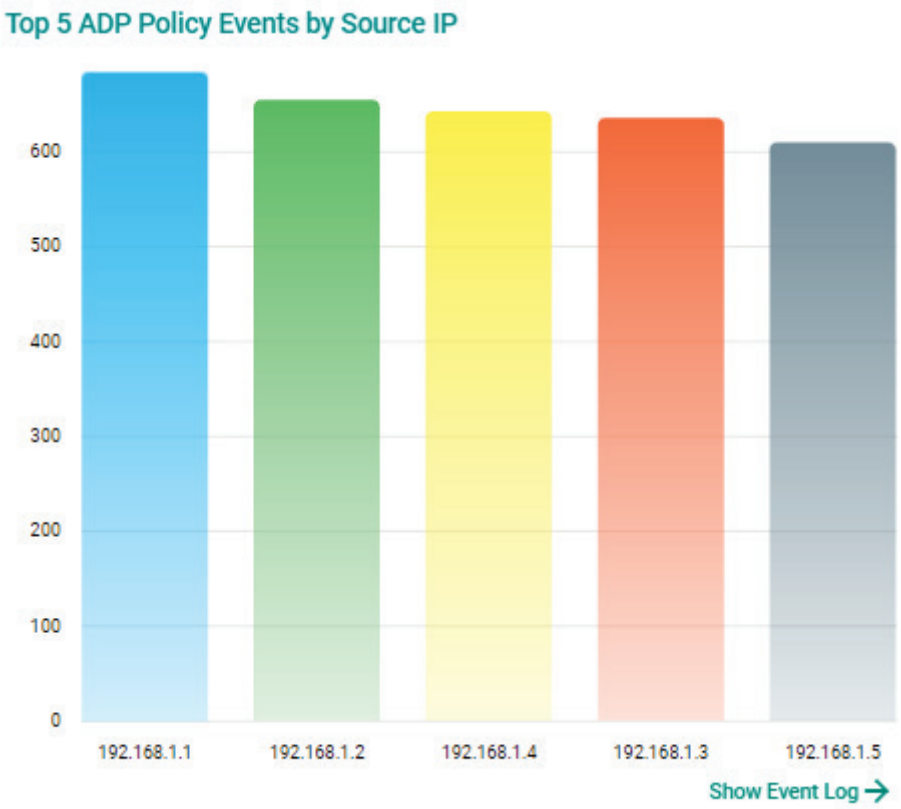
Top 5 Protocol Filter Policy Events by Severity

This widget displays the number of the Protocol Filter Policy Events in the selected device group(s) within the last 24 hours categorized by severity level.



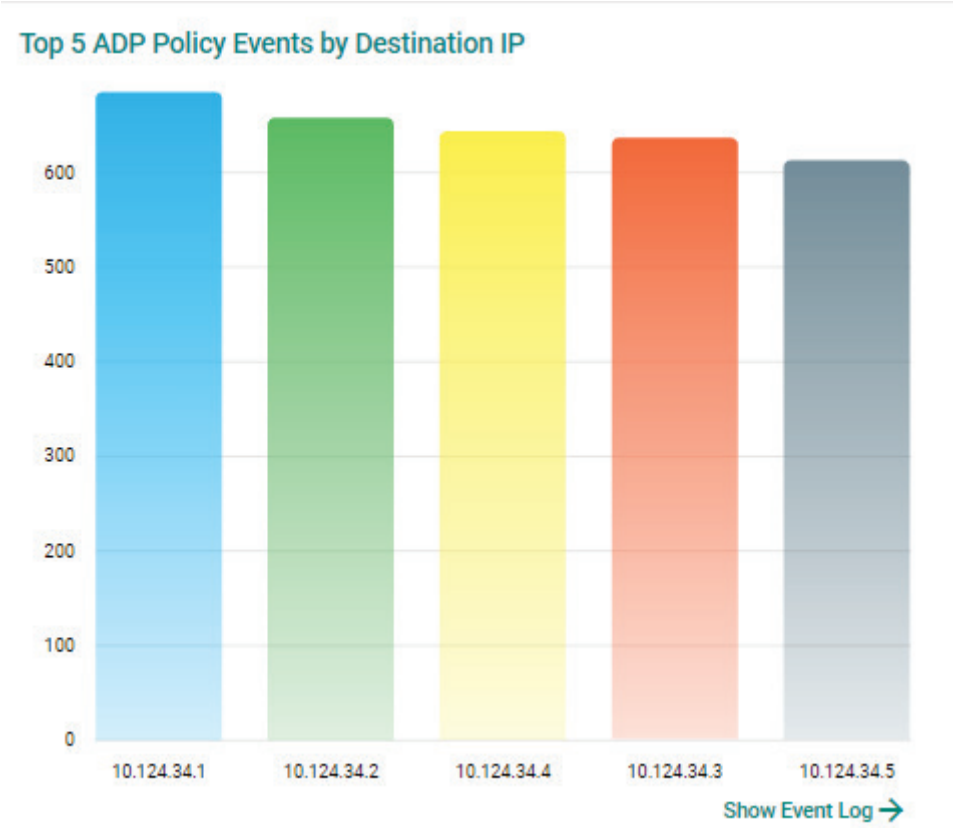
Top 5 ADP Events by Source IP

This widget displays the top 5 source IP addresses in the selected device group(s) where the most ADP Events were detected within the last 24 hours.



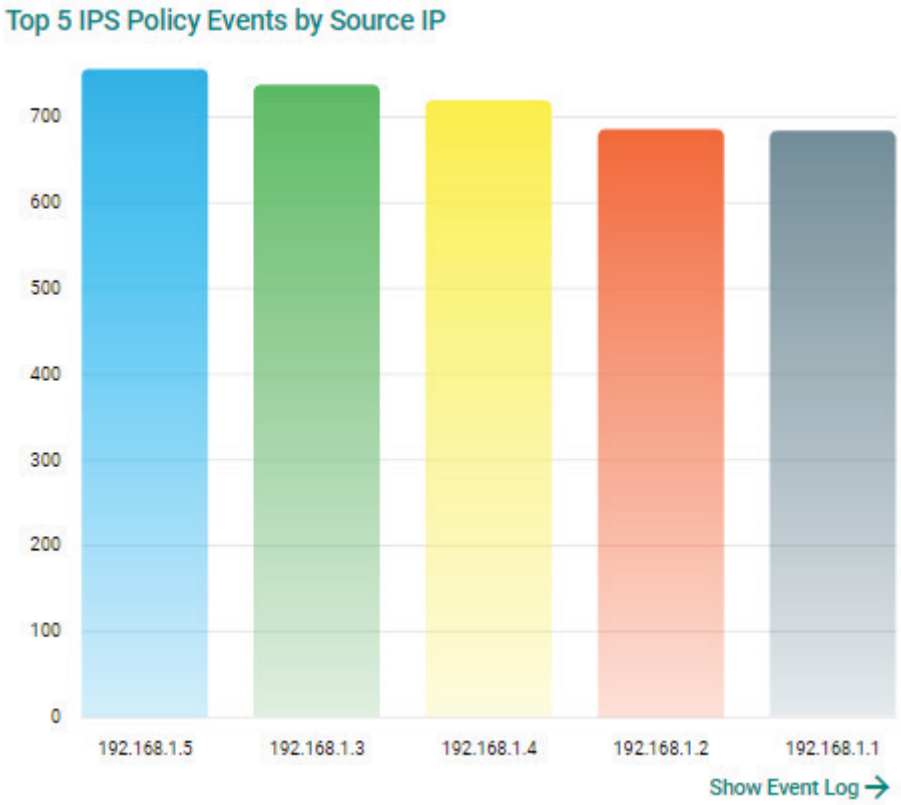
Top 5 ADP Events by Destination IP

This widget displays the top 5 destination IP addresses in the selected device group(s) where the most ADP Events were detected within the last 24 hours.



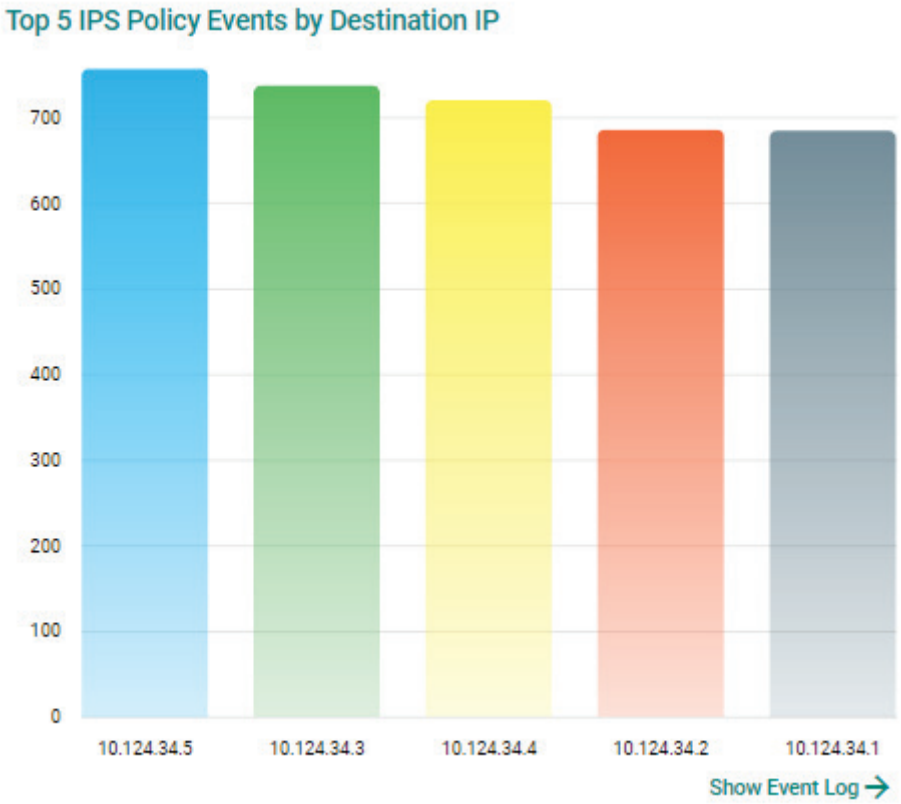
Top 5 IPS Events by Source IP

This widget displays the top 5 source IP addresses in the selected device group(s) where the most IPS Events were detected within the last 24 hours.



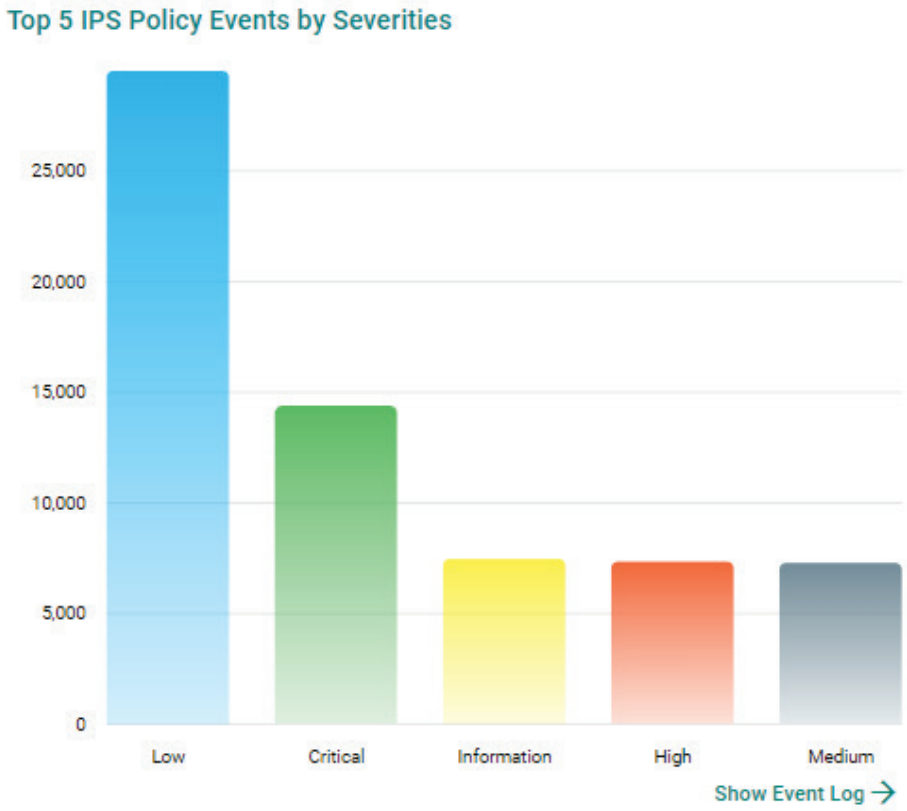
Top 5 IPS Events by Destination IP

This widget displays the top 5 destination IP addresses in the selected device group(s) where the most IPS Events were detected within the last 24 hours.


Top 5 IPS Policy Events by Destination IP
700
600
500
400
300
200
100
0
10.124.34.5
10.124.34.3
10.124.34.4
10.124.34.2
10.124.34.1
Show Event Log

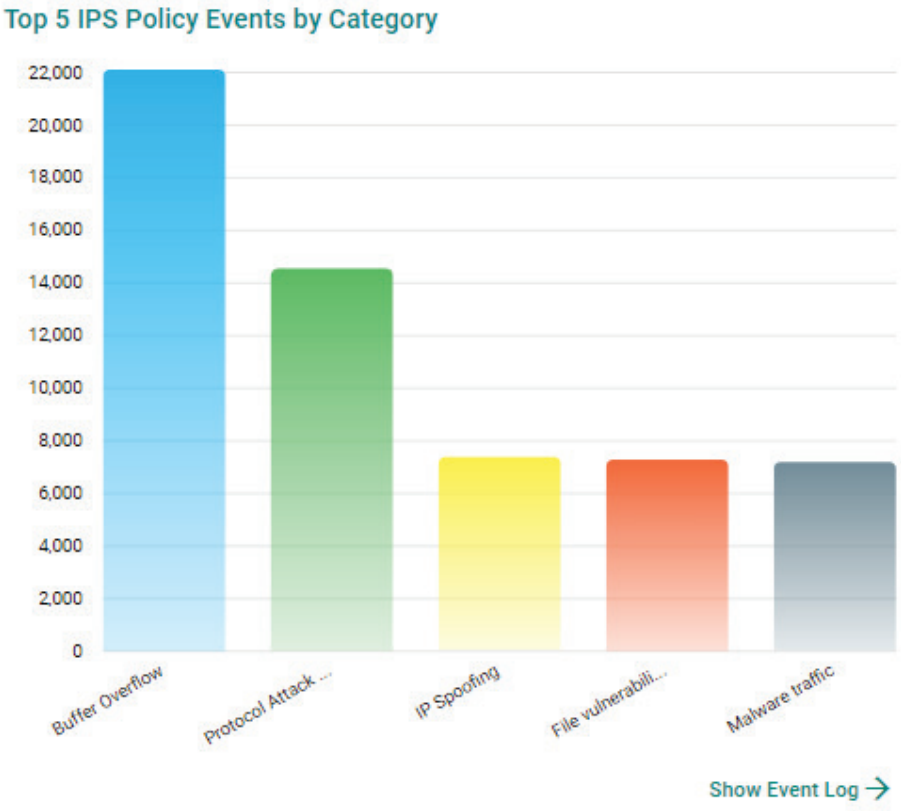
Top 5 IPS Events by Severity

This widget displays the number of IPS Events in the selected device group(s) within the last 24 hours categorized by severity level.



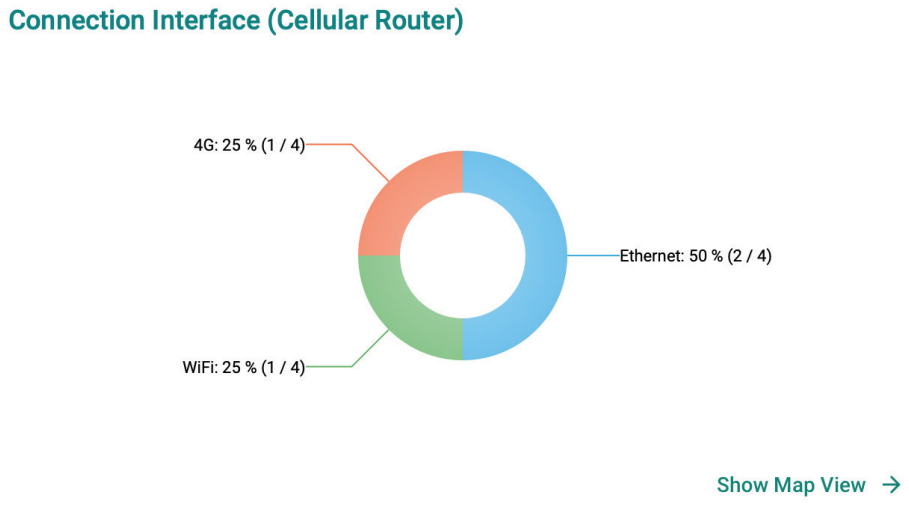
Top 5 IPS Events by Category

This widget displays the number of IPS Events in the selected device group(s) within the last 24 hours categorized by category.



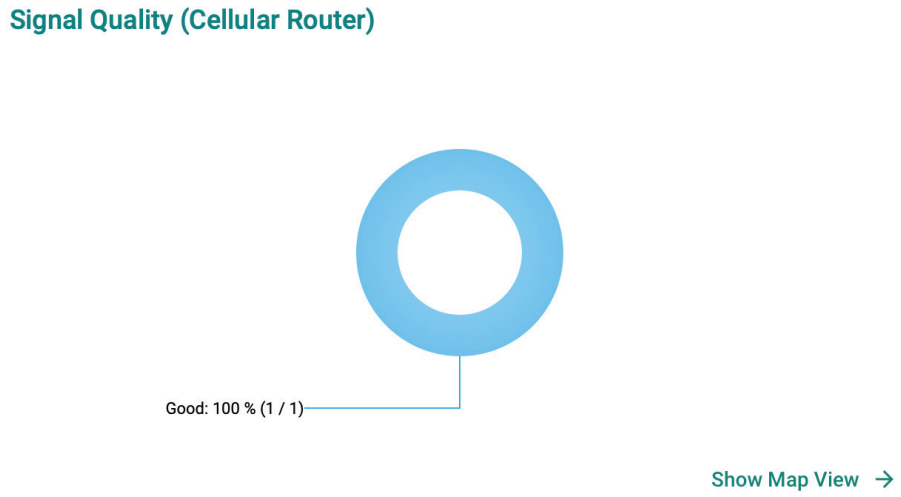
Connection Interface (Cellular Router)

This widget displays a summary of the type of interface currently being used for internet connectivity across all OnCell Series routers. The categories include 5G, 4G, 3G, 2G, Ethernet, and Wi-Fi.



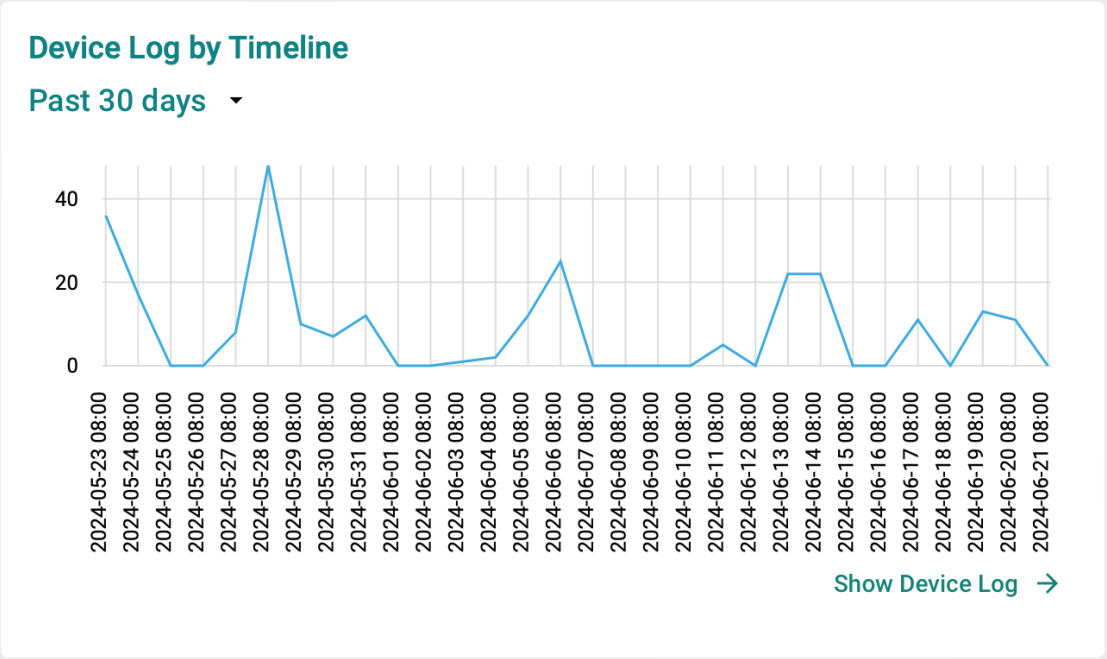
Signal Quality (Cellular Router)

This widget displays a summary of the cellular interface signal quality across all OnCell Series routers, including Good, Fair, Poor, and No Signal.



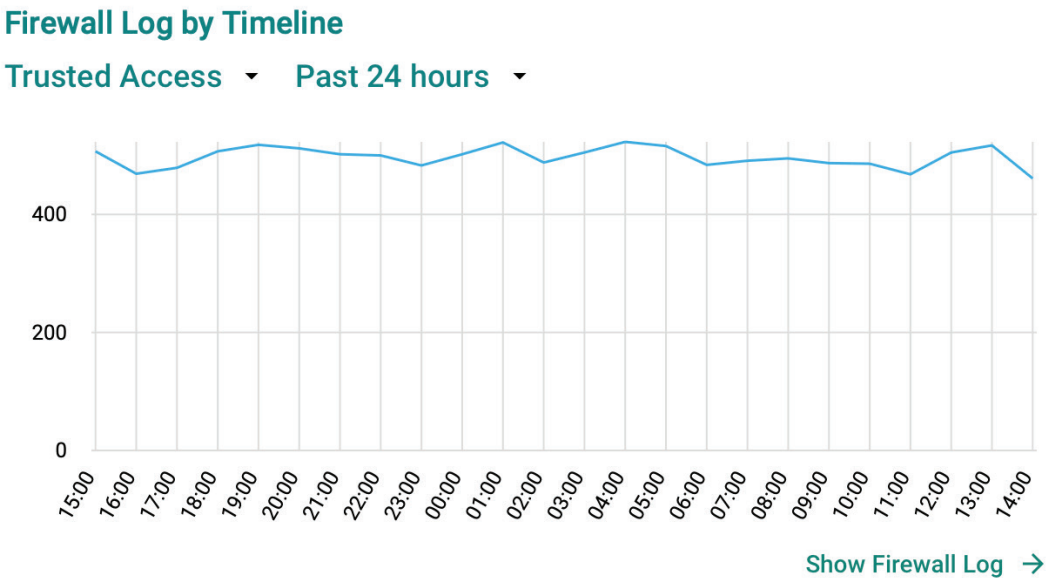
Device Log by Timeline

This widget provides a visual representation of device log events over a specified period. Users can configure the timeline to display events for either the past 24 hours or the past 30 days.



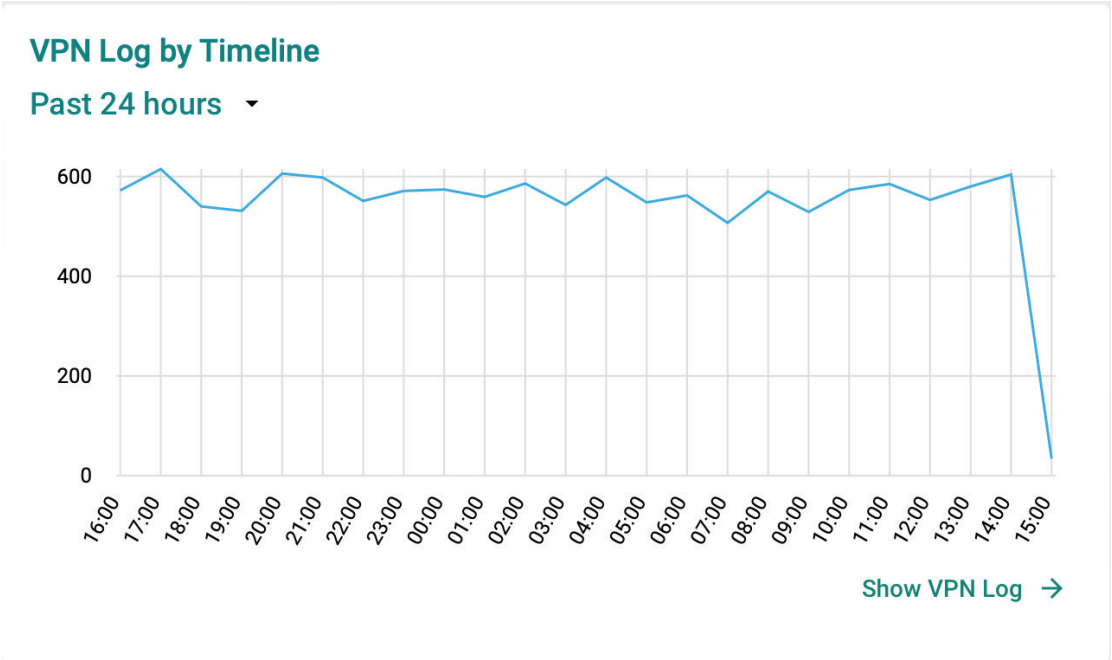
Firewall Log by Timeline

This widget offers a visual representation of firewall events over a specified period. Users can configure the timeline to display events for either the past 24 hours or the past 30 days. Additionally, users can select different subcategories of firewall events, such as DoS policy, to display on the 24-hour or 30-day view.



VPN Log by Timeline

This widget provides a visual representation of VPN events over a specified period. Users can configure the timeline to display events for either the past 24 hours or the past 30 days.



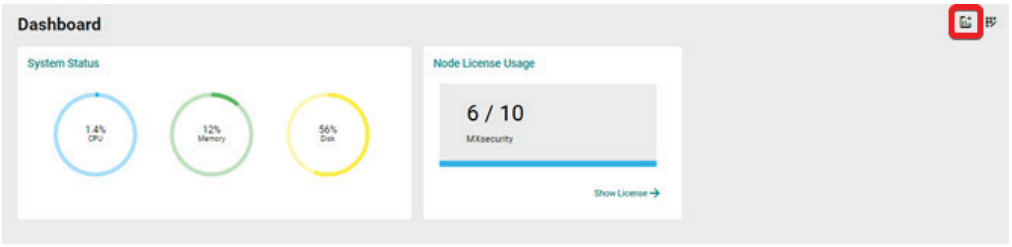
Widget Management

This section describes how to manage the widgets on the MXsecurity Dashboard.

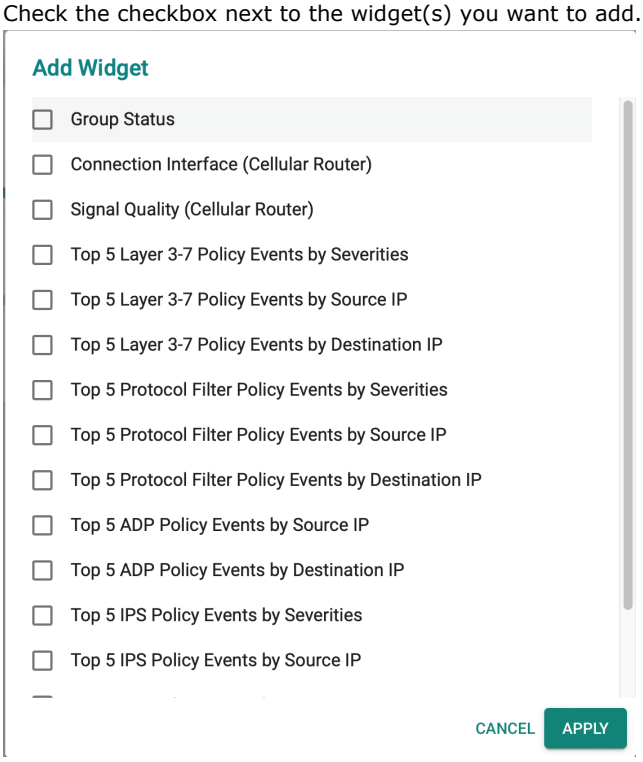
Adding a Widget to the Dashboard

Steps:

1. Click the icon to add widgets.



2. Check the checkbox next to the widget(s) you want to add.



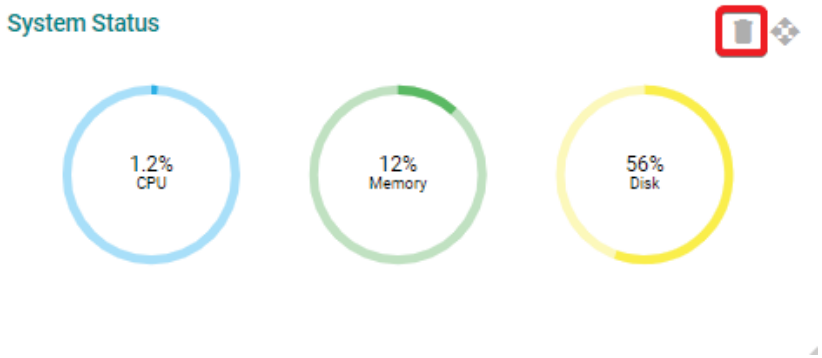
3. Click **APPLY** to add the selected widget(s) to the tab.

Removing a Widget from the Dashboard

Steps:

1. Click the icon to edit the dashboard.

2. Click the **icon of the widget you want to remove**.

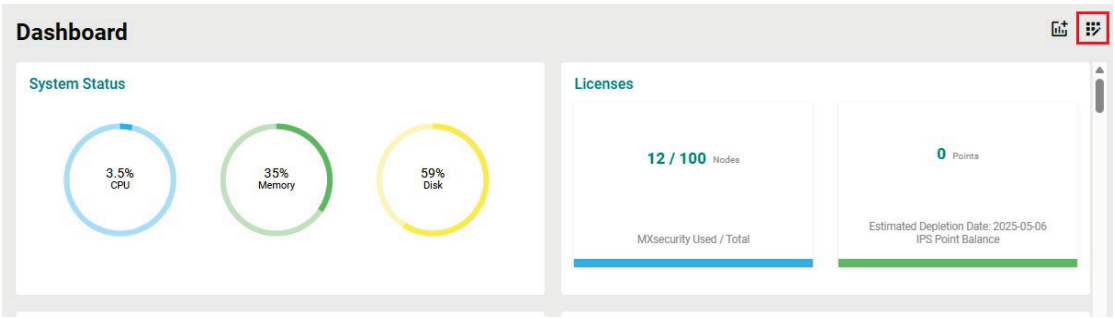


3. Click the icon again to save your changes and leave edit mode.

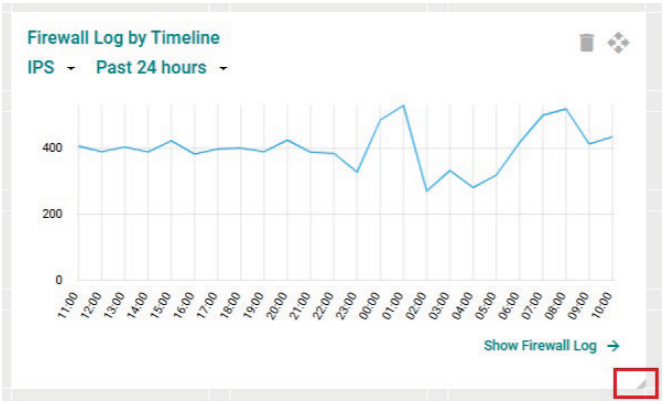
Resizing a Widget

Steps:

1. Click the icon to edit the dashboard.



2. Hover the mouse cursor over the bottom-right corner of the widget until the resize icon is visible.



3. Click and drag the corner of the widget to the desired size, then release the mouse. The dark grey area in the Dashboard background indicates the final size of the widget.

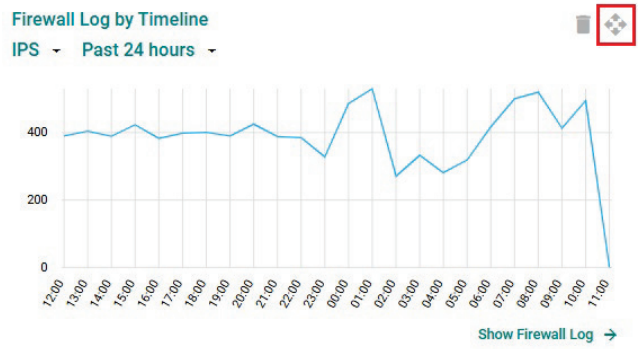
4. Click the  icon again to save your changes and leave edit mode.

Moving the Widget Position

Steps:

1. Click the  icon to edit the dashboard.

2. Click and hold the  icon then drag the widget to the desired position and release the mouse. The widget will automatically snap into place.
The dark grey area in the Dashboard background indicates the final location of the widget.



3. Click the  icon again to save your changes and leave edit mode.

6. Management

The Management page lets you manage device groups, and system databases for firmware software, packages, objects, policy profiles, and device configuration files. With these databases, you can deploy each device individually or arrange them in groups to share the same configuration and policy.

> **NOTE**
>
> The information shown depends on your user account role and whether permission to manage the device groups has been shared with you.

Device Group Management

To easily manage a large number of devices using MXsecurity, devices can be conveniently grouped so that the same security policy configurations can be shared among the devices that belong to the same group.

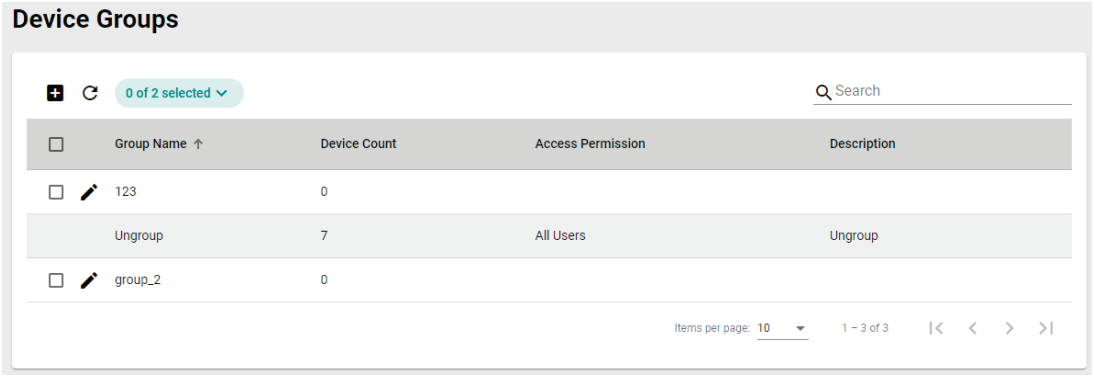
The configurations and policies that can be shared are:

- Firmware
- Software packages
- Objects
- Policy profiles
- Device configurations

Creating a New Device Group

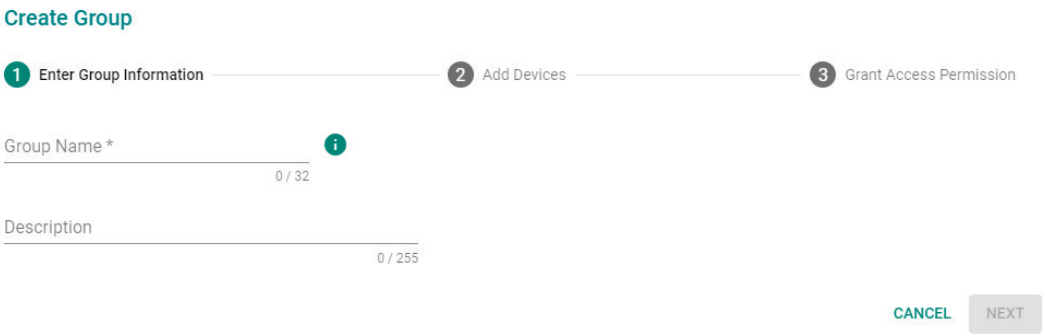
Steps:

1. Navigate to **Management > Device Groups**.

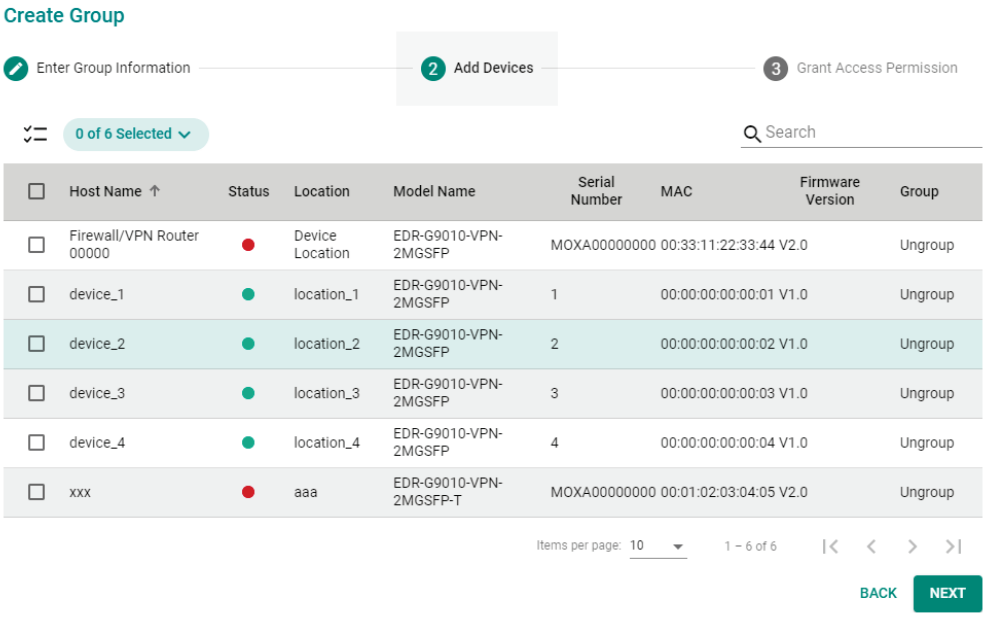


2. Click the  icon to create a new group.
3. Provide a name and description for the group and click **NEXT**.

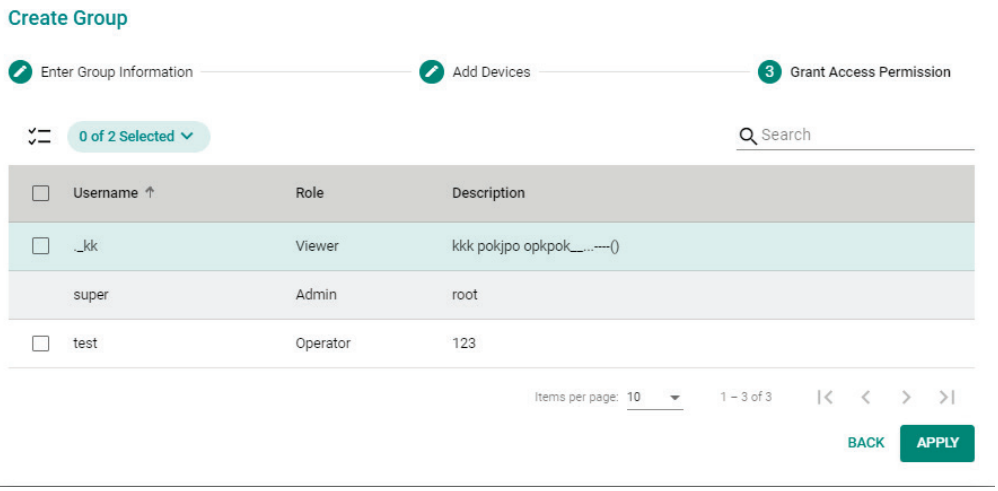
   The group name can be up to 32 characters long and supports a-z, A-Z, 0-9, periods (.), and underscores (_).



4. Check the box of the device(s) that you want to add to the group and click **NEXT**.



5. Check the box of the username(s) that you want to assign to the group and click **APPLY**.

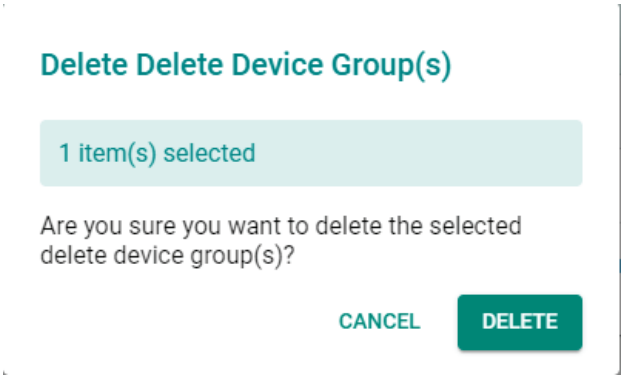


Deleting a Device Group

Steps:

1. Navigate to **Management > Device Groups**.
2. Check the box of the group(s) you want to delete.
3. Click the  icon to delete the selected group(s).

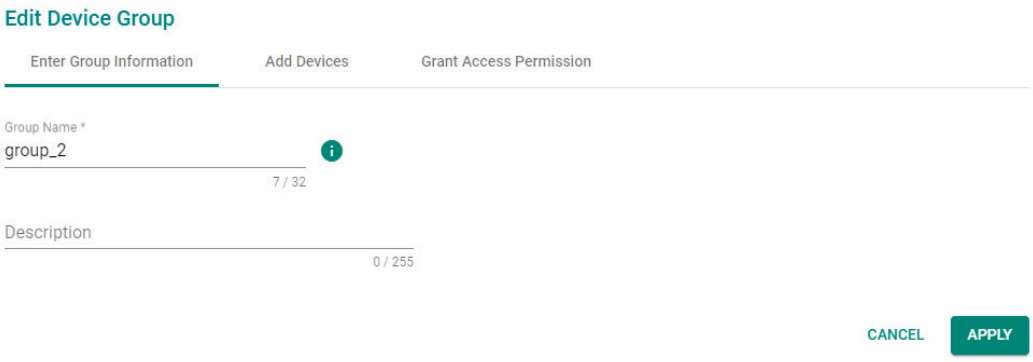
4. When prompted to confirm, click **DELETE**.



Editing a Device Group

Steps:

1. Navigate to **Management > Device Groups**.
2. Click the icon to edit a device group.
3. Edit the device group information, add devices, or grant access permissions.



4. Click **APPLY** to save the changes.

Firmware Management

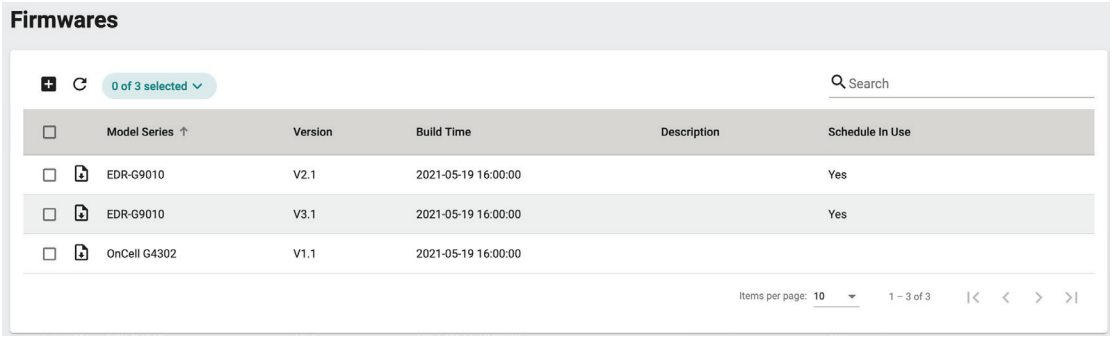
This section describes how to manage the local firmware database from MXsecurity.

Uploading New Firmware

Steps:

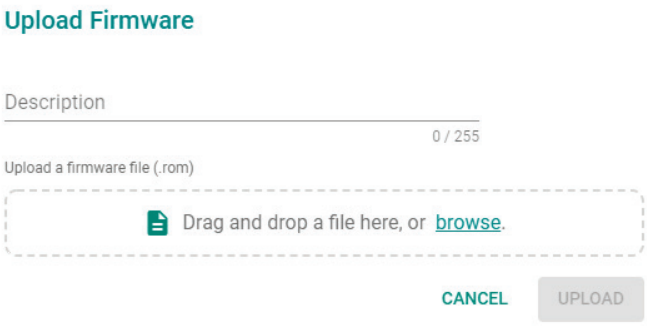
1. Navigate to **Management > Firmwares**.

2. Click the icon to add a new firmware.



> **NOTE**
>
> "Schedule in Use" indicates there is an upcoming scheduled deployment to apply this firmware to the device. To avoid any disruptions or deployment process failures, firmware files with planned deployments cannot be deleted.

3. Drag and drop or browse to the firmware file on the local machine and enter a description.

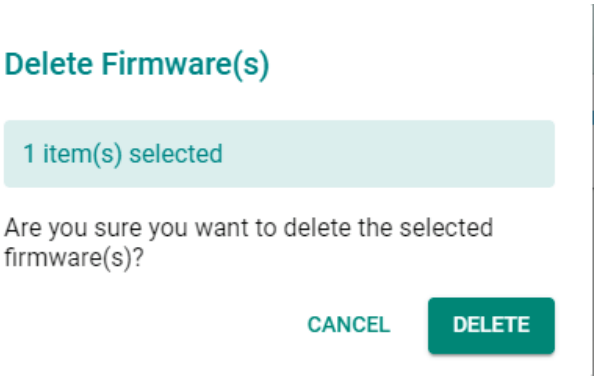


4. Click **UPLOAD**.

Deleting Firmware

Steps:

1. Navigate to **Management > Firmwares**.
2. Check the box of the firmware you want to delete.
3. Click the icon to delete the selected firmware.
4. When prompted to confirm, click **DELETE**.



Exporting Firmware

You can export the firmware files from MXsecurity to the local computer.

Steps:

1. Navigate to **Management > Firmwares**.
2. Click the  icon to download the firmware.

Software Package Management

This section describes how to manage the software package either manually from a local PC or automatically by syncing to the Moxa server.

The following packages can be managed in MXsecurity:

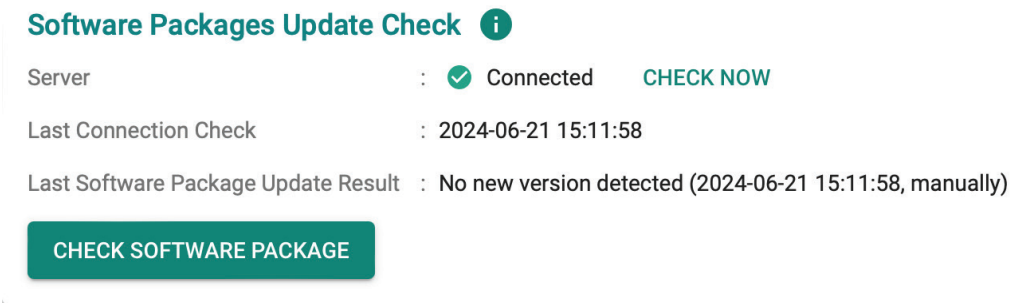
- Network Security Package

This section contains the following tabs:

- **Software Packages File:** Manage software package files for supported devices.
- **Log:** Shows software package-related event logs.
- **Sync:** Configure scheduled software package update checks.

Checking the Security Package Status

The **Software Packages Update Check** section provides information about the Moxa server connection status, the time and date of the last check, and the result of the last check. To access this section, navigate to **Management > Software Packages > Software Packages File.**

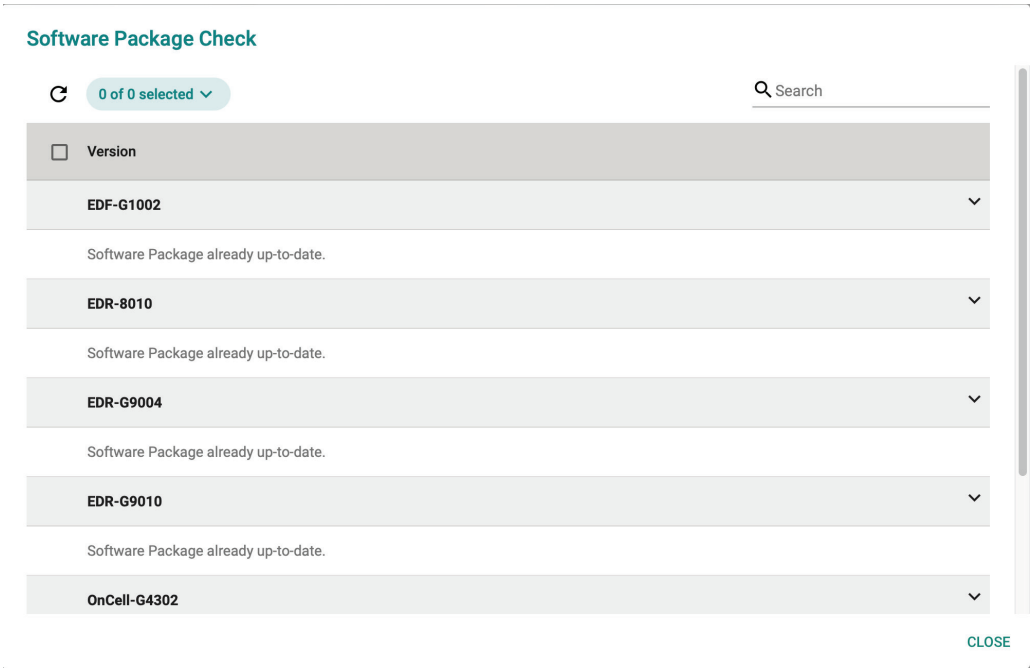


The widget shows the following information:

Field	Description
Server	Shows the current status of the connection to the Moxa update server.
Last Connection Check	Shows the date and time of the last connection check.
Last Software Package Update Result	Shows the result of the most recent software package update check.

To check for software package updates, click the **CHECK SOFTWARE PACKAGE** button. A list of models and any available software package updates will be shown. The models shown in the list are configured in

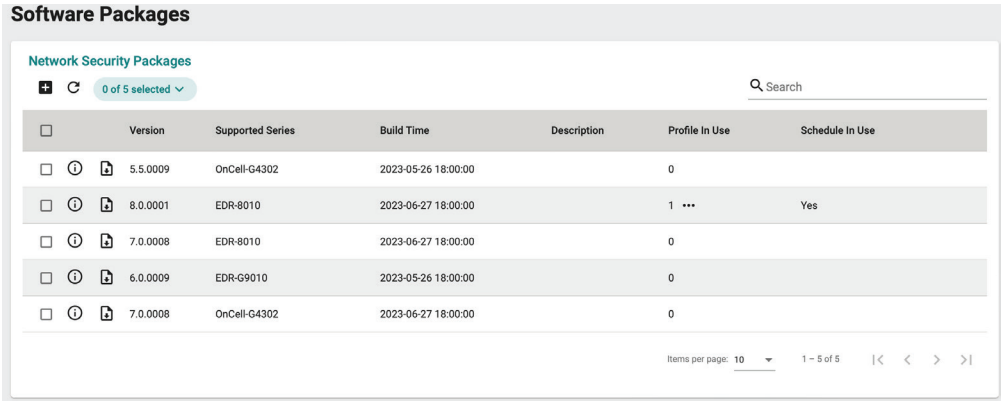
the **Sync Settings** tab. Refer to Setting Up a Scheduled Security Package Update Check.



Uploading a New Software Package

Steps:

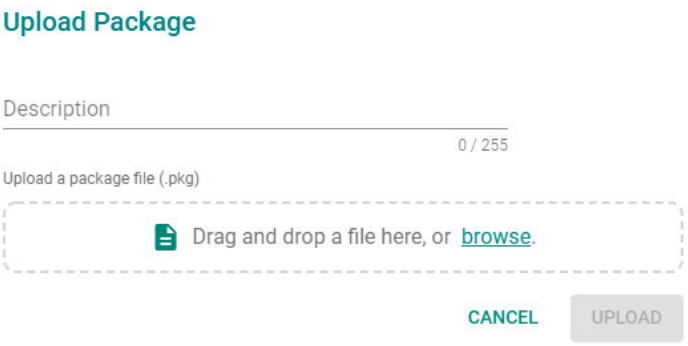
1. Navigate to **Management > Software Packages > Software Packages File**.
2. Click the icon to upload a new software package.



> **NOTE**
>
> "Profile in Use" indicates the number of policy profiles the file is being used by. Files used by policy profiles cannot be deleted. Click the "**...**" icon in the column to see details of the referenced policy profile(s).

> **NOTE**
>
> "Schedule in Use" indicates there is an upcoming scheduled deployment to apply this software package to the device. To avoid any disruptions or deployment process failures, software packages with planned deployments cannot be deleted.

3. Drag and drop or browse to the package file on the local computer and enter a description.

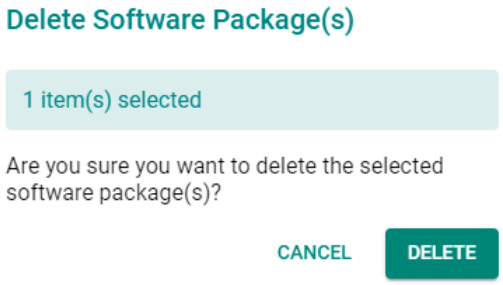


4. Click **UPLOAD**.

Deleting a Software Package

Steps:

1. Navigate to **Management > Software Packages > Software Packages File**.
2. Check the box of the package(s) you want to delete.
3. Click the icon to delete the selected software package(s).
4. When prompted to confirm, click **DELETE**.



Exporting Software Packages

You can export the software packages from MXsecurity to the local computer.

Steps:

1. Navigate to **Management > Software Packages > Software Packages File**.
2. Click the icon to download the software packages.

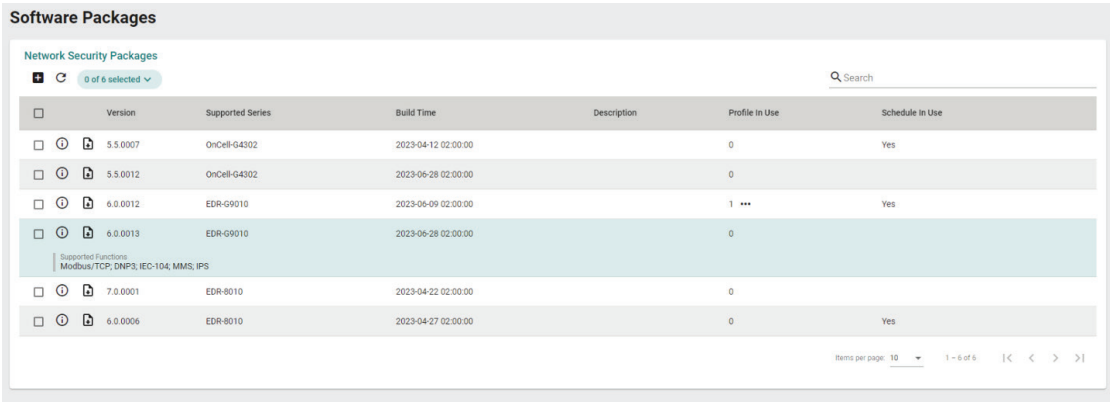
Viewing Detailed Information of a Software Package

You view more detailed information about each software package, including the supported products, build time, and how many devices use the software package.

Steps:

1. Navigate to **Management > Software Packages > Software Packages File**.

2. Click the icon to show detailed information for the software package.



> **NOTE**
>
> "Profile in Use" indicates the number of policy profiles the file is being used by. Files used by policy profiles cannot be deleted. Click the "…" icon in the column to see details of the referenced policy profile(s).

> **NOTE**
>
> "Schedule in Use" indicates there is an upcoming scheduled deployment to apply this software package to the device. To avoid any disruptions or deployment process failures, software packages with planned deployments cannot be deleted.

Viewing Network Security Package Logs

Steps:

1. Navigate to **Management > Software Packages > Log**.
2. You can perform the following actions:

   a. Click the button to export the current search results as a CSV file.

   b. Click the button to renew the search results.

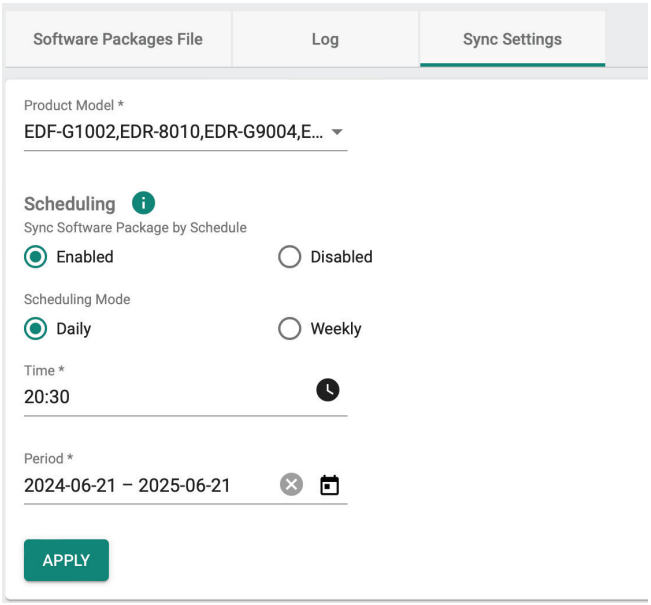
The following table describes the log's fields.

Field	Description
Time	The time the log entry was created.
Severity	The severity level assigned to the event.
Event	The category of the event.
Username	The username of the user that generated the log.
Message	Additional details about the event.

Setting Up a Scheduled Security Package Update Check

Steps:

1. Navigate to **Management > Software Packages**.
2. Click the **Sync Settings** tab.



3. In the Product Model field, select the product models to include the software package update check.
4. Set the Sync Software Package by Schedule radio to **Enabled** to enable scheduled update checks.
5. Select a Scheduling Mode, either daily or weekly:
   a. If daily: Set the time of the day to perform the check.
   b. If weekly: Set the day of the week and time of the day to perform the check.
6. In the Period field, specify the check period. The system will only perform update checks on the specified time and date during this period.
7. Click **APPLY**.

Object Management

This section describes how to manage the local object database from MXsecurity. The objects simplify policy management by storing configurations that can be used by the device group they are associated with.

You can configure the following types of objects in MXsecurity:

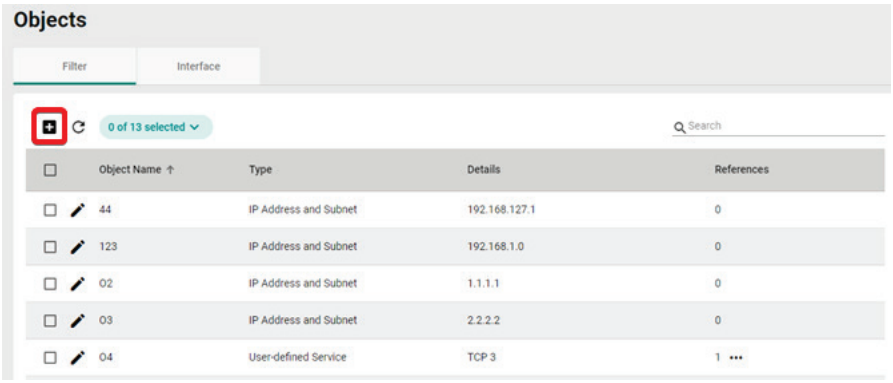
- **Filter Objects**: Contain the IP address and subnet, network service, industrial application service, and user-defined service that you can apply to a policy rule.
- **Interface Objects**: Contain the VLAN interface and bridge interface that you can apply to a policy rule.

Creating a New Filter Object

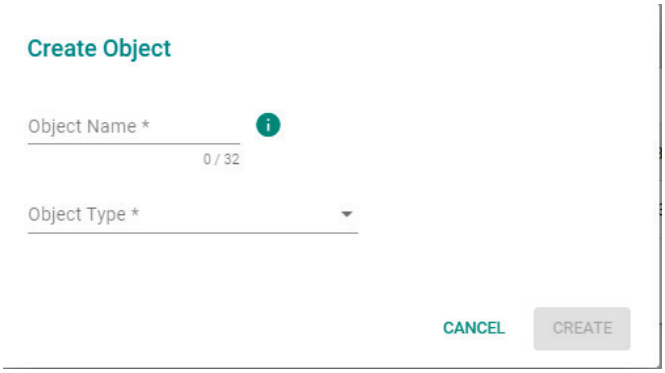
Steps:

1. Navigate to **Management > Objects**.
2. Click the **Filter** tab.

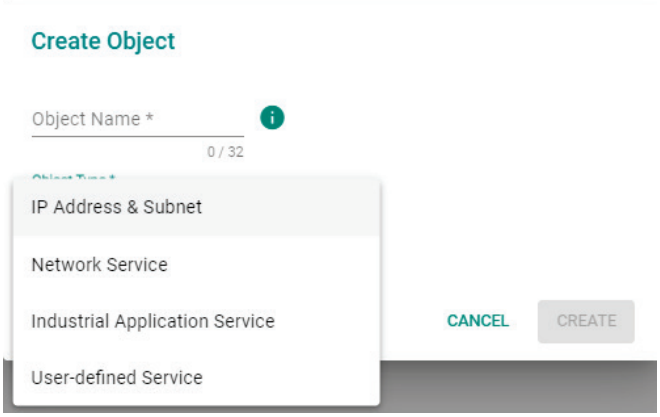
3. Click the icon to create a new object.



4. Enter a name for the object.



5. Select the Object Type. Depending on the select type, configure the following settings:

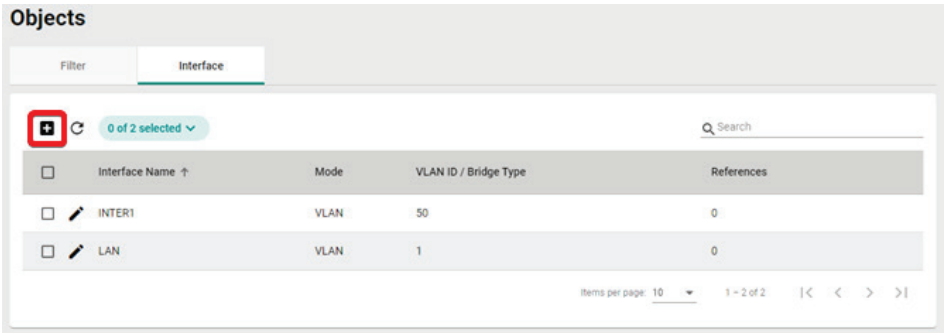


   a. **IP Address and Subnet**:
      i. Depending on the selected IP Type, enter the IP address, IP range, or subnet.
   b. **Network Service**:
      i. Check the box next to the service(s) you want to add to the object.
   c. **Industrial Application Service**:
      i. Check the box next to the industrial application service(s) you want to add to the object.
   d. **User-defined Service**:
      i. Select an IP protocol.
      ii. Depending on the select protocol, specify the port, port range, ICMP Type and Code, or protocol decimal.
6. Click **CREATE**.

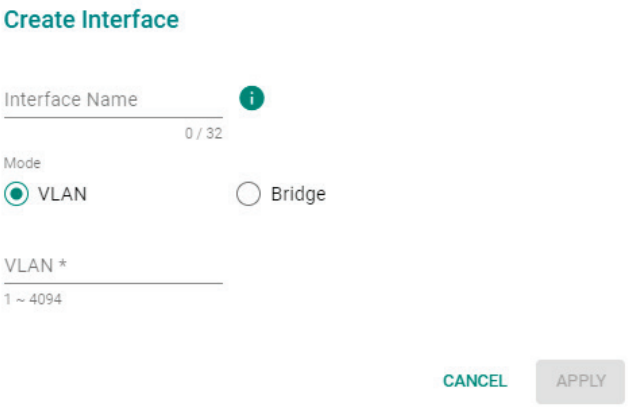
Creating a New Interface Object

Steps:

1. Navigate to **Management > Objects**.
2. Click the **Interface** tab.
3. Click the icon to create a new object.



4. Enter a name for the object.



5. Select the Mode. Depending on the selected mode, configuring the following settings:
   a. **VLAN**:
      i. Enter the VLAN ID.
   b. **Bridge**:
      i. Select a bridge mode.
6. Click **CREATE**.

Editing an Object

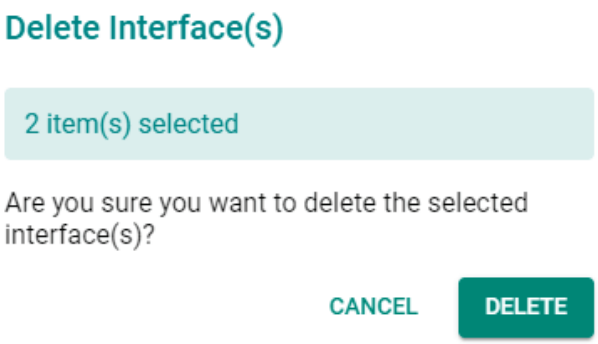
Steps:

1. Navigate to **Management > Objects**.
2. Depending on the object you want to edit, click the **Filter** or **Interface** tab.
3. Click the icon to edit the object.
4. Modify the object settings.
   For Filter Objects, refer to Creating a New Filter Object.
   For Interface Objects, refer to Creating a New Interface Object.
5. When finished, click **APPLY** to save the changes.

Deleting an Object

Steps:

1. Navigate to **Management > Objects**.
2. Depending on the object you want to delete, click the **Filter** or **Interface** tab.
3. Check the box of the object(s) that you want to delete.
4. Click the icon to delete the selected object(s).
5. When prompted to confirm, click **DELETE**.



Policy Profile Management

This section describes how to manage the local policy profile database from MXsecurity. Policy profiles aggregate various firewall policies and can be deployed to device groups based on network security requirements.

You can configure the following types of policies in MXsecurity:

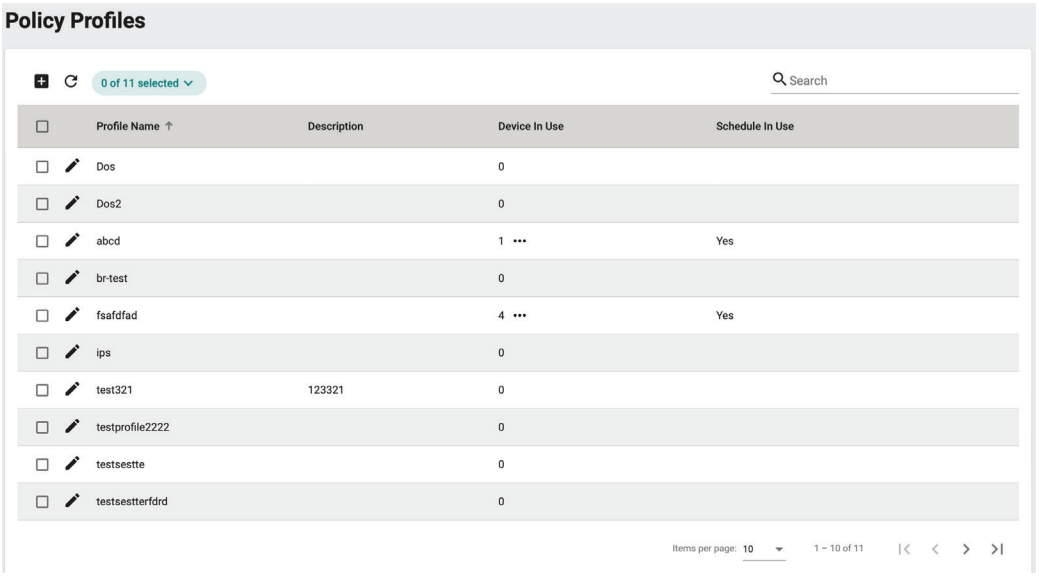
- **Layer 3-7 Policy**: Provides secure traffic control, allowing users to control network traffic based on security needs.
- **Session Control**: Protects network hosts or services from exceeding performance limitations.
- **DoS Policy**: Provides different DoS protection functions for detecting or defining abnormal packet formats or traffic flows.
- **IPS Policy**: Performs intrusion detection and prevention to protect networks from security threats.

Creating a New Layer 3-7 Policy Profile

Steps:

1. Navigate to **Management > Policy Profiles**.

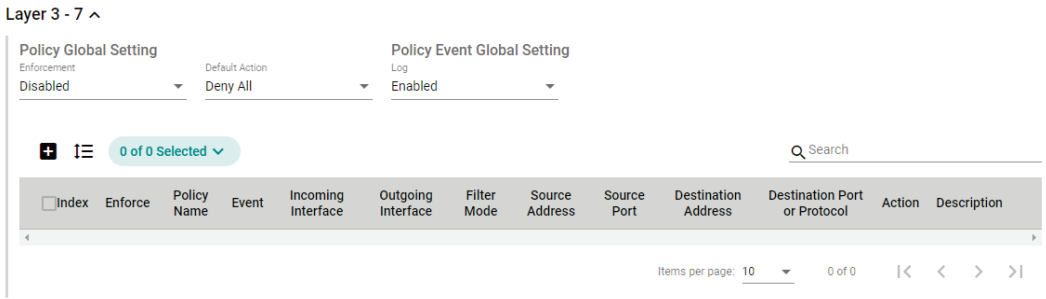
2. Click the icon to create a policy profile.



> **NOTE**
>
> "Device in Use" indicates the number of devices the policy profile is being used by. Policy profiles applied to devices cannot be deleted. Click the "**...**" icon in the column to see details of the referenced device(s).

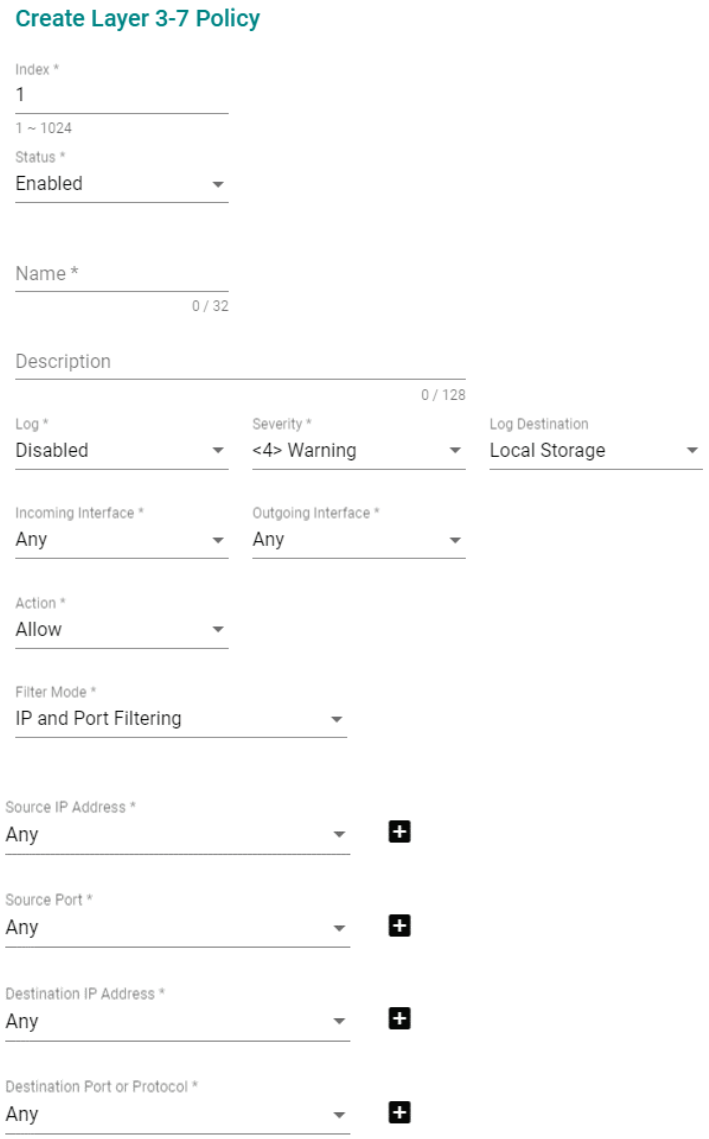
> **NOTE**
>
> "Schedule in Use" indicates there is an upcoming scheduled deployment to apply this policy profile to the device. To avoid any disruptions or deployment process failures, policy profiles with planned deployments cannot be deleted.

3. Enter a name and description for the policy profile.
4. Expand the **Layer 3-7** profile options.



5. Configure the global policy and log settings:
   a. **Enforcement**: Enable or disable the Layer 3-7 policy profiles.
   b. **Default Action**: Choose to deny or allow packets if the packets do not match any configured rules.
   c. **Log**: Enable or disable logging Layer 3-7 policy events.
6. Click the icon to create a Layer 3-7 policy profile.

7. Configure the Layer 3-7 Policy Profile settings:



a. **Index**: Specify the index for the policy profile.
b. **Status**: Enable or disable the policy profile.
c. **Name**: Enter a description for the policy profile.
d. **Description**: Enter a description for the policy profile.
e. **Log**: Enable or disable event logs.
f. **Severity**: Select the log severity level.
g. **Log Destination**: If logging is enabled, choose where the logs will be stored. Multiple options can be selected.
h. **Incoming/Outgoing Interface**: Select the incoming and outgoing interfaces.
i. **Action**: Select the action when traffic matches the policy rule.
j. **Filter Mode**: Select a filtering mode. Depending on the selected mode, configure the following settings:
IP and Port Filtering:
    i. **Source/Destination IP Address**: Select Any or a preconfigured Filter Object. Refer to Creating a New Filter Object.
    ii. **Source Port/Destination Port or Protocol**: Select Any or a preconfigured Interface Object. Refer to Creating a New Interface Object.

IP and Source MAC Binding:

i. **Source MAC Address**: Specify the source MAC address.

ii. **Source IP Address**: Select a preconfigured Filter Object. Refer to Creating a New Filter Object.

Source MAC Filtering:

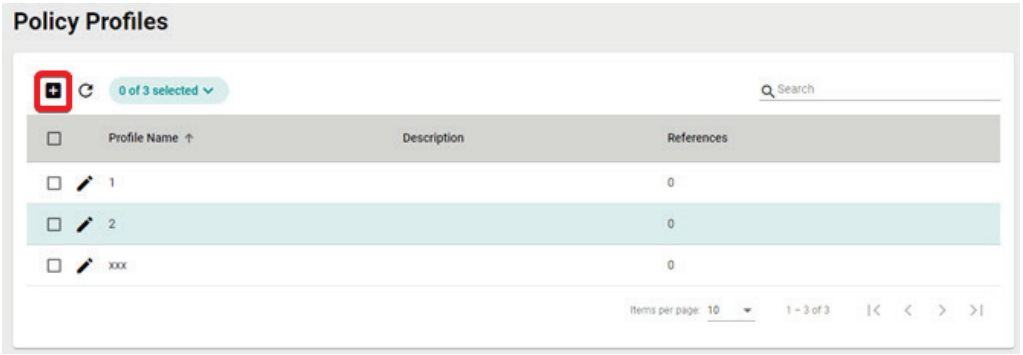
iii. Source MAC Address: Specify the source MAC address.

8. Click **CREATE** to create the Layer 3-7 Policy Profile.
9. Click **APPLY**.

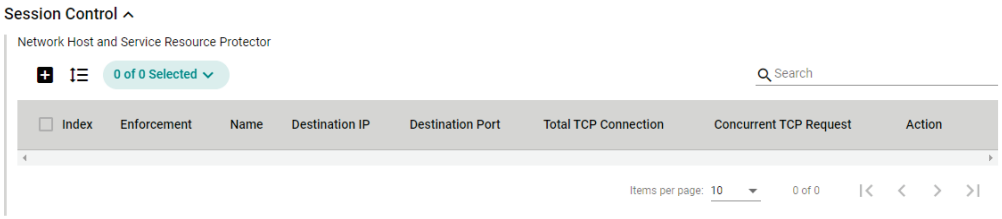
Creating a New Session Control Policy Profile

Steps:

1. Navigate to **Management > Policy Profiles**.
2. Click the  icon to create a policy profile.

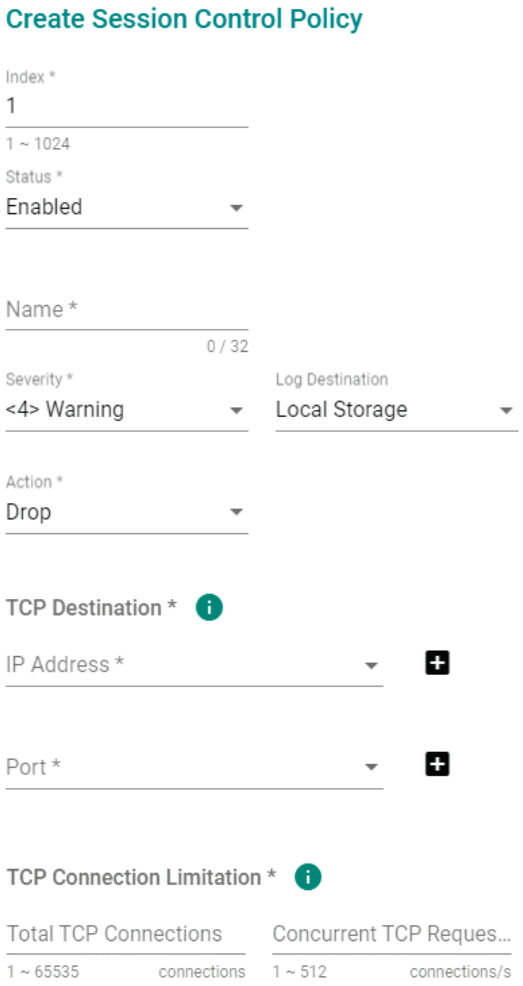


3. Enter a name and description for the policy profile.
4. Expand the **Session Control** profile options.



5. Click the  icon to create a Session Control policy profile.

6. Configure the Session Control Profile settings:



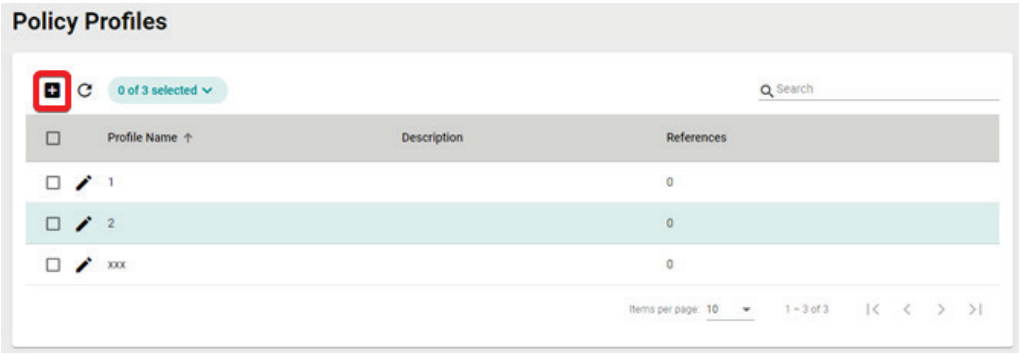
   a. **Index**: Specify the index for the policy profile.
   b. **Status**: Enable or disable the policy profile.
   c. **Name**: Enter a description for the policy profile.
   d. **Severity**: Select the log severity level.
   e. **Log Destination**: If logging is enabled, choose where the logs will be stored. Multiple options can be selected.
   f. **Action**: Select the action when traffic matches the policy rule.
   g. **IP Address**: Select Any or a preconfigured Filter Object. Refer to Creating a New Filter Object.
   h. **Port**: Select Any or a preconfigured Interface Object. Refer to Creating a New Interface Object.
   i. **Total TCP Connections**: Specify the maximum allowed TCP connections.
   j. **Concurrent TCP Requests**: Specify the maximum allowed concurrent connections.
7. Click **CREATE** to create the Session Control Policy.
8. Click **APPLY**.

Creating a New DoS Policy Profile

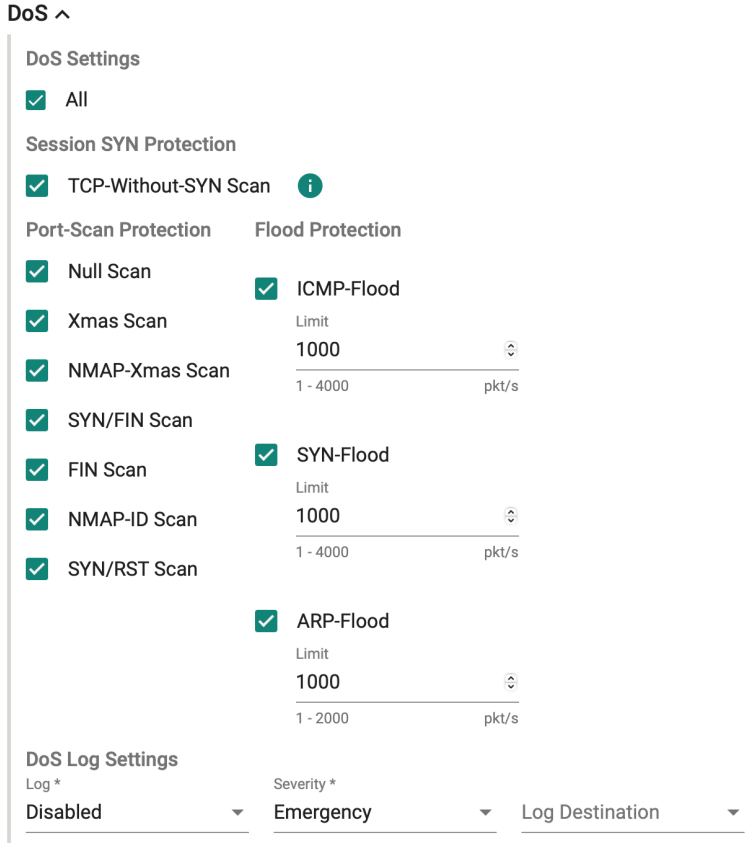
Steps:

1. Navigate to **Management > Policy Profiles**.

2. Click the icon to create a policy profile.



3. Enter a name and description for the policy profile.
4. Expand the **DoS** profile options.
5. Configure the following settings:

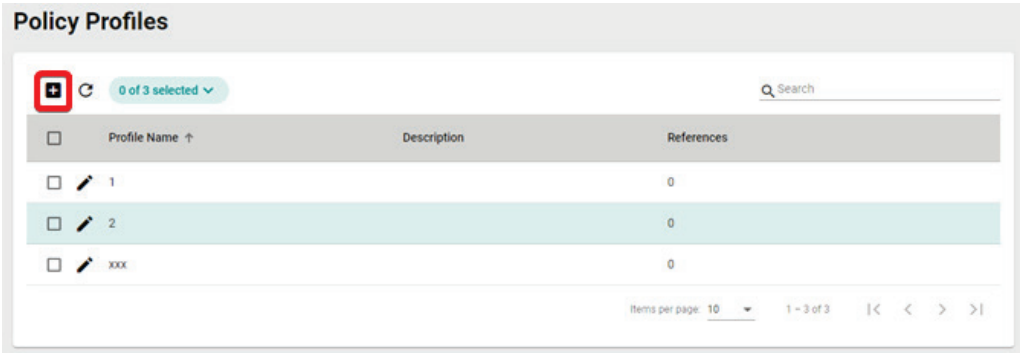


   a. **DOS Setting**: Check the box of the DoS types you want to enable. If you selected ICMP-Death, SYN-Flood, or ARP-Flood, specify the packet limit.
   b. **Log**: Enable or disable event logs.
   c. **Severity**: Select the log severity level.
   d. **Log Destination**: If logging is enabled, choose where the logs will be stored. Multiple options can be selected.
6. Click **APPLY**.

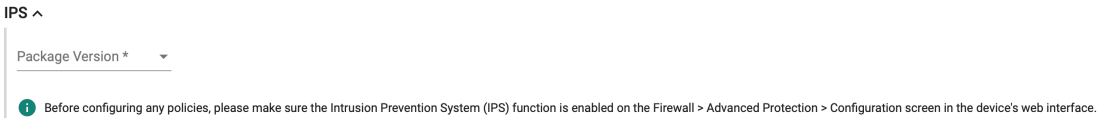
Creating a New IPS Policy Profile

Steps:

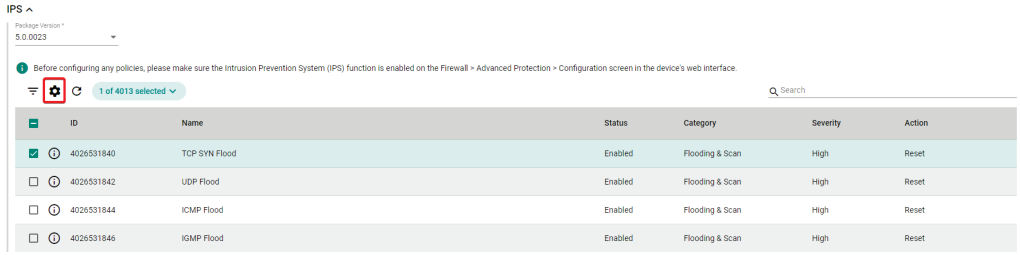
1. Navigate to **Management > Policy Profiles**.
2. Click the  icon to create a policy profile.



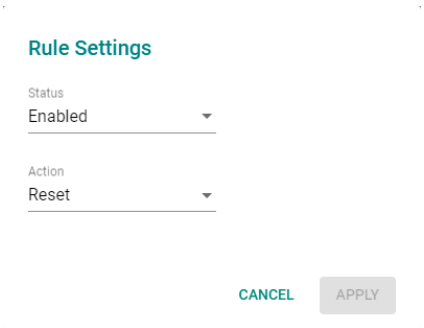
3. Enter a name and description for the policy profile.
4. Expand the **IPS** profile options.
5. Select a previously uploaded IPS software package version.
   Refer to Software Package Management for more information.



6. In the IPS rule table, check the box of the rule(s) you want to configure.
   You can select multiple rules at once.
7. Click the  icon to configure the selected rule(s).



8. Configure the following settings:



   a. **Status**: Enable or disable the rule.
   b. **Action**: Select the action when traffic matches the policy rule.
9. Click **APPLY** to save the changes.
10. On the Policy Profiles screen, click **APPLY**.

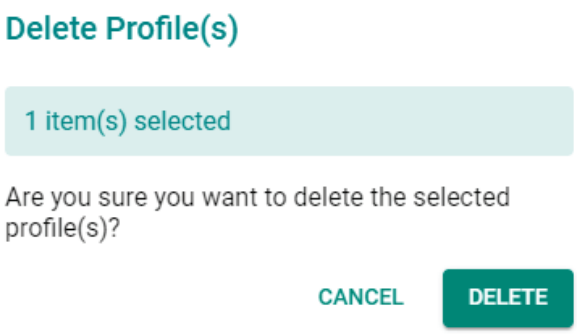
Editing a Policy Profile

1. Navigate to **Management > Policy Profiles**.
2. Click the icon to edit the policy profile.
3. Modify the profile settings.
   For Layer 3-7 policy profiles, refer to Creating a New Layer 3-7 Policy Profile.
   For Session Control policy profiles, refer to Creating a New Session Control Policy Profile.
   For DoS policy profiles, refer to Creating a New DoS Policy Profile.
   For IPS policy profiles, refer to Creating a New IPS Policy Profile.
4. Click **APPLY**.

Deleting a Policy Profile

Steps:

1. Navigate to **Management > Policy Profiles**.
2. Check the box of the policy profile(s) you want to delete.
3. Click the icon to delete the selected profile(s).
4. When prompted to confirm, click **DELETE**.



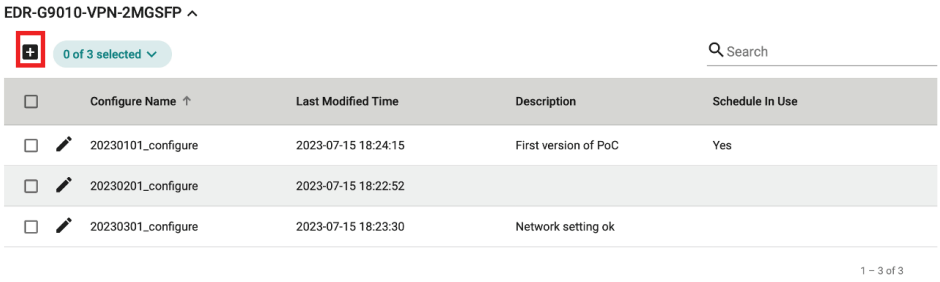
Device Configuration Management

This section describes how to manage the device configuration database from MXsecurity.

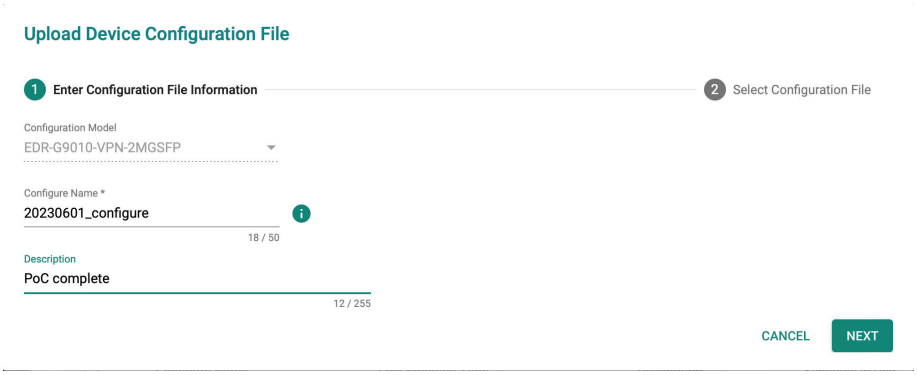
Uploading a Device Configuration File From a Local Host

Steps:

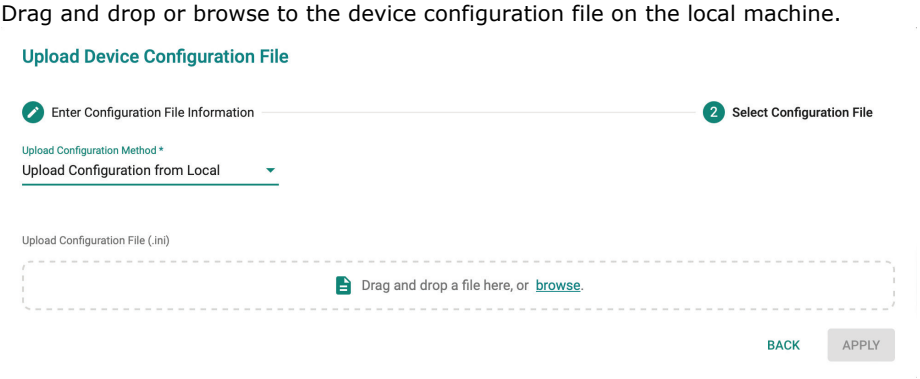
1. Navigate to **Management > Device Configuration**.
2. Click the icon to add a device configuration.



3. Enter the name and description for the configuration file.



4. Click **NEXT**.
5. Select **Upload Configuration from Local** from the Upload Configuration Method drop-down menu.
6. Drag and drop or browse to the device configuration file on the local machine.

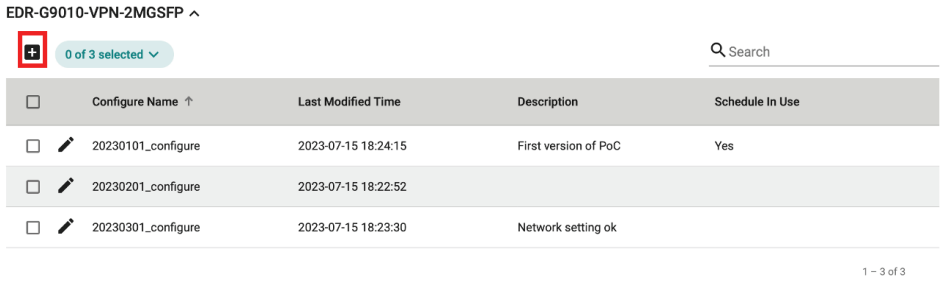


7. Click **APPLY**.

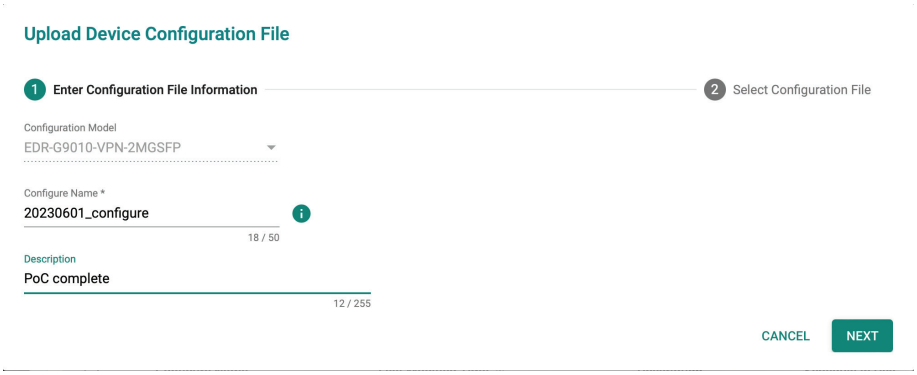
Uploading a Configuration From a Device

Steps:

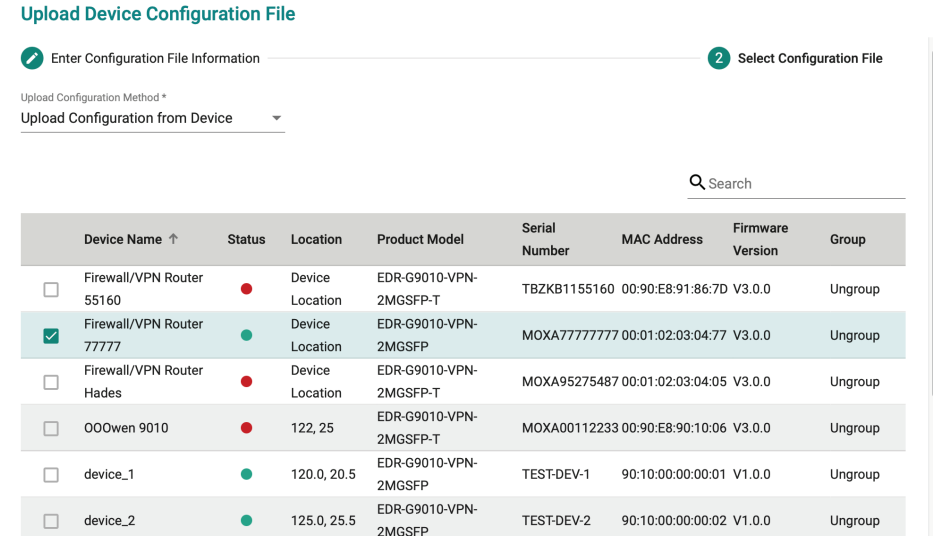
1. Navigate to **Management > Device Configuration**.
2. Click the  icon to add a device configuration.



3. Enter the name and description for the configuration file.



4. Click **NEXT**.
5. Select **Upload Configuration from Device** from the Upload Configuration Method drop-down menu.
6. Select the device to back up and generate the configuration file from.



7. Click **APPLY**.

NOTE

Each device model can have a maximum of five configuration files. When this limit is reached, the **Add** button will become unavailable.

7. Deployment

The Deployment section lets users configure multiple device groups at a time and check the synchronization status between MXsecurity and the managed devices.

You can configure the following types of deployments in MXsecurity:

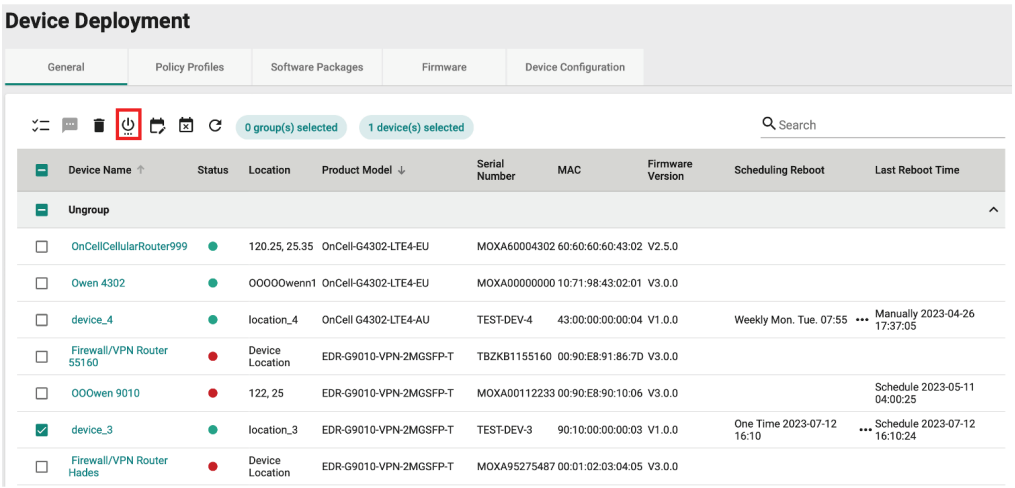
- **General:** Remove and reboot devices.
- **Policy Profiles:** Deploy policy profiles to managed devices.
- **Software Packages:** Upgrade the software package of managed devices.
- **Firmware**: Upgrade the firmware of managed devices.
- **Device Configure**: Deploy device configuration files to managed devices.

Rebooting a Managed Device

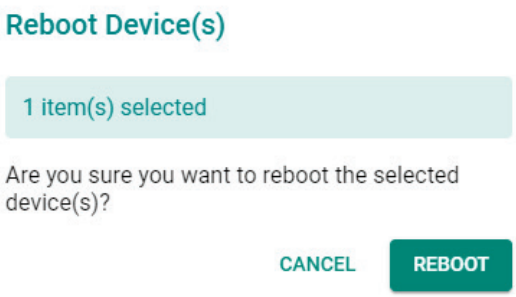
Steps:

1. Navigate to **Device Deployment > General**.
2. Check the box of the device(s) you want to reboot.

   Click the  icon to reboot the selected device(s).



3. When prompted to confirm, click **REBOOT**.

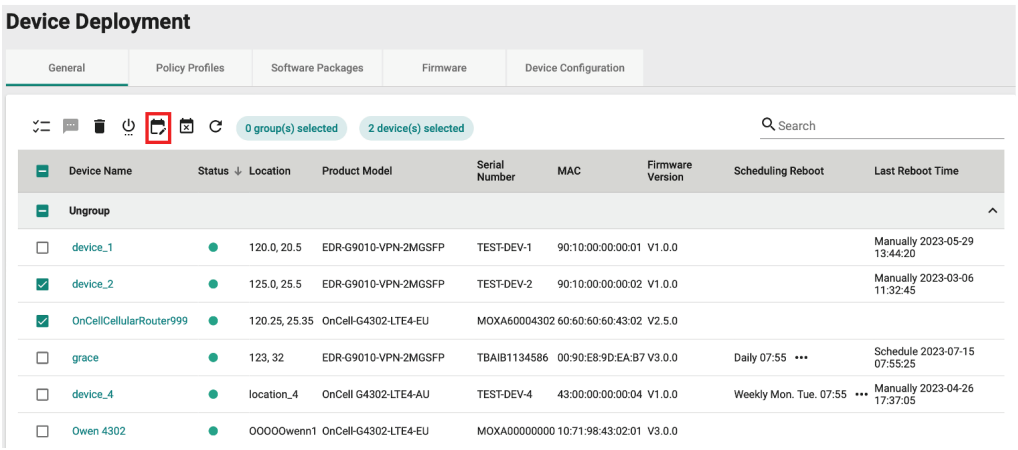


Scheduling a Managed Device Reboot

Rebooting a device may disrupt services or operations. To minimize the potential impact of rebooting devices, users can schedule device reboots for specific times where they are least likely to affect operations. Schedules can be configured to execute only once, or on a daily or weekly recurring basis.

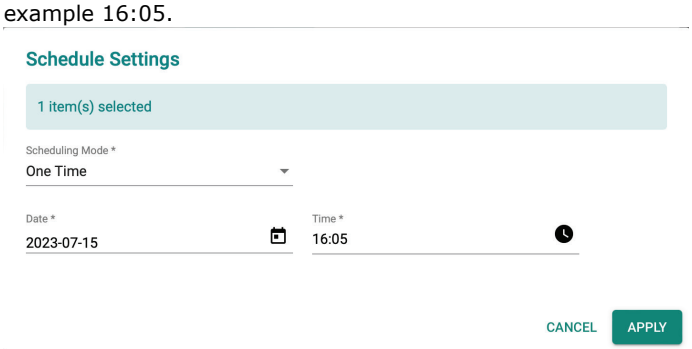
Steps:

1. Navigate to **Device Deployment > General**.
2. Check the box of the device(s) you want to reboot.
3. Click the  icon to configure a reboot schedule for the selected device(s).



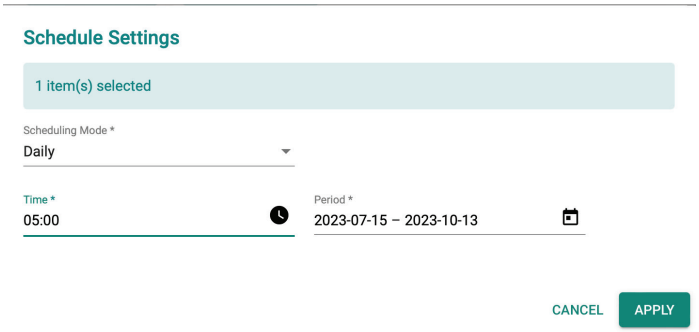
4. Select a scheduling mode:

   a. **One Time**: Select the date and time the device(s) will reboot. One-time schedules can be configured for up to 30 days in the future. The reboot time should be set in 5-minute increments, for example 16:05.

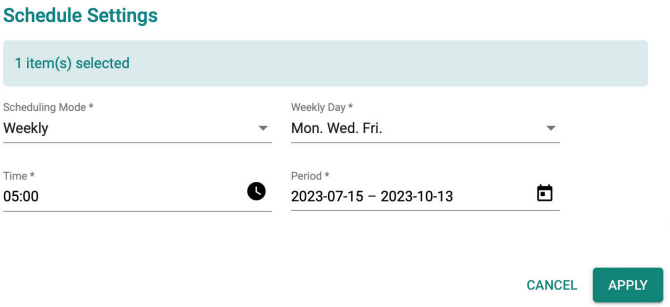


   b. **Daily**: Select the time and the schedule period. Daily schedules can be configured for up to 90 days in the future. For example, the selected device(s) will reboot every day at 05:00 from July 15

through October 13.



c. **Weekly**: Select the day of the week, the time, and schedule period. Weekly schedules can be configured for up to 90 days in the future. For example, the selected device(s) will reboot every Monday, Wednesday, and Friday at 05:00 from July 15 through October 13.

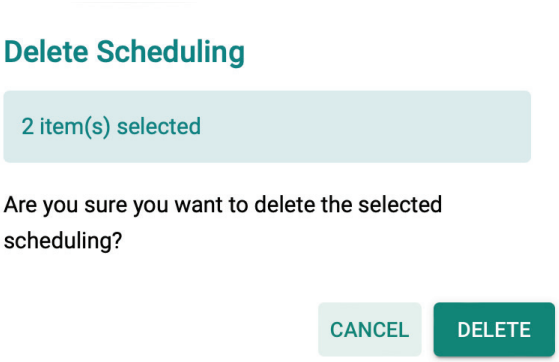


5. Click **APPLY**.

Deleting a Managed Device Reboot Schedule

Steps:

1. Navigate to **Device Deployment > General**.
2. Check the box of the device(s) with the reboot schedule you want to delete.
3. Click the icon to delete the selected reboot schedules.
4. When prompted to confirm, click **DELETE**.

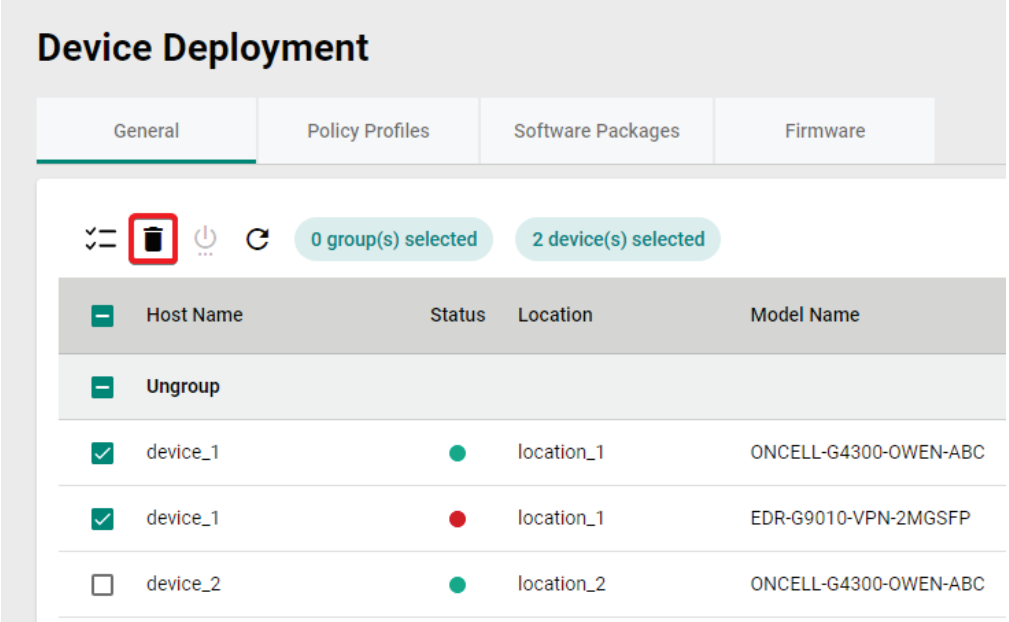


Removing a Managed Device

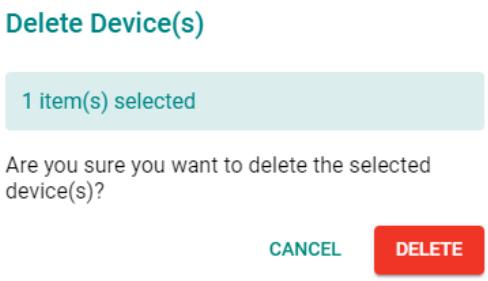
Steps:

1. Navigate to **Device Deployment > General**.

2. Check the box of the device(s) you want to remove.



3. Click the icon to remove the selected device(s).
4. When prompted to confirm, click **DELETE**.



Deploying Policy Profiles to Managed Devices

You can deploy specific policy profiles to managed devices and check the synchronization status between the device and MXsecurity.

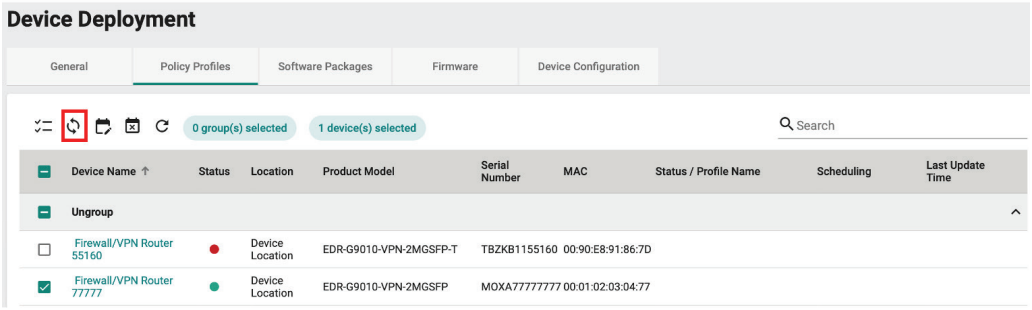
The synchronization status can be one of the following:

- **Sync**: The policy profile has been successfully synced between MXsecurity and the device.
- **Not Sync**: The policy profile failed to synchronize between MXsecurity and the device.
- **Out of Sync**: Indicates the deployed policy profile has been modified on the device side.
- **Sync (modified)**: Indicates the deployed policy profile has been modified in MXsecurity.

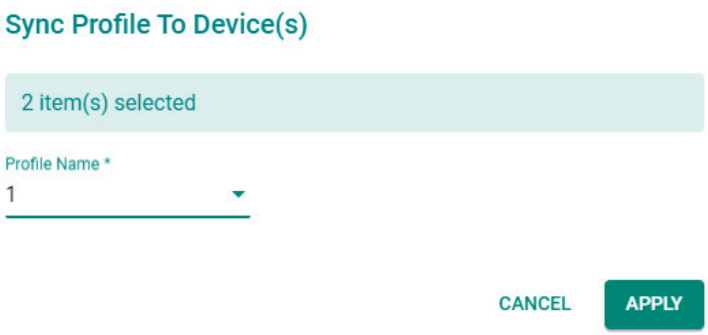
Steps:

1. Navigate to **Device Deployment > Policy Profiles**.
2. Check the box of the device(s) you want to deploy a policy profile to.

3. Click the icon to deploy a policy profile to the selected device(s).



4. Select a previously configured policy profile.
   Refer to Policy Profile Management for instructions on how to create policy profiles.



5. Click **APPLY**.

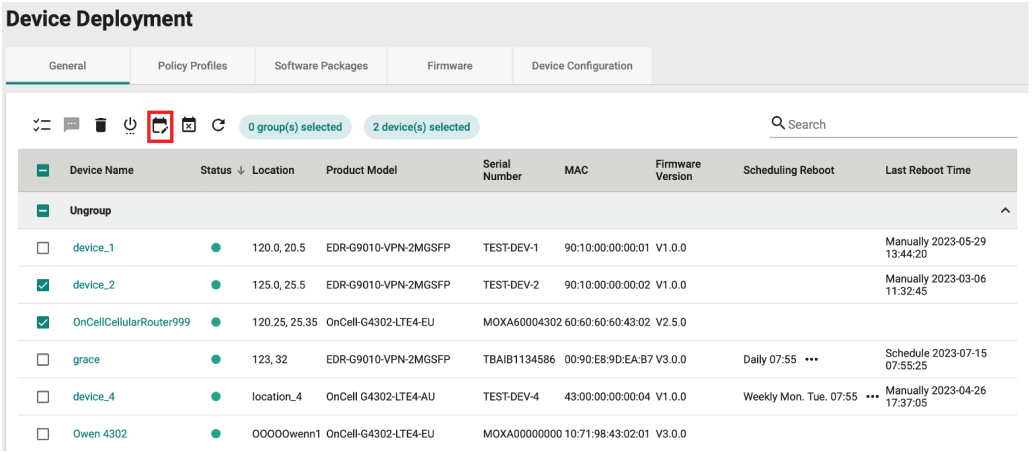
Scheduling a Policy Profile Deployment for Managed Devices

Deploying a policy profile to a device may disrupt services or operations. To minimize the potential impact of policy profile deployments, users can schedule the deployment for specific times where they are least likely to affect operations. Schedules can be configured to execute only once, or on a daily or weekly recurring basis.

Steps:

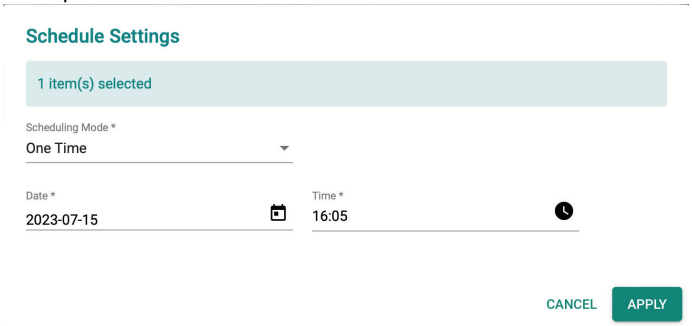
1. Navigate to **Device Deployment > Policy Profiles**.
2. Check the box of the device(s) to configure.

3. Click the icon to configure a policy profile deployment schedule for the selected device(s).

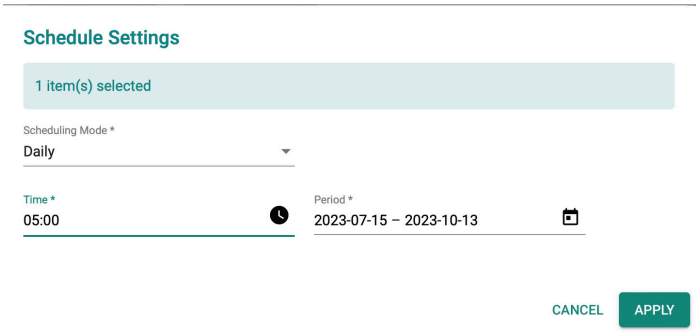


4. Select a scheduling mode:

a. **One Time**: Select the date and time the device(s) will reboot. One-time schedules can be configured for up to 30 days in the future. The reboot time should be set in 5-minute increments, for example 16:05.

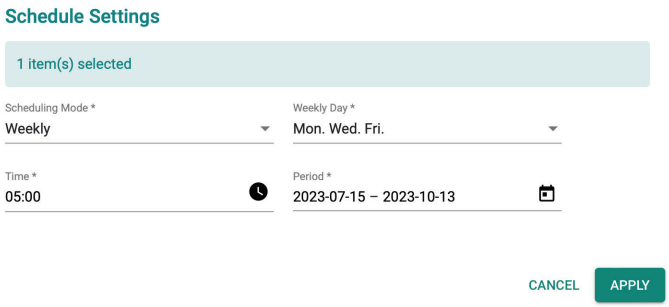


b. **Daily**: Select the time and the schedule period. Daily schedules can be configured for up to 90 days in the future. For example, the selected device(s) will reboot every day at 05:00 from July 15 through October 13.



c. **Weekly**: Select the day of the week, the time, and schedule period. Weekly schedules can be configured for up to 90 days in the future. For example, the selected device(s) will reboot every

Monday, Wednesday, and Friday at 05:00 from July 15 through October 13.

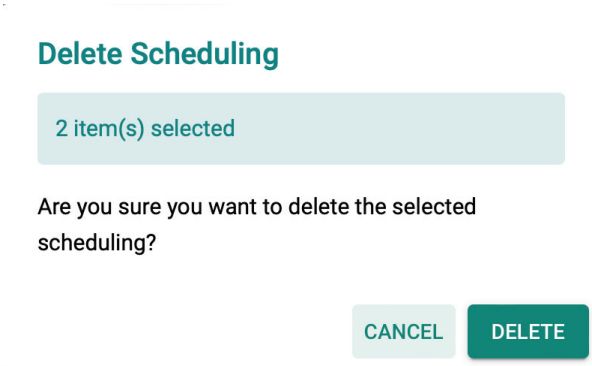


5. Click **APPLY**.

Deleting a Policy Profile Deployment Schedule

Steps:

1. Navigate to **Device Deployment > Policy Profiles**.
2. Check the box of the device(s) with the deployment schedule you want to delete.
3. Click the icon to delete the selected deployment schedules.
4. When prompted to confirm, click **DELETE**.



Upgrading the Software Package of Managed Devices

You can upgrade the software package of managed devices and check basic software package version information.

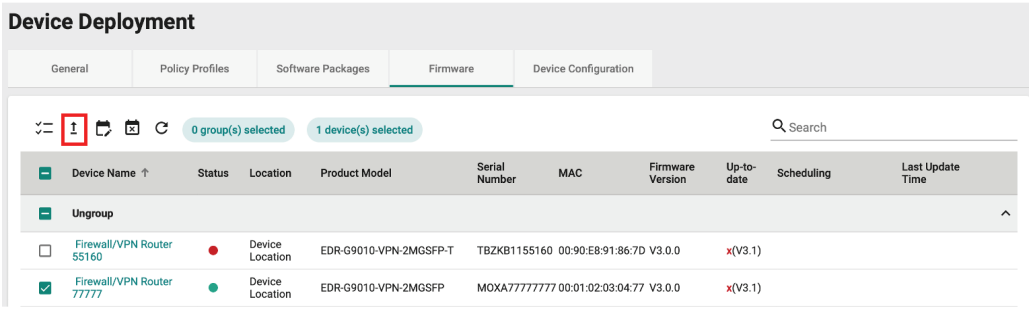
You can check the following software package information:

- **Package Version**: Shows the version of the software package currently installed on the device.
- **Up-To-Date**: Indicates if the currently installed version is up to date. If not, the latest available version will be shown.

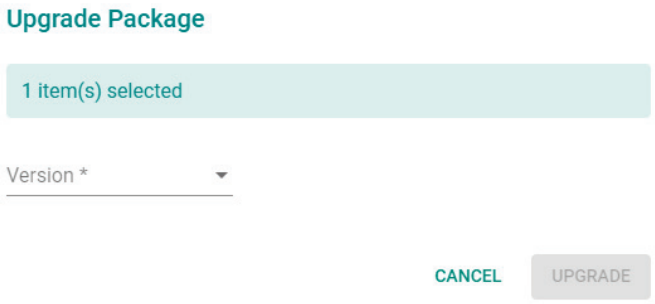
Steps:

1. Navigate to **Device Deployment > Software Packages**.
2. Check the box of the device(s) you want to upgrade the software package for.

3. Click the icon to upgrade the software package for the selected device(s).



4. Select a previously uploaded software package to upgrade to.
Refer to Software Package Management for instructions on how to upload software packages.



5. Click **UPGRADE**.

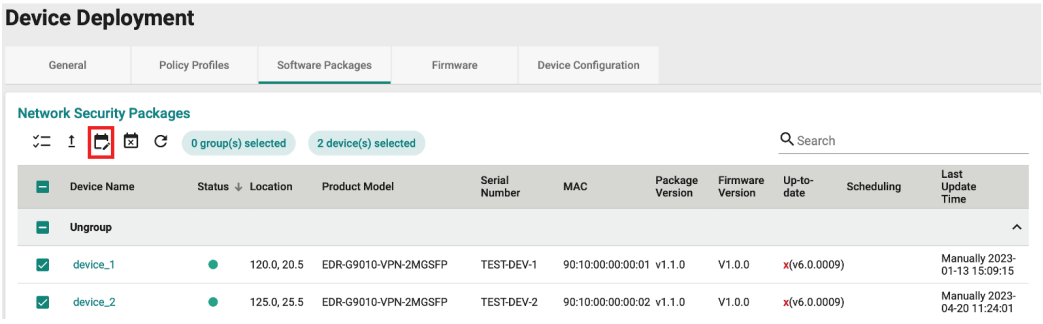
Scheduling a Software Package Deployment for Managed Devices

Deploying a software package to a device may disrupt services or operations. To minimize the potential impact of software package deployments, users can schedule the deployment for specific times where they are least likely to affect operations. Schedules can be configured to execute only once, or on a daily or weekly recurring basis.

Users have the flexibility to choose either a specific version or the "Up-to-date" option for the security package. If the "Up-to-date" option is selected, MXsecurity will deploy the most-recent version available in the management database to the devices.

Steps:

1. Navigate to **Device Deployment > Software Packages**.
2. Check the box of the device(s) to configure.
3. Click the icon to configure a software package deployment schedule for the selected device(s).

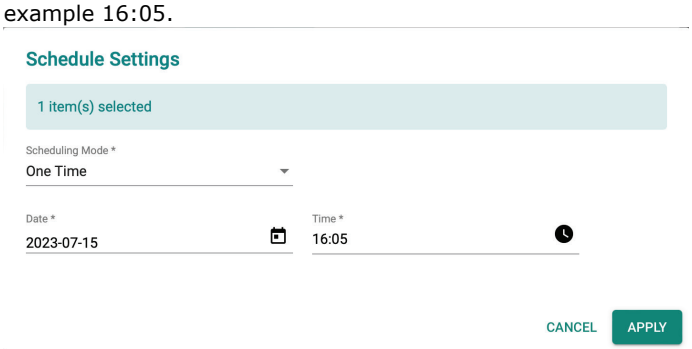


4. Select the software package version to deploy.
If you select **Up-to-date**, MXsecurity will deploy the latest version of the software package available in

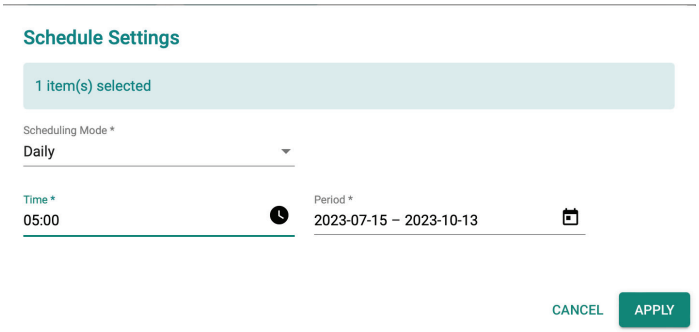
the database. If the device's software package version is the same or newer than the latest database version, the system will not perform the upgrade.

5. Select a scheduling mode:

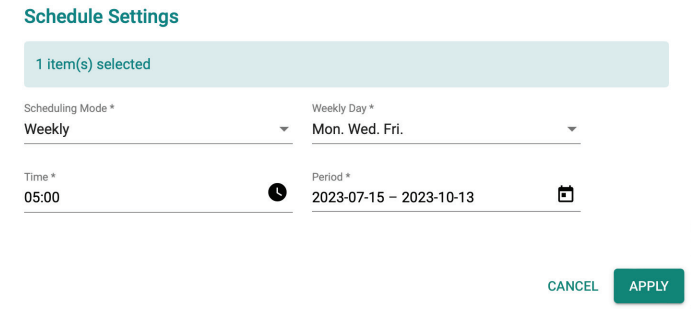
a. **One Time**: Select the date and time the device(s) will reboot. One-time schedules can be configured for up to 30 days in the future. The reboot time should be set in 5-minute increments, for example 16:05.



b. **Daily**: Select the time and the schedule period. Daily schedules can be configured for up to 90 days in the future. For example, the selected device(s) will reboot every day at 05:00 from July 15 through October 13.



c. **Weekly**: Select the day of the week, the time, and schedule period. Weekly schedules can be configured for up to 90 days in the future. For example, the selected device(s) will reboot every Monday, Wednesday, and Friday at 05:00 from July 15 through October 13.

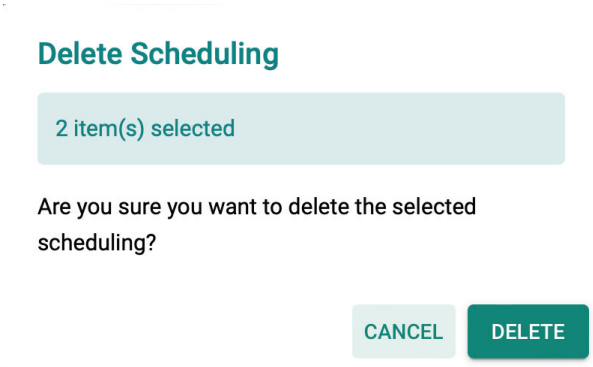


6. Click **APPLY**.

Deleting a Software Package Deployment Schedule

Steps:

1. Navigate to **Device Deployment > Software Packages**.
2. Check the box of the device(s) with the deployment schedule you want to delete.
3. Click the icon to delete the selected deployment schedules.
4. When prompted to confirm, click **DELETE**.



Upgrading the Firmware of Managed Devices

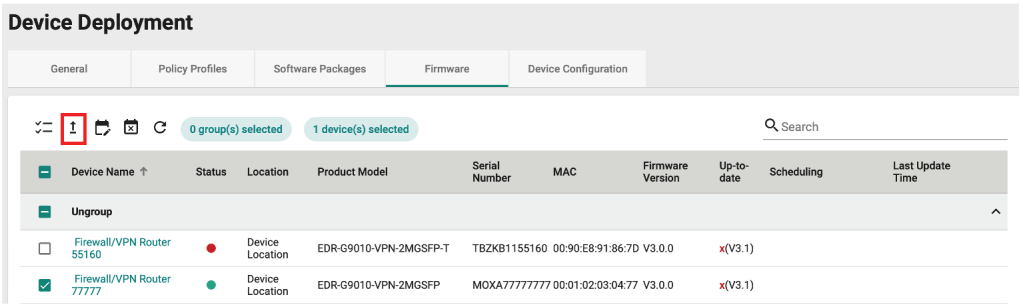
You can upgrade the firmware of managed devices and check basic firmware version information.

You can check the following firmware information:

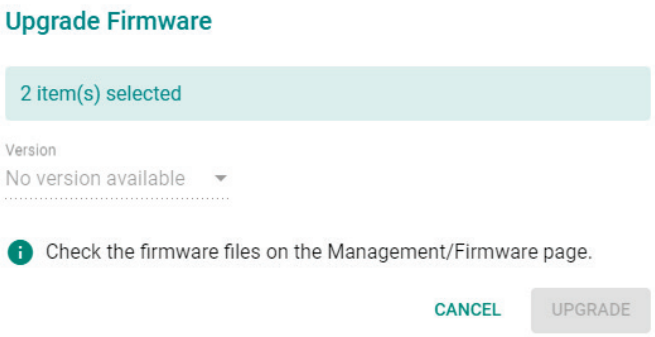
- **Package Version**: Shows the firmware version currently installed on the device.
- **Up-to-date**: Indicates if the currently installed version is up to date. If not, the latest available version will be shown.

Steps:

1. Navigate to **Device Deployment > Firmware**.
2. Check the box of the device(s) you want to upgrade the firmware for.
3. Click the icon to upgrade the firmware for the selected device(s).



4. Select a previously uploaded firmware to upgrade to.
   Refer to Firmware Management for instructions on how to upload firmware.



5. Click **UPGRADE**.

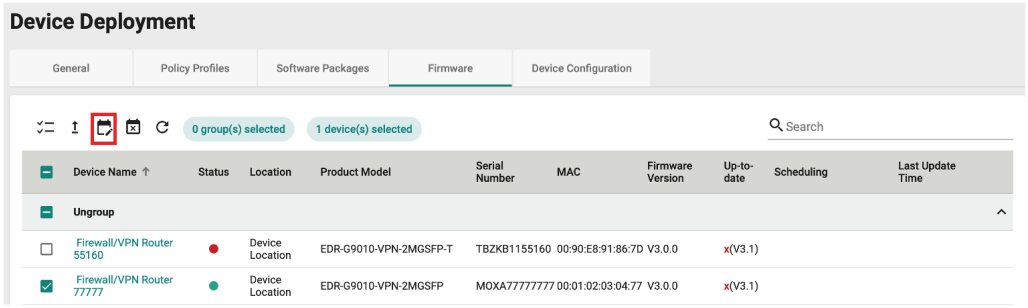
Scheduling a Firmware Deployment for Managed Devices

Deploying firmware to a device may disrupt services or operations. To minimize the potential impact of firmware deployments, users can schedule the deployment for specific times where they are least likely to affect operations. Schedules can be configured to execute only once, or on a daily or weekly recurring basis.

Users have the flexibility to choose either a specific version or the "Up-to-date" option for the firmware. If the "Up-to-date" option is selected, MXsecurity will deploy the most-recent version available in the management database to the devices.

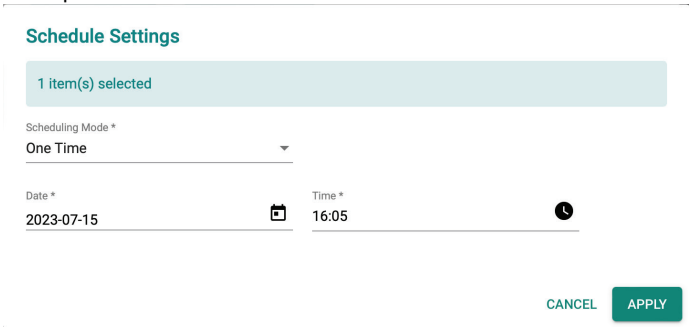
Steps:

1. Navigate to **Device Deployment > Firmware**.
2. Check the box of the device(s) to configure.
3. Click the  icon to configure a firmware deployment schedule for the selected device(s).

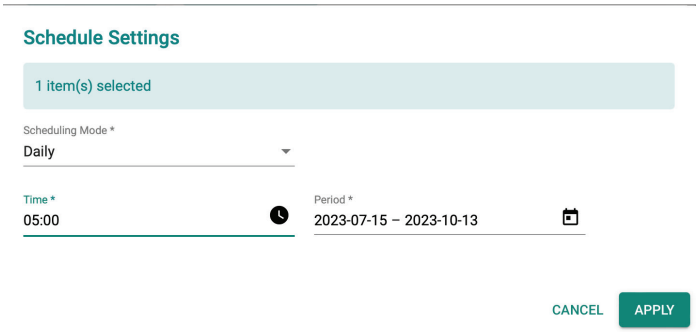


4. Select the firmware version to deploy.
   If you select **Up-to-date**, MXsecurity will deploy the latest version of the firmware available in the database. If the device's firmware version is the same or newer than the latest database version, the system will not perform the upgrade.
5. Select a scheduling mode:

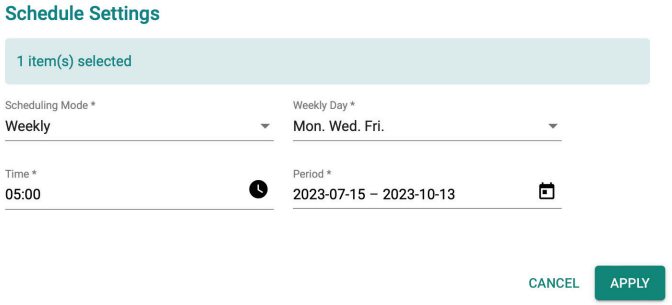
a. **One Time**: Select the date and time the device(s) will reboot. One-time schedules can be configured for up to 30 days in the future. The reboot time should be set in 5-minute increments, for example 16:05.



b. **Daily**: Select the time and the schedule period. Daily schedules can be configured for up to 90 days in the future. For example, the selected device(s) will reboot every day at 05:00 from July 15 through October 13.



c. **Weekly**: Select the day of the week, the time, and schedule period. Weekly schedules can be configured for up to 90 days in the future. For example, the selected device(s) will reboot every Monday, Wednesday, and Friday at 05:00 from July 15 through October 13.



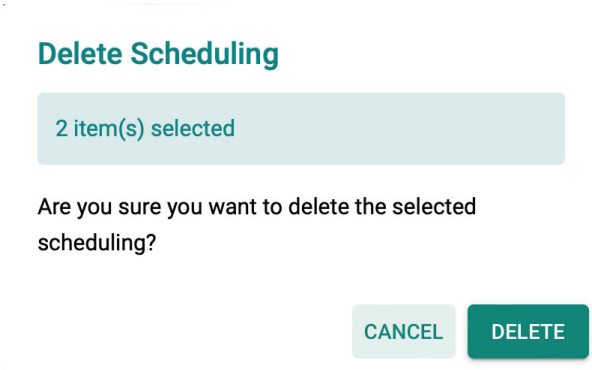
6. Click **APPLY**.

Deleting a Firmware Deployment Schedule

Steps:

1. Navigate to **Device Deployment > Firmware**.
2. Check the box of the device(s) with the deployment schedule you want to delete.
3. Click the icon to delete the selected deployment schedules.

4. When prompted to confirm, click **DELETE**.

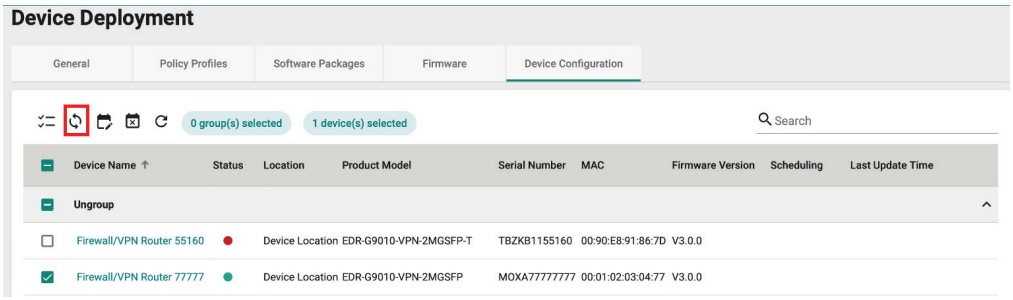


Deploying a Configuration to Managed Devices

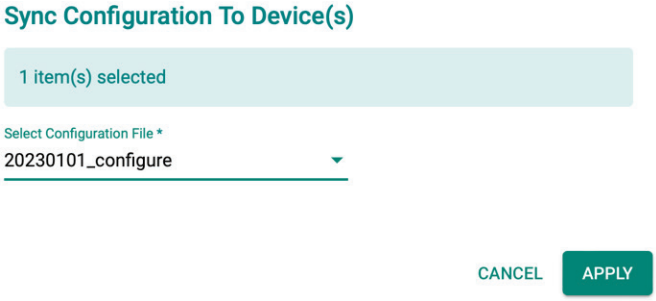
You can deploy a previously uploaded configuration to managed devices. This is useful for quickly deploying an identical configuration to multiple devices at once.

Steps:

6. Navigate to **Device Deployment > Device Configuration**.
7. Check the box of the device(s) you want to deploy the configuration to.
8. Click the icon to deploy the configuration to the selected device(s).



9. Select a previously uploaded device configuration to deploy.
   Refer to Device Configuration Management for instructions on how to upload a configuration.



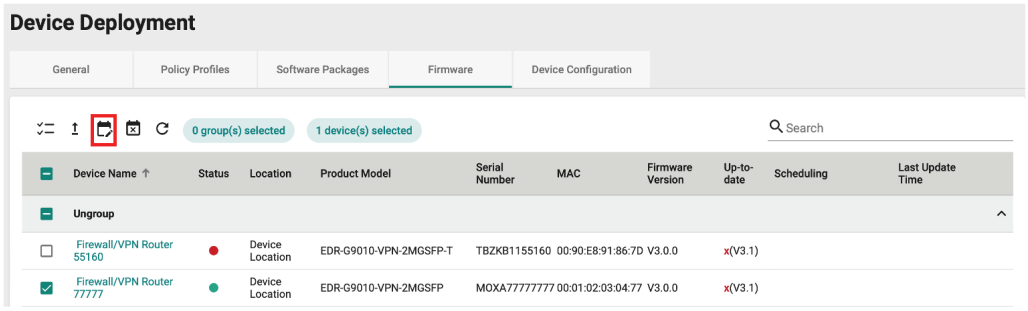
10. Click **APPLY**.

Scheduling a Configuration Deployment for Managed Devices

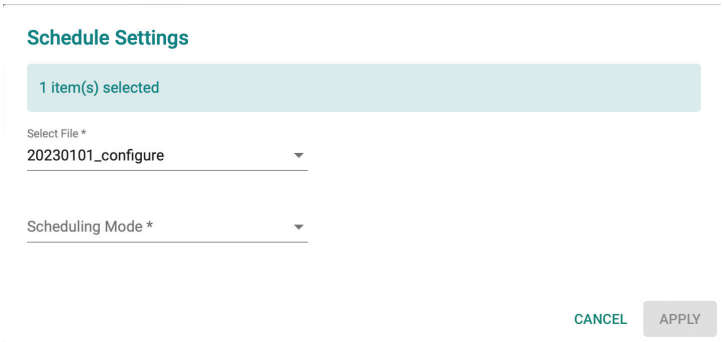
Deploying a configuration to a device may disrupt services or operations. To minimize the potential impact of configuration deployments, users can schedule the deployment for specific times where they are least likely to affect operations. Schedules can be configured to be executed only once, or on a daily or weekly recurring basis.

Steps:

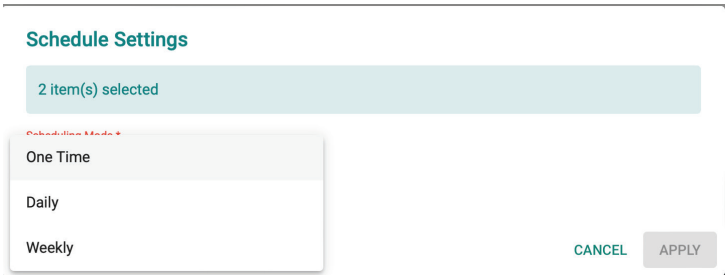
1. Navigate to **Device Deployment > Device Configuration**.
2. Check the box of the device(s) to configure.
3. Click the  icon to configure a configuration deployment schedule for the selected device(s).



4. Select a previously uploaded configuration file to deploy.

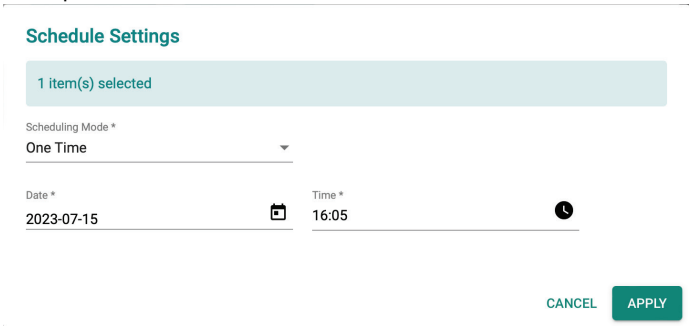


5. Select a scheduling mode:

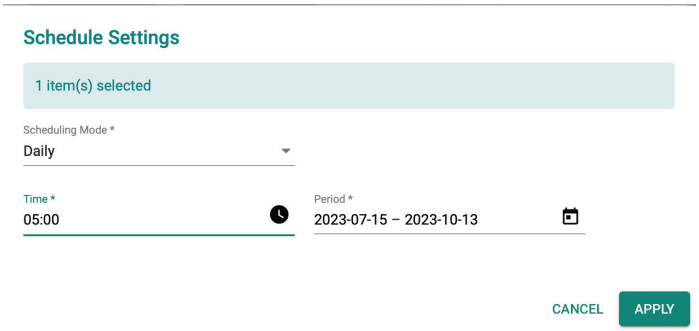


   a. **One Time**: Select the date and time the device(s) will reboot. One-time schedules can be configured for up to 30 days in the future. The reboot time should be set in 5-minute increments, for

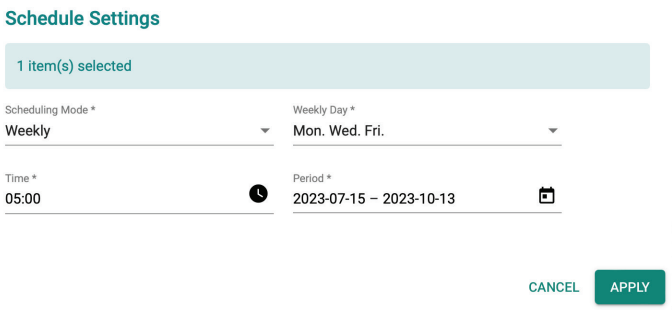
example 16:05.



b. **Daily**: Select the time and the schedule period. Daily schedules can be configured for up to 90 days in the future. For example, the selected device(s) will reboot every day at 05:00 from July 15 through October 13.



c. **Weekly**: Select the day of the week, the time, and schedule period. Weekly schedules can be configured for up to 90 days in the future. For example, the selected device(s) will reboot every Monday, Wednesday, and Friday at 05:00 from July 15 through October 13.



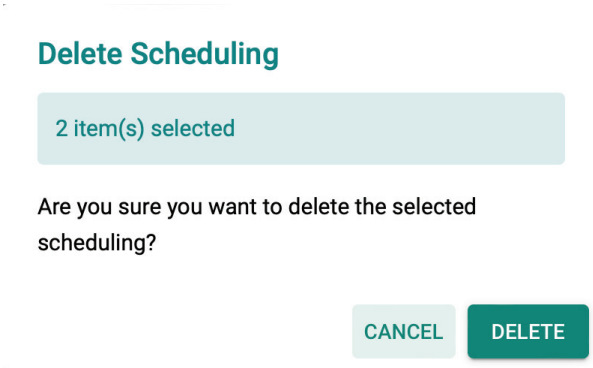
6. Click **APPLY**.

Deleting a Configuration Deployment Schedule

Steps:

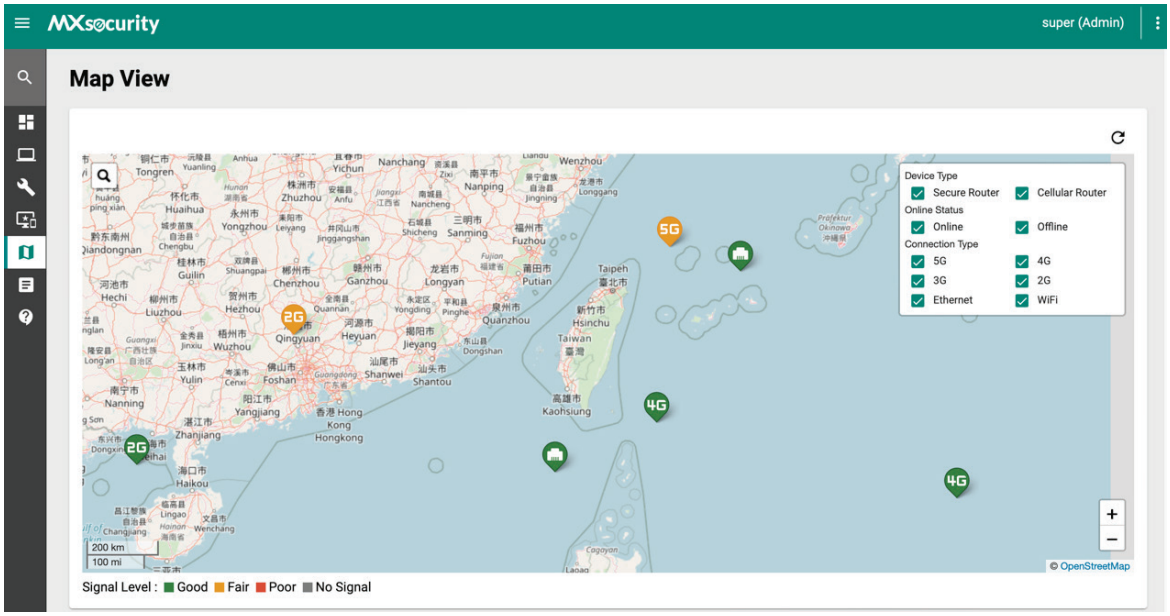
1. Navigate to **Device Deployment > Device Configuration**.
2. Check the box of the device(s) with the deployment schedule you want to delete.
3. Click the icon to delete the selected deployment schedules.

4. When prompted to confirm, click **DELETE**.



8. Map View

The Map View feature allows network administrators to identify the current location of devices, the interfaces in use, and the quality of the connection. For secure routers equipped with a GPS module such as OnCell devices, the map will display their exact location on the map if the GPS function is enabled on the device. For devices without a GPS module, users can manually enter the latitude and longitude details.



Refer to the following sections for more information about each function of the map.

Basic Functions

From the Map View screen, you can perform the following basic functions.

Icon	Function	Description
	Refresh	Click the Refresh button to update the map with the latest GPS data.
	Search	Search for a device by serial number, device name, or MAC address.
	Filter	Filter the devices to display on the map based on device type, online status, and connection type
	Zoom in/out	Click the corresponding icon to zoom in or zoom out on the map. When zoomed out too far, devices in an adjacent area will be grouped together and shown as a single, numbered dot (2). The number inside the dot represents the number of devices in that area. Zoom in to view the device icons individually.

Signal Level

The map shows the current signal strength of managed devices. Refer to the table below for an overview of each status.

Icon	Description
Good Signal	The cellular signal RSSI is higher than -73 dBm or the Ethernet WAN link is up.
Fair Signal	The cellular signal RSSI is between -73 to -89 dBm.
Poor Signal	The cellular signal RSSI is between -89 to -113 dBm.

No Signal	No cellular signal or the Ethernet interface link is down.

Interface in Use

The device icons on the map show which interface is being used to connect to the Internet. Refer to the table below for an overview of each interface.

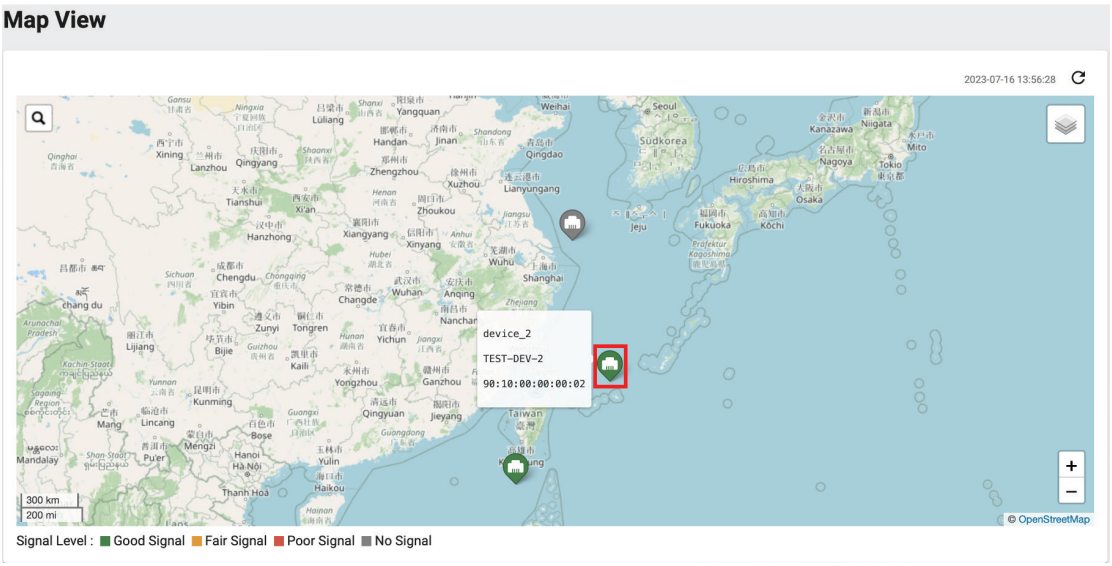
Icon	Description
	The device is using Ethernet WAN to connect to the internet.
	The device is using cellular 5G to connect to the internet.
	The device is using cellular 4G to connect to the internet.
	The device is using cellular 3G to connect to the internet.
	The device is using cellular 2G to connect to the internet.
	The device is using Wi-fi to connect to the internet.

Viewing Detailed Device Information

Clicking the device icon on the map or the device name from the No Location Devices list will bring up additional information about the device.

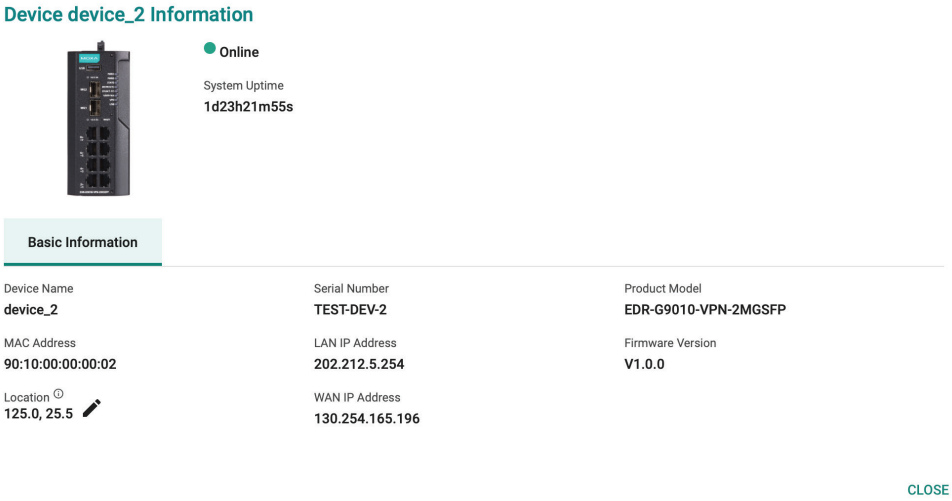
Steps:

1. Navigate to **Map View.**
2. Click the device's icon on the map or the device name in the No Location Devices list.

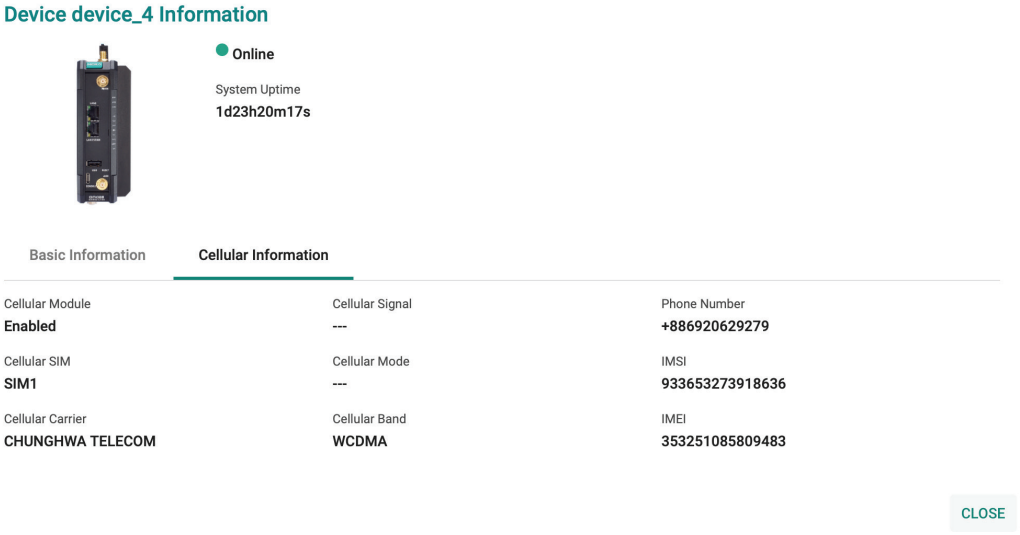


3. Depending on the selected device, the following information will be shown:

a. **Basic Information**: Basic information about the device, including device name, model, S/N, IP LAN/WAN address, MAC address, location, and firmware version.



b. **Cellular Information**: Information about the cellular interface, connection, carrier, and SIM. This is only available for OnCell devices.



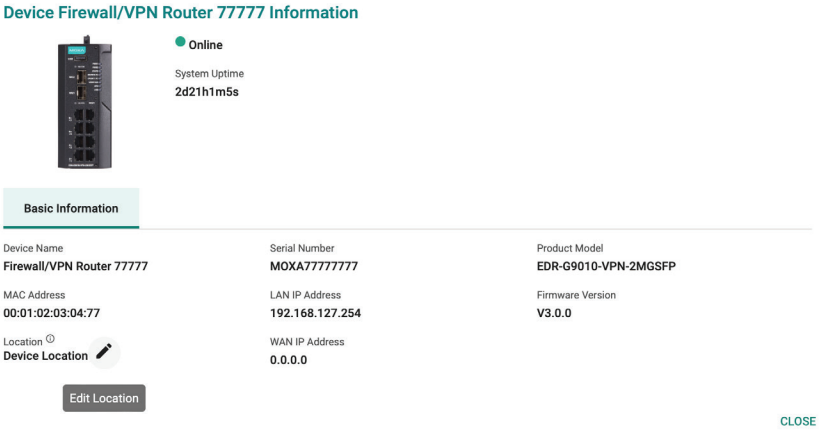
Editing the Location of a Device

For managed devices that do not support GPS or have their GPS module disabled, users can manually enter geographic coordinates to display the device on the map.

Steps:

1. Navigate to **Map View.**
2. In the No Location Devices list, click the device name.

3. Click the icon in the Location field.



4. Enter the longitude and latitude coordinates.

5. Click .

6. Click the icon on the map to refresh the map.
   The device will now appear on the map based on the specified coordinates.

9. Report

The Report function simplifies audits and reviewing cellular secure router performance. Users can also set up an email server to send reports directly to network administrators.

This section will provide information for the following reports:

- **Inventory Reports:** List of all assets of the devices in the field.
- **Cellular Signal Reports:** The signal status of managed cellular secure routers.
- **Data Usage Reports:** The status of the managed cellular secure routers' SIM card data usage.
- **Trail Reports:** The GPS movement tracking records of managed cellular secure routers.

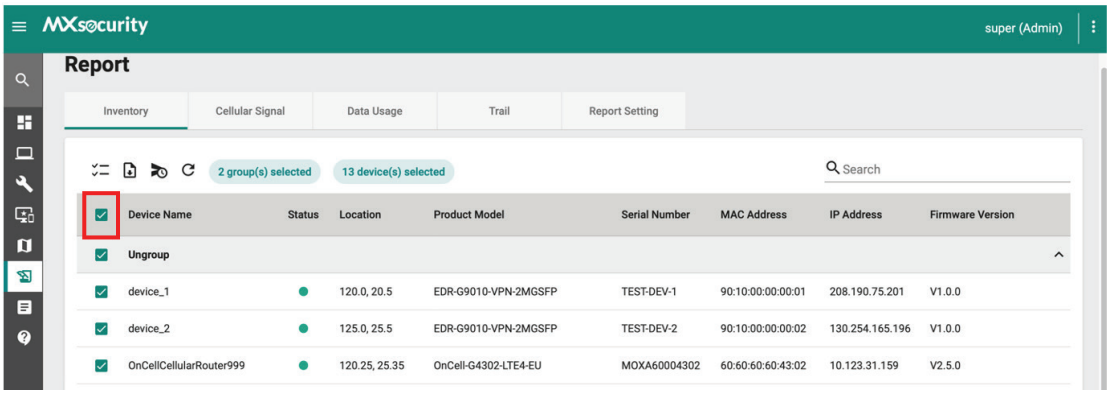
Inventory Reports

Generating a Current Inventory Report

Inventory reports make it easier for users to conduct audits and to monitor the number of field devices and their status.

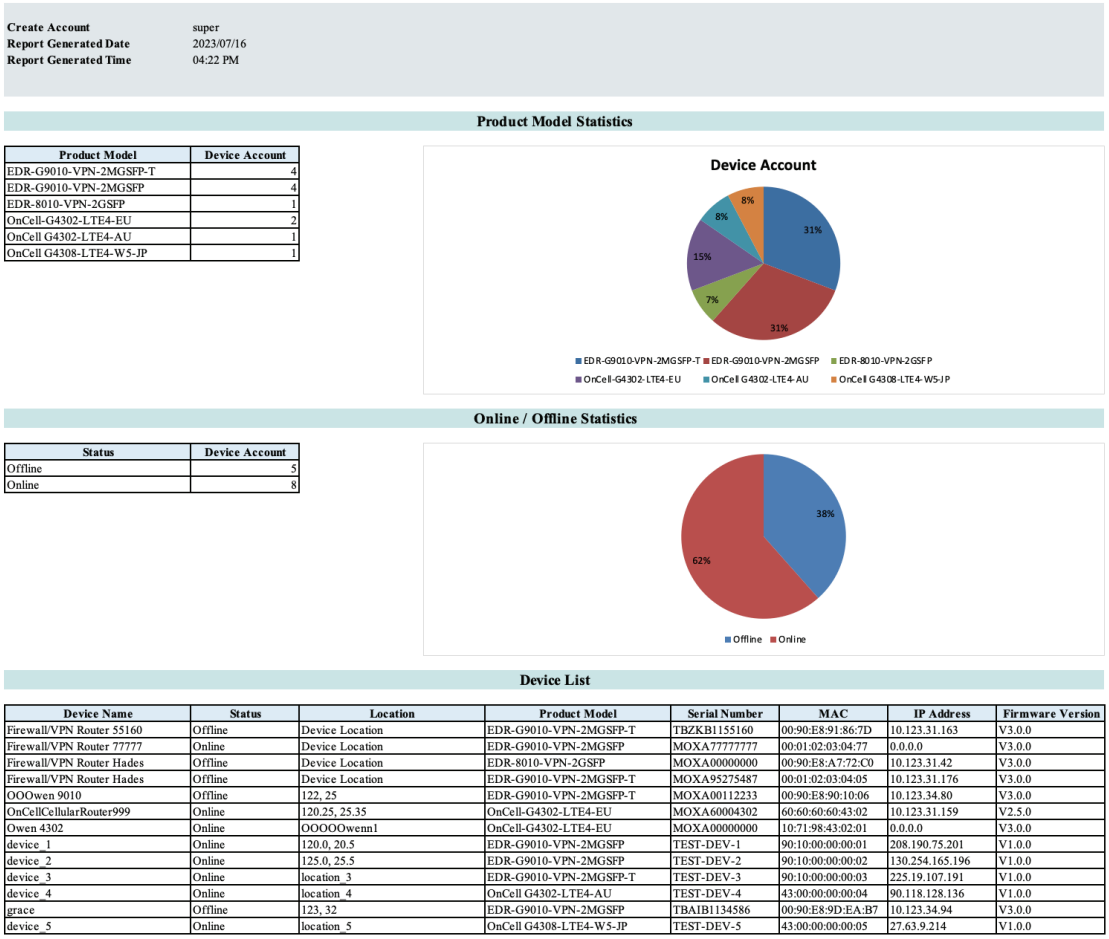
Steps:

1. Navigate to **Report > Inventory**.
2. Select all devices.



3. Click the  icon to generate a report in CSV format.

The inventory report includes the following information:



Create Account super
Report Generated Date 2023/07/16
Report Generated Time 04:22 PM

Product Model Statistics

Product Model	Device Account
EDR-G9010-VPN-2MGSFP-T	4
EDR-G9010-VPN-2MGSFP	4
EDR-8010-VPN-2GSFP	1
OnCell-G4302-LTE4-EU	2
OnCell G4302-LTE4-AU	1
OnCell G4308-LTE4-W5-JP	1

Online / Offline Statistics

Status	Device Account
Offline	5
Online	8

Device List

Device Name	Status	Location	Product Model	Serial Number	MAC	IP Address	Firmware Version
Firewall/VPN Router 55160	Offline	Device Location	EDR-G9010-VPN-2MGSFP-T	TBZKB1155160	00:90:E8:91:86:7D	10.123.31.163	V3.0.0
Firewall/VPN Router 77777	Online	Device Location	EDR-G9010-VPN-2MGSFP	MOXA77777777	00:01:02:03:04:77	0.0.0.0	V3.0.0
Firewall/VPN Router Hades	Offline	Device Location	EDR-8010-VPN-2GSFP	MOXA00000000	00:90:E8:A7:72:C0	10.123.31.42	V3.0.0
Firewall/VPN Router Hades	Offline	Device Location	EDR-G9010-VPN-2MGSFP-T	MOXA95275487	00:01:02:03:04:05	10.123.31.176	V3.0.0
OOOwen 9010	Offline	122, 25	EDR-G9010-VPN-2MGSFP-T	MOXA00112233	00:90:E8:90:10:06	10.123.34.80	V3.0.0
OnCellCellularRouter999	Online	120.25, 25.35	OnCell-G4302-LTE4-EU	MOXA60004302	60:60:60:60:43:02	10.123.31.159	V2.5.0
Owen 4302	Online	OOOOOwenn1	OnCell-G4302-LTE4-EU	MOXA00000000	10:71:98:43:02:01	0.0.0.0	V3.0.0
device_1	Online	120.0, 20.5	EDR-G9010-VPN-2MGSFP	TEST-DEV-1	90:10:00:00:00:01	208.190.75.201	V1.0.0
device_2	Online	125.0, 25.5	EDR-G9010-VPN-2MGSFP	TEST-DEV-2	90:10:00:00:00:02	130.254.165.196	V1.0.0
device_3	Online	location_3	EDR-G9010-VPN-2MGSFP-T	TEST-DEV-3	90:10:00:00:00:03	225.19.107.191	V1.0.0
device_4	Online	location_4	OnCell G4302-LTE4-AU	TEST-DEV-4	43:00:00:00:00:04	90.118.128.136	V1.0.0
grace	Offline	123, 32	EDR-G9010-VPN-2MGSFP	TBAIB1134586	00:90:E8:9D:EA:B7	10.123.34.94	V3.0.0
device_5	Online	location_5	OnCell G4308-LTE4-W5-JP	TEST-DEV-5	43:00:00:00:00:05	27.63.9.214	V1.0.0

The following table describes the report's fields.

Field	Description
Create Account	The MXsecurity account used to generate the report.
Report Generated Date	The date the report was generated.
Report Generated Time	The time the report was generated.
Product Model Statistics	A summary of the total number of managed devices, organized according by product model.
Online / Offline Statistics	A summary of the total number of managed devices, organized according by status.

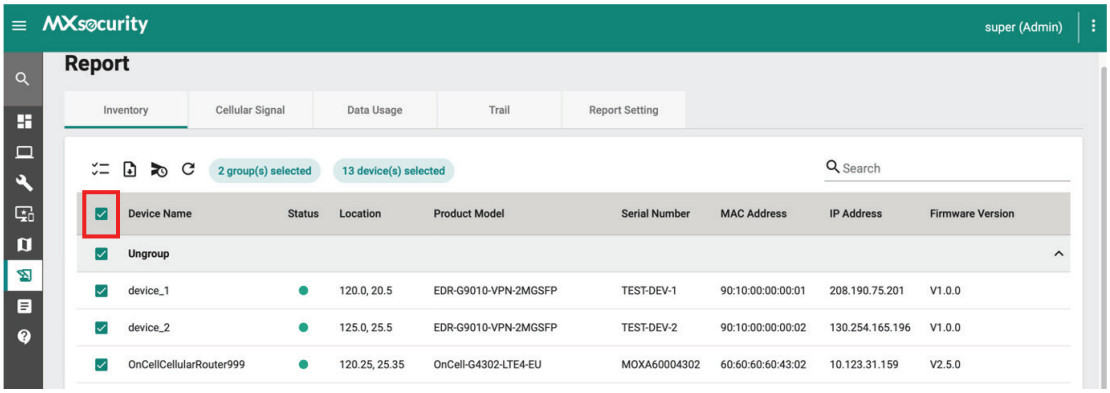
Scheduling an Inventory Report

Users can generate inventory reports according to a pre-configured schedule and automatically send it to specified recipients by email.

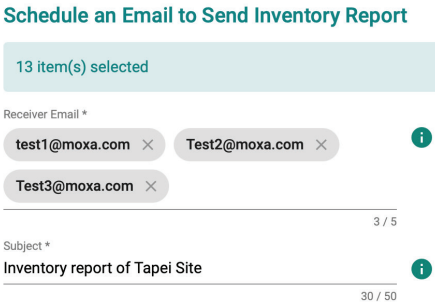
Steps:

1. Navigate to **Report > Inventory**.

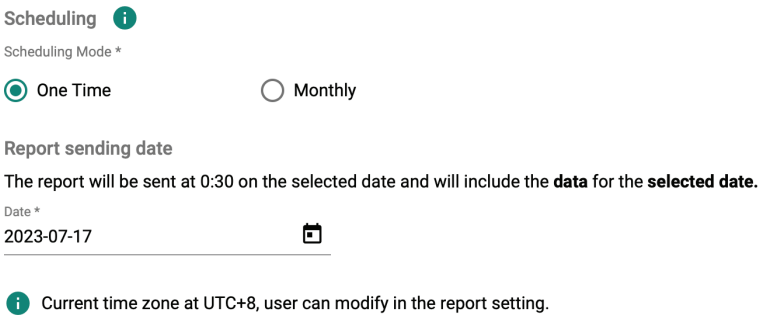
2. Select all devices.



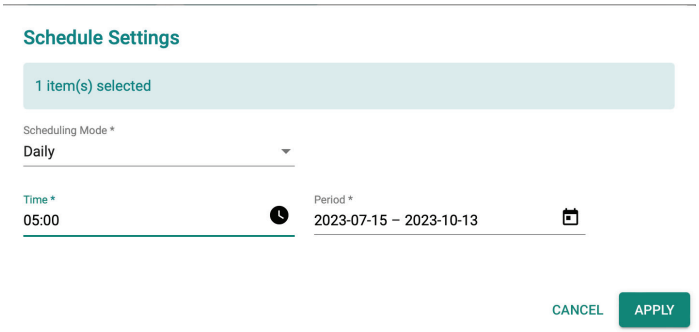
3. Click the icon to configure a report schedule.
4. Specify the email recipients for the report. You can specify up to 5 recipients.
5. Enter the subject. This will act as the report email subject.



6. Select a scheduling mode:
   a. **One Time**: Select the report date. One-time schedules can be configured for up to one year in the future.



   b. **Monthly**: Select the report date and period. Monthly schedules can be configured for up to one year in the future.



7. Click **APPLY**.
   The schedule will appear on the **Report > Report Setting > Schedule Report** page.

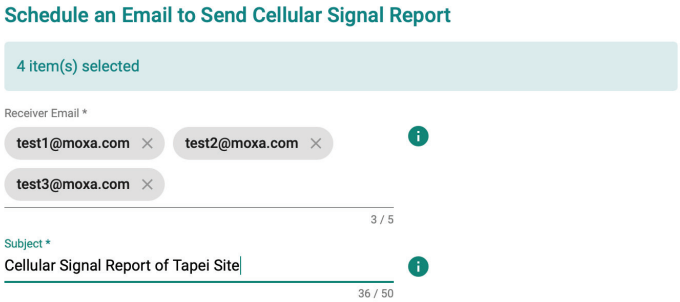
Cellular Signal Reports

Scheduling a Cellular Signal Report

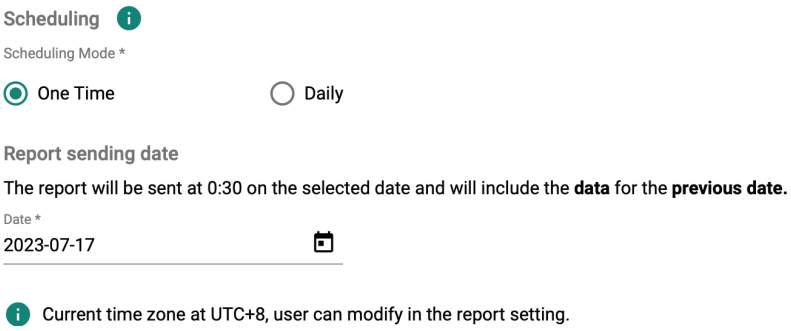
Users can generate cellular signal reports according to a pre-configured schedule and automatically send these reports to specified recipients via email.

Steps:

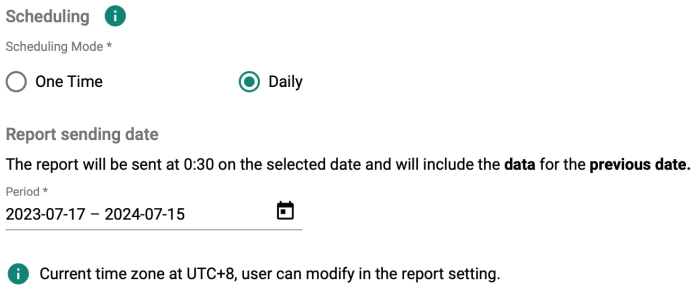
1. Navigate to **Report > Cellular Signal**.
2. Select the device(s) you want to generate a report for.
3. Click the icon to configure a report schedule.
4. Specify the email recipients for the report. You can specify up to 5 recipients.
5. Enter the subject. This will act as the report email subject.



6. Select a scheduling mode:
   a. **One Time**: Select the report date. One-time schedules can be configured for up to one year in the future. To ensure complete 24-hour data, the report data will be of the day prior to the report date.



   b. **Daily**: Select the report period. Monthly schedules can be configured for up to one year in the future. To ensure complete 24-hour data, the report data will be of the day prior to the report date.



7. Click **APPLY**.
   The schedule will appear on the **Report > Report Setting > Schedule Report** page.

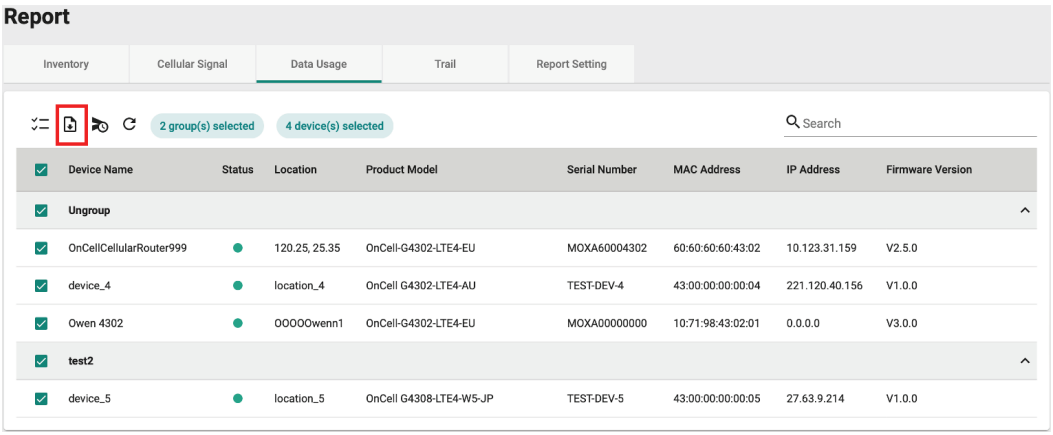
Data Usage Reports

Generating a Cellular Data Usage Report

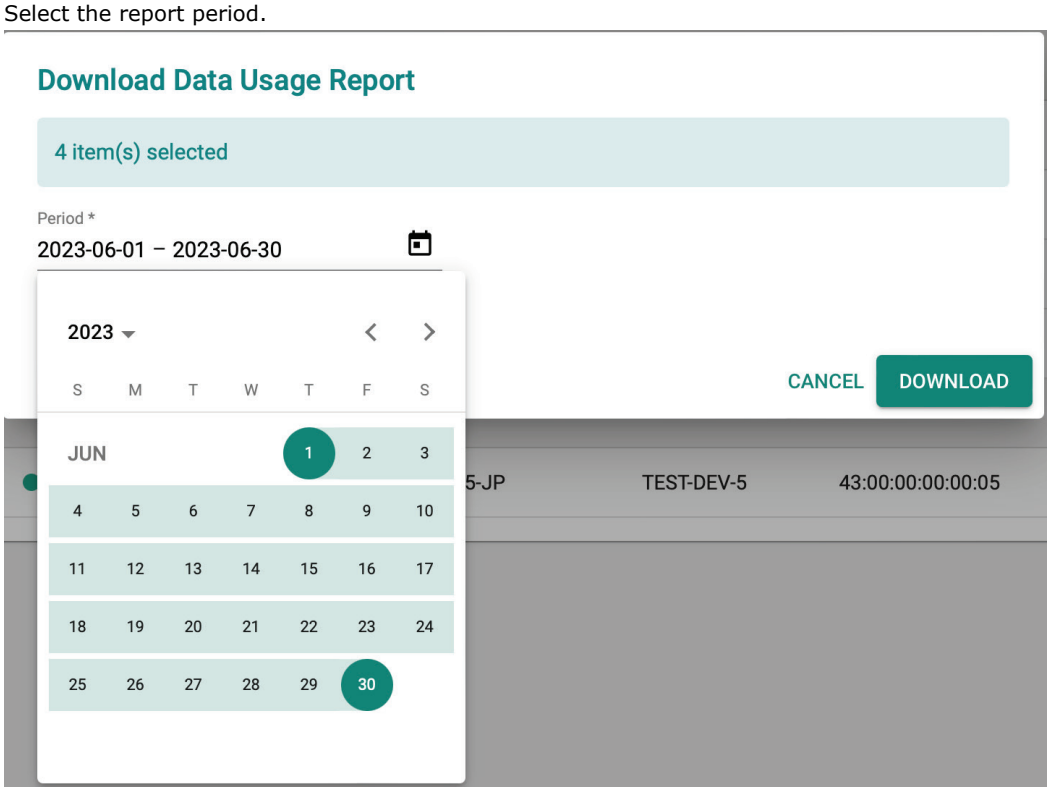
Cellular data usage reports provide useful insights into the data usage of SIM cards for a specific period. The report will include a separate CSV file for each selected OnCell secure router.

Steps:

1. Navigate to **Report > Data Usage**.
2. Select the device(s) you want to generate a report for.
3. Click the  icon to generate a report in CSV format.



4. Select the report period.

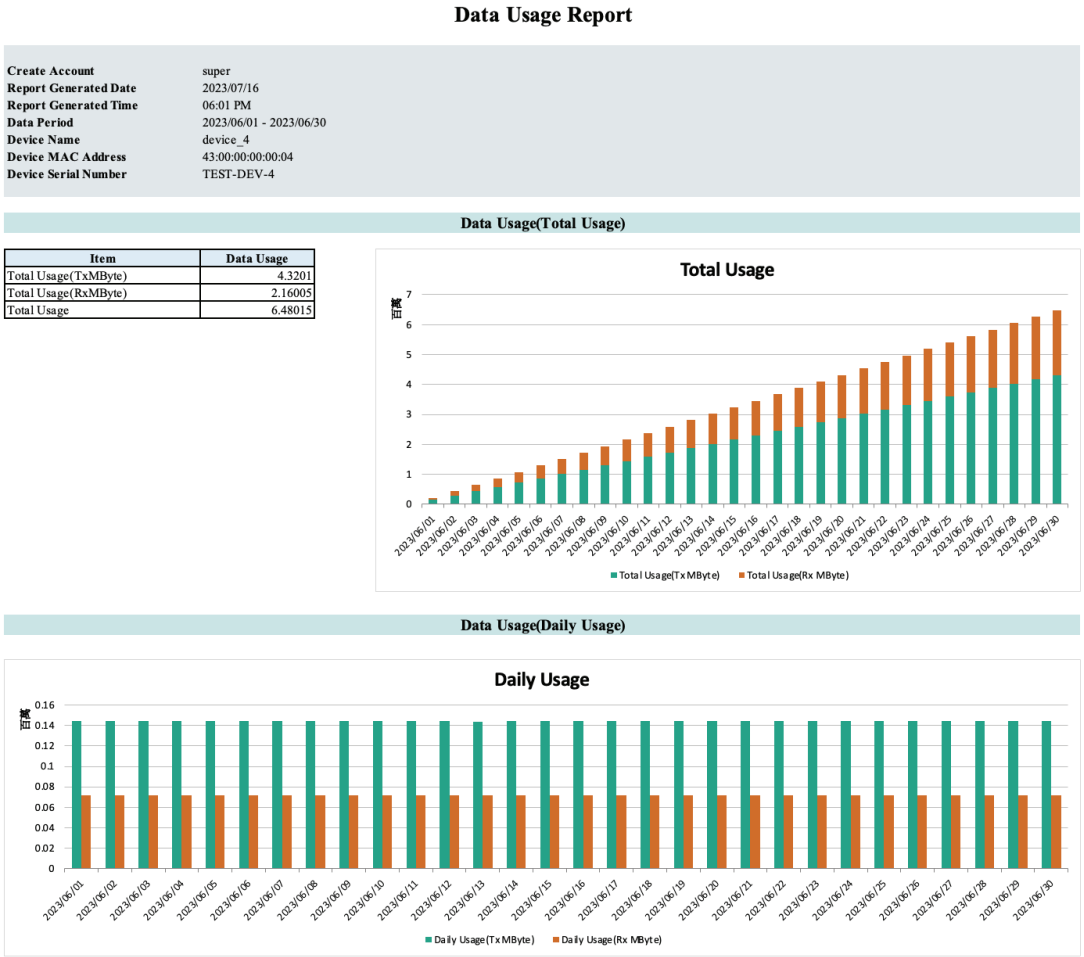


> **NOTE**
>
> You can select a period of up to 30 days within the last 90 days.

> **NOTE**
>
> If you select the current day, the data included in the report will span from 00:00 of that day to the present time.

5. Click **DOWNLOAD**.

The cellular data usage report includes the following information:



Data Usage Report

Create Account	super
Report Generated Date	2023/07/16
Report Generated Time	06:01 PM
Data Period	2023/06/01 - 2023/06/30
Device Name	device_4
Device MAC Address	43:00:00:00:00:04
Device Serial Number	TEST-DEV-4

Data Usage(Total Usage)

Item	Data Usage
Total Usage(TxMByte)	4.3201
Total Usage(RxMByte)	2.16005
Total Usage	6.48015

Data Usage(Daily Usage)

The following table describes the report's fields.

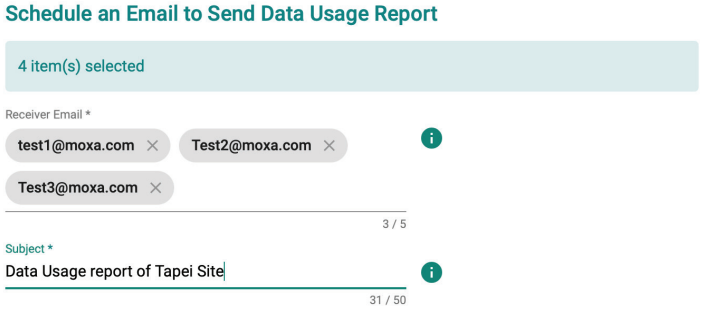
Field	Description
Create Account	The MXsecurity account used to generate the report.
Report Generated Date	The date the report was generated.
Report Generated Time	The time the report was generated.
Data Period	The period for which the data was collected.
Device Name	The name of the device.
Device MAC Address	The device MAC address.
Device Serial Number	The device serial number.
Data Usage (Total Usage)	Summary chart showing the cumulative total data usage in MB.
Data Usage (Daily Usage)	Summary chart showing the daily data usage in MB.

Scheduling a Cellular Data Usage Report

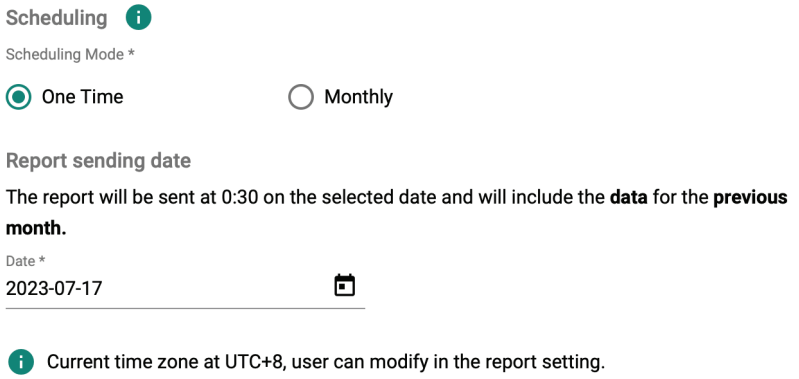
Users can generate cellular data usage reports according to a pre-configured schedule and automatically send these reports to specified recipients via email.

Steps:

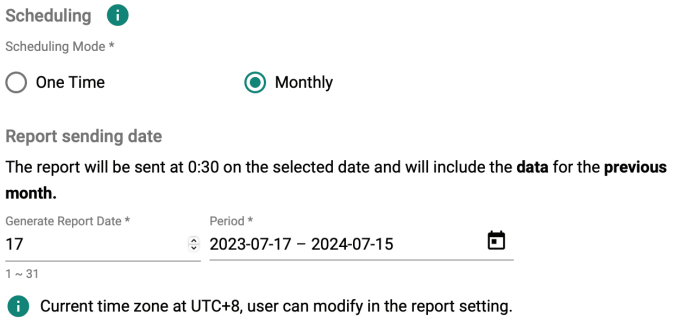
1. Navigate to **Report > Data Usage**.
2. Select the device(s) you want to generate a report for.
3. Click the  icon to configure a report schedule.
4. Specify the email recipients for the report. You can specify up to 5 recipients.
5. Enter the subject. This will act as the report email subject.



6. Select a scheduling mode:
   a. **One Time**: Select the report date. One-time schedules can be configured for up to one year in the future. To ensure complete 30-day data, the report data will be of the month prior to the report date.



   b. **Monthly**: Select the report date and period. Monthly schedules can be configured for up to one year in the future. To ensure complete 30-day data, the report data will be of the month prior to the report date.



7. Click **APPLY**.
   The schedule will appear on the **Report > Report Setting > Schedule Report** page.

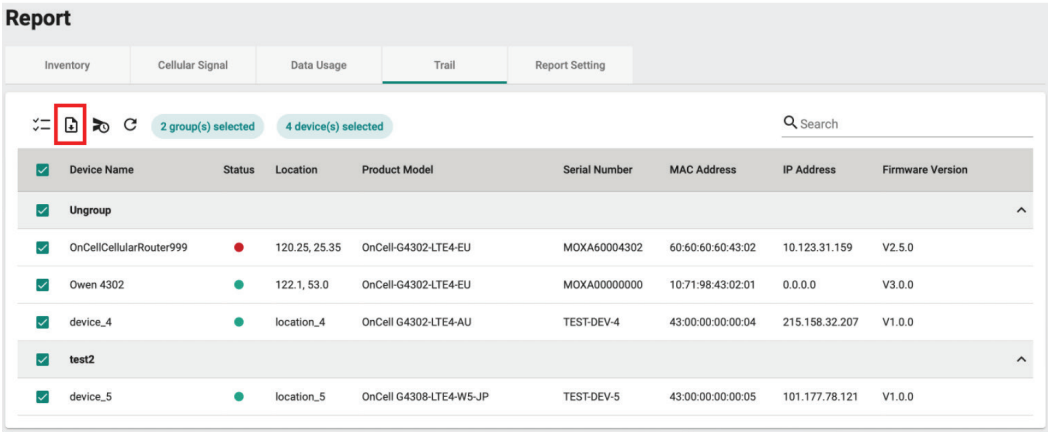
Trail Reports

Generating a Trail Report

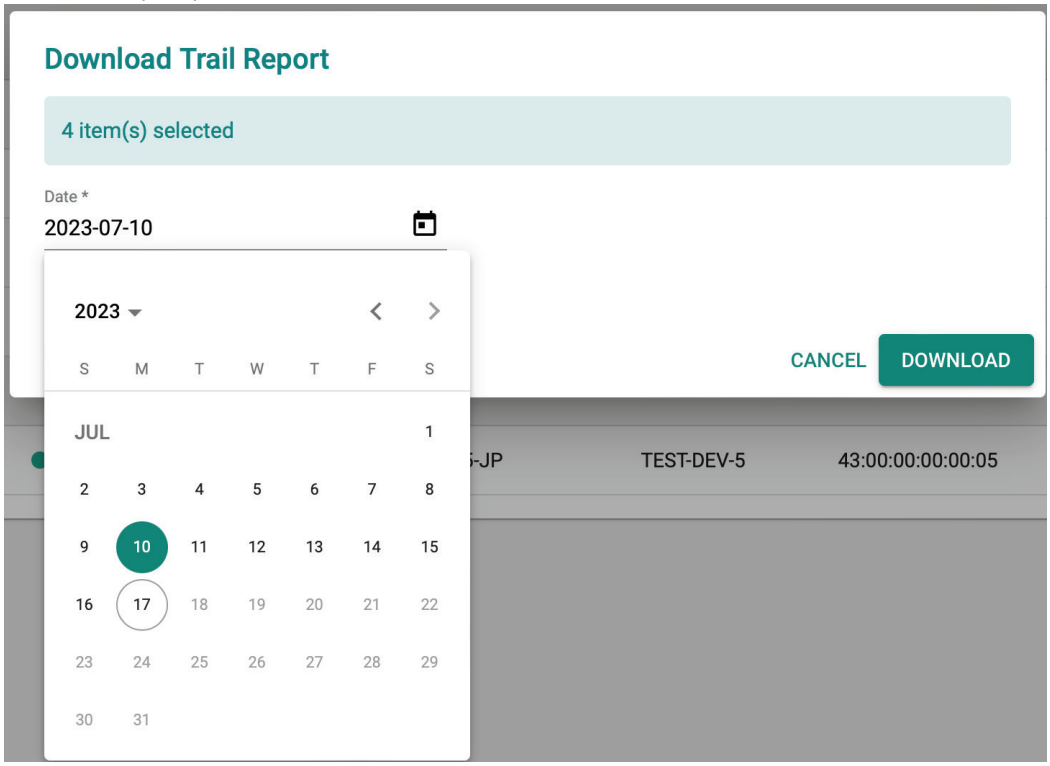
Trail reports let users compile GPS trail records for each device. This information is useful for auditing and management purposes. The collected data can help optimize operations in a variety of applications. For example, trail reports can show the trajectory of a vehicle with an OnCell secure router on board using GPS trail records. Based on this report data, administrators can optimize vehicles routes and schedules.

Steps:

1. Navigate to **Report > Trail**.
2. Select the device(s) you want to generate a report for.
3. Click the  icon to generate a report in CSV format.



4. Select the report period.



> **NOTE**
>
> You can select a period of up to 30 days within the last 90 days.

> **NOTE**
>
> If you select the current day, the data included in the report will span from 00:00 of that day to the present time.

5. Click **DOWNLOAD**.

The trail report includes the timestamps and GPS coordinates of the device. Users can import this data into third-party software to visualize the locations of the device.

A	B	C
Time	Latitude	Longitude
2023/07/14 00:00	29.31019	124.8241
2023/07/14 00:01	29.21019	124.7241
2023/07/14 00:02	29.26019	124.6741
2023/07/14 00:03	29.36019	124.7241
2023/07/14 00:04	29.31019	124.7741
2023/07/14 00:05	29.21019	124.8741
2023/07/14 00:06	29.16019	124.8241
2023/07/14 00:07	29.06019	124.9241
2023/07/14 00:08	29.16019	125.0241
2023/07/14 00:09	29.11019	124.9241
2023/07/14 00:10	29.06019	124.8241
2023/07/14 00:11	29.16019	124.9241
2023/07/14 00:12	29.21019	124.9741
2023/07/14 00:13	29.16019	125.0741
2023/07/14 00:14	29.26019	125.1741
2023/07/14 00:15	29.21019	125.2241
2023/07/14 00:16	29.26019	125.2741
2023/07/14 00:17	29.21019	125.3241
2023/07/14 00:18	29.16019	125.2741
2023/07/14 00:19	29.26019	125.3241
2023/07/14 00:20	29.21019	125.2741
2023/07/14 00:21	29.11019	125.3241
2023/07/14 00:22	29.01019	125.2241
2023/07/14 00:23	28.96019	125.3241

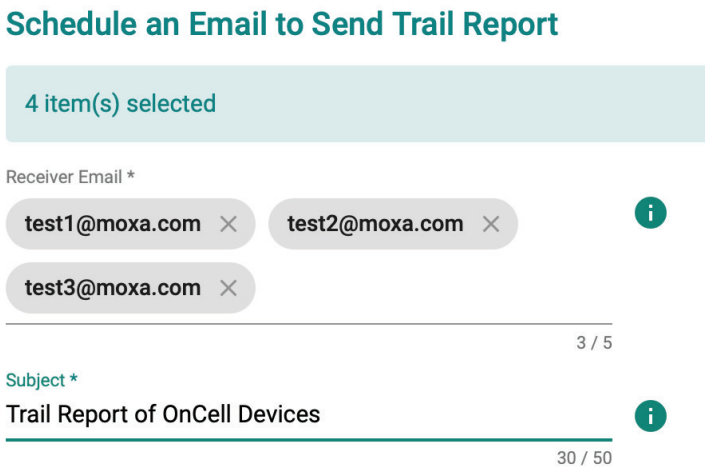
Scheduling a Trail Report

Users can generate trail reports according to a pre-configured schedule and automatically send these reports to specified recipients via email.

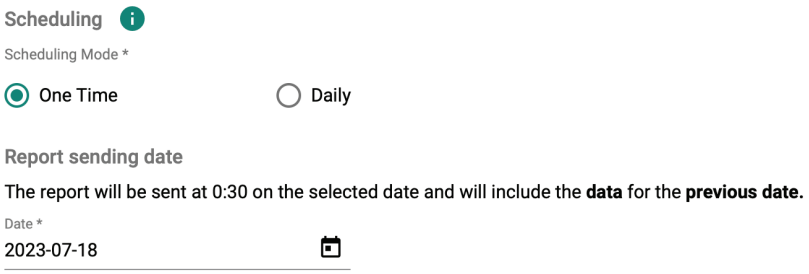
Steps:

1. Navigate to **Report > Trail**.
2. Select the device(s) you want to generate a report for.
3. Click the  icon to configure a report schedule.
4. Specify the email recipients for the report. You can specify up to 5 recipients.

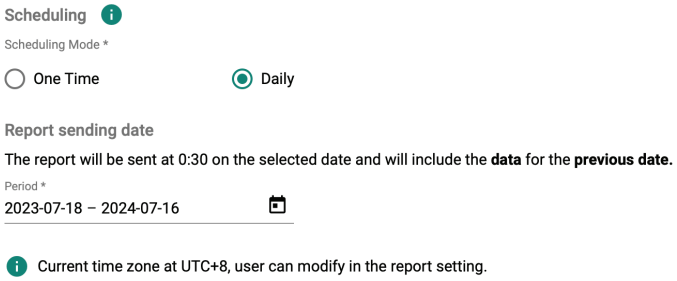
5. Enter the subject. This will act as the report email subject.



6. Select a scheduling mode:
   a. **One Time**: Select the report date. One-time schedules can be configured for up to one year in the future. To ensure complete 24-hour data, the report data will be of the day prior to the report date.



   b. **Daily**: Select the report date and period. Monthly schedules can be configured for up to one year in the future. To ensure complete 24-hour data, the report data will be of the day prior to the report date.



7. Click **APPLY**.
   The schedule will appear on the **Report > Report Setting > Schedule Report** page.

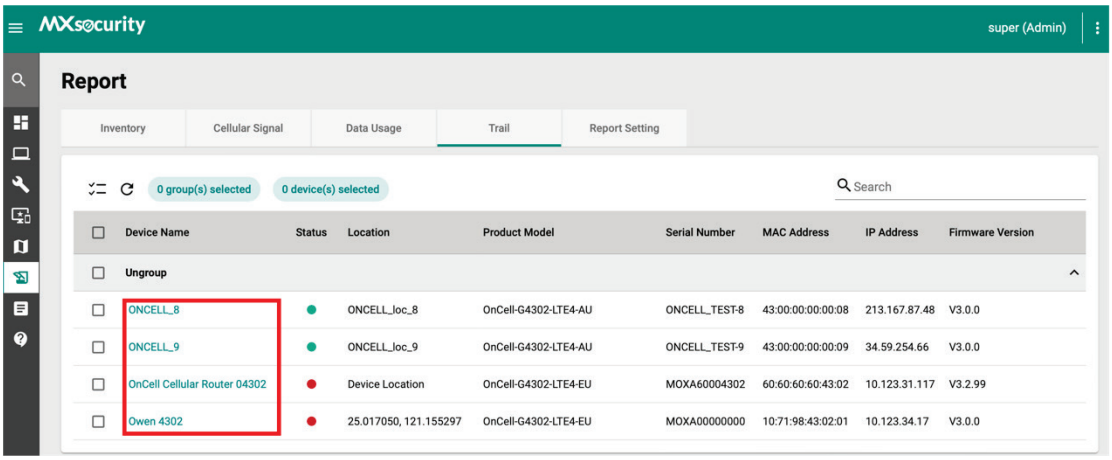
Viewing GPS Trajectories

To visualize and improve the quality of trail reports, MXsecurity supports an online GPS trajectory view for trail reports. This feature allows users to easily track and analyze movement patterns within their network, providing a more intuitive and efficient way to understand network dynamics.

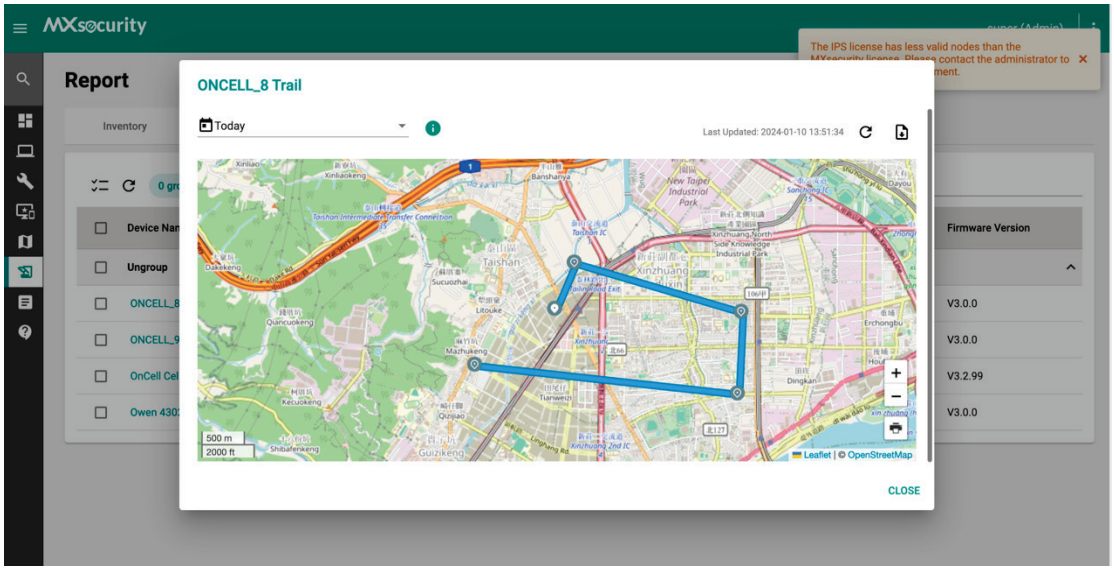
Steps:

1. Navigate to **Report > Trail**.

2. Click on the device name.
   The device's GPS trajectory map will appear.



3. Select a date to show the device's GPS movement history up until that day.



Report Settings

From the Report Settings tab, users can set the report time zone and manage configured report schedules.

Configure Report Time Zone Settings

The device and MXsecurity might be deployed in different time zones. To ensure correct report data, users can configure the time zone for reports.

Steps:

1. Navigate to **Report > Report Setting > Time Zone Setting**.
2. Select the time zone from the drop-down menu.
3. Click **APPLY**.

Editing a Report Schedule

Steps:

1. Navigate to **Report > Report Setting > Schedule Report**.
2. Select the schedule you want to modify.
3. Click the  icon to edit the schedule.
4. When finished editing the schedule, click **APPLY**.

10. Logging

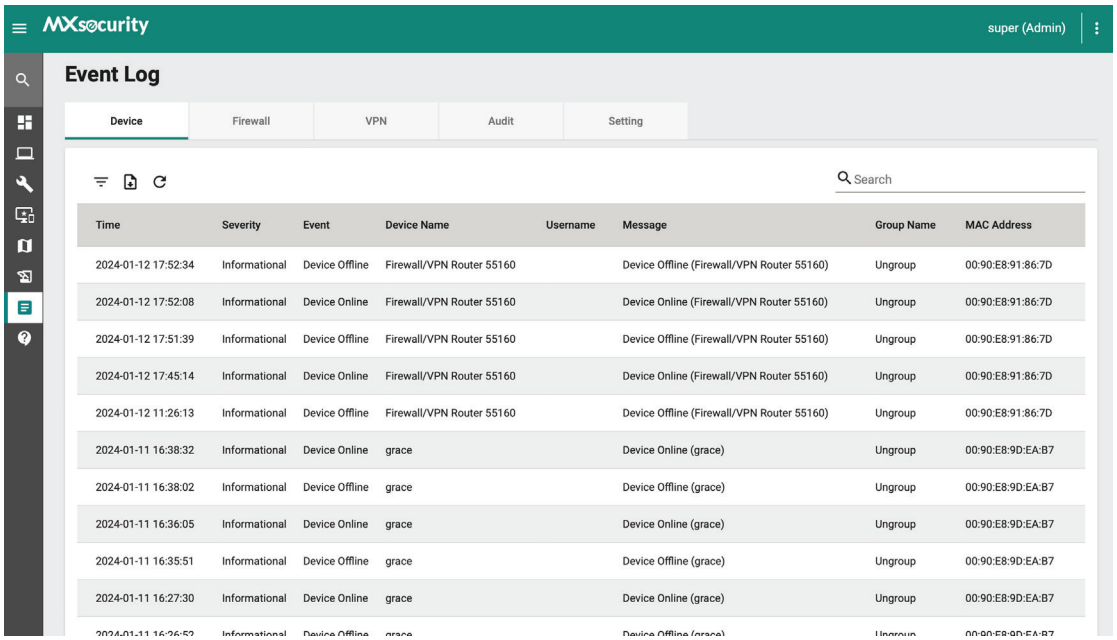
This chapter covers the event log and notification functions. Users can view logs related to the device, firewall, VPN, and audits. The notification function enables users to receive notifications for particular event logs. Users can send these notifications to designated email recipients or a syslog server.

Event Log

The event log contains all system- and device-related logs. Logs are categorized by type, including device, firewall, VPN, and audit logs. Refer to the following sections for more information about each log type.

Device Log

The device log records interactions between the device and MXsecurity, such as Device Added, Device Deleted, Device Online/Offline, Device Deployment Success/Failure, and Send SMS.

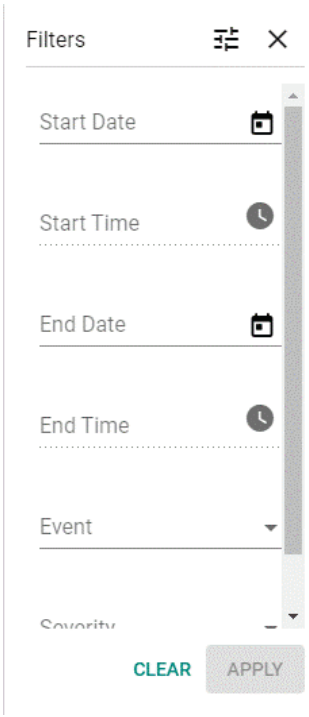


Viewing Device Logs

Steps:

1. Navigate to **Logging > Event Log > Device**.
2. You can perform the following actions:

   a. Click the icon to open the filter menu. Select a start/end day and time or log severity from the respective drop-menu.



Click the button to configure advanced filters. Check the box of the specific event(s) you want to filter. Click **APPLY**. The logs will renew immediately to reflect the selected criteria.

b. Click the button to export the current search results as a CSV file.

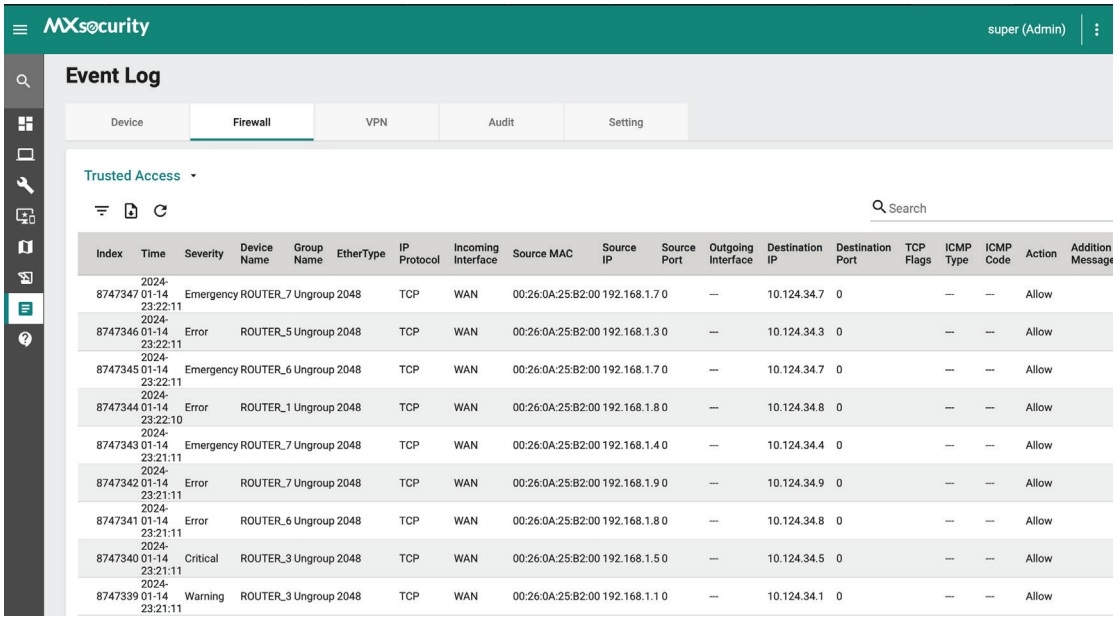
c. Click the button to renew the search results.

The following table describes the log's fields.

Field	Description
Time	The time the log entry was created.
Severity	The severity level assigned to the system event.
Event	The category of the system event.
Device Name	The hostname of the device that generated the log.
Username	The username of the user that generated the log.
Message	This field displays a detailed description of the event.
Group Name	The group name of the device group that generated the log.
MAC Address	The MAC address of the device that generated the log.

Firewall Log

The firewall logs include logs detected by the Trusted Access, Malformed Packets, DoS policy, L3-L7 policies, protocol filter policies, ADP, IPS and Session Control features.

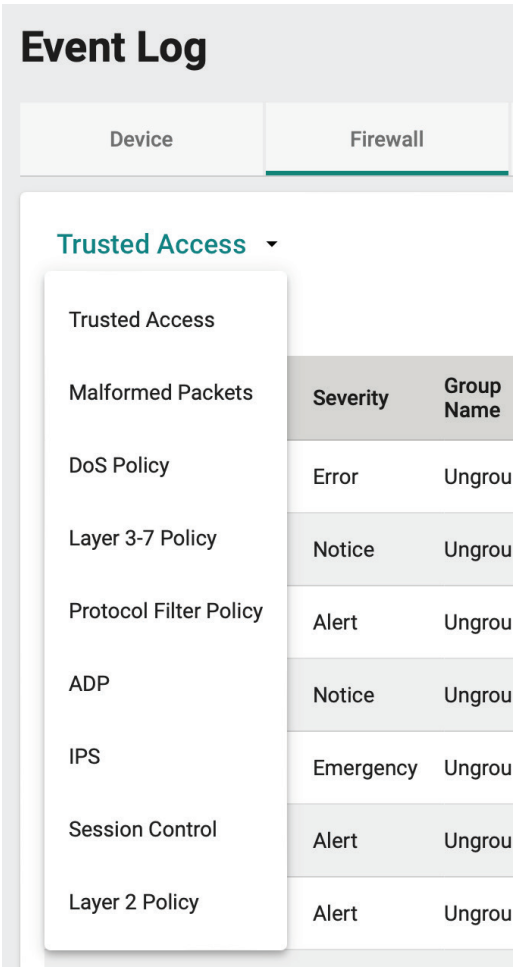


Viewing Firewall Logs

Steps:

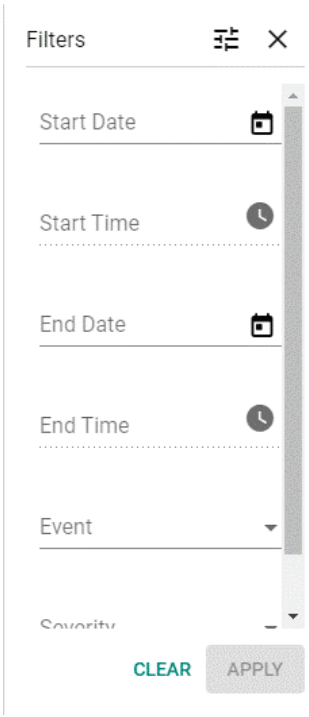
1. Navigate to **Logging > Event Log > Firewall**.

2. Select the firewall function event log type from the drop-down menu.



3. You can perform the following actions:

   a. Click the  icon to open the filter menu. Select a start/end day and time or log severity from the respective drop-menu.



Click the button to configure advanced filters. Check the box of the specific event(s) you want to filter. Click **APPLY**. The logs will renew immediately to reflect the selected criteria.

b. Click the button to export the current search results as a CSV file.

c. Click the button to renew the search results.

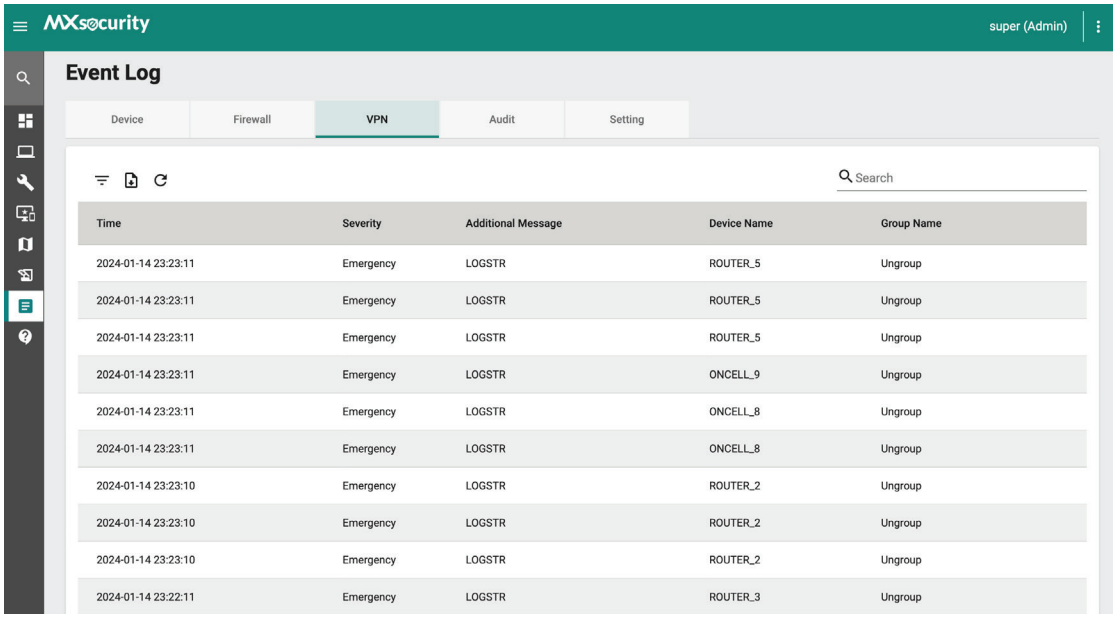
The following table describes the log's fields.

Field	Description
Index	The index of the log.
Time	The time the log entry was created.
Severity	The severity level assigned to the firewall event.
Device Hostname	The host name of the device that generated the log.
Group Name	The group name of the device group that generated the log.
IPS Severity	The severity level assigned to the IPS event.
IPS Category	The category of the IPS event.
Ethernet Type	The Ethernet type of the connection.
IP Protocol	The IP protocol of the connection.
Incoming Interface	The name of the incoming interface where the event was registered.
Source MAC	The source MAC address of the connection.
Source IP	The source IP address of the connection.

Field	Description
Source Port	The source port of the connection.
Outgoing Interface	The name of the outgoing interface where the event was registered.
Destination IP	The destination IP address of the connection.
Destination Port	The destination port of the connection.
TCP Flags	The TCP flags of the TCP protocol.
ICMP Type	The ICMP type of the ICMP protocol.
ICMP Code	The ICMP Code of the ICMP protocol.
Action	The action performed based on the policy settings.
Additional Message	The additional message provided with the log.

VPN Log

The VPN logs show details about the status of tunnel connections and related events.

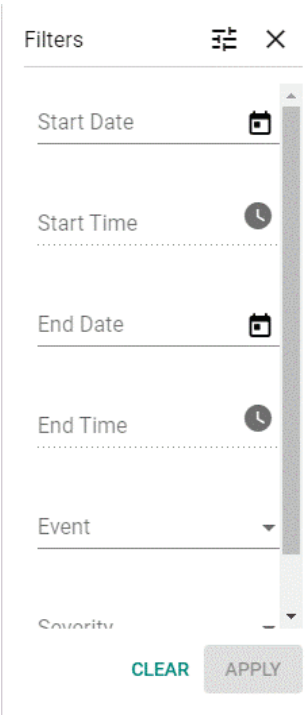


Viewing VPN Logs

Steps:

1. Navigate to **Logging > Event Log > Audit**.
2. You can perform the following actions:

   a. Click the icon to open the filter menu. Select a start/end day and time or log severity from the respective drop-menu.



Click the button to configure advanced filters. Check the box of the specific event(s) you want to filter. Click **APPLY**. The logs will renew immediately to reflect the selected criteria.

b. Click the button to export the current search results as a CSV file.

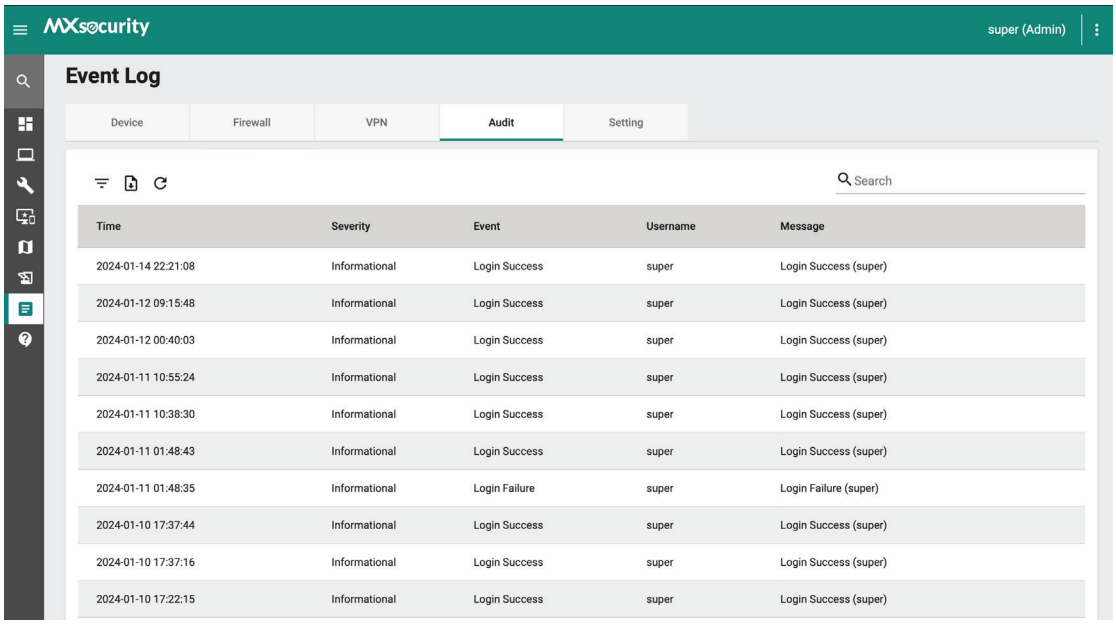
c. Click the button to renew the search results.

The following table describes the log's fields.

Field	Description
Time	The time the log entry was created.
Severity	The severity level assigned to the system event.
Event	The category of the system event.
Additional Message	The additional message provided with the log.
Device Hostname	The host name of the device that generated the log.
Username	The username of the user that generated the log.
Group Name	The group name of the device group that generated the log.

Audit Log

The audit logs show details about user access, configuration changes, and other events that occurred when using MXsecurity.

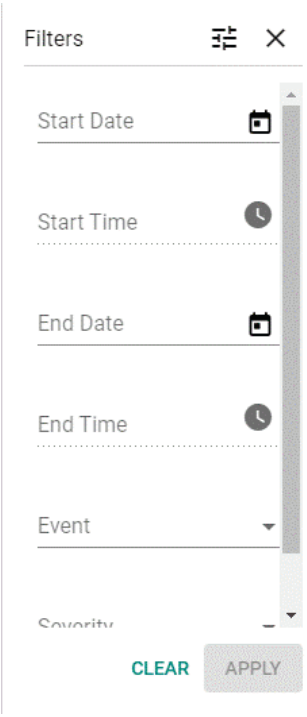


Viewing Audit Logs

Steps:

1. Navigate to **Logging > Event Log > Audit**.
2. You can perform the following actions:

   a. Click the icon to open the filter menu. Select a start/end day and time or log severity from the respective drop-menu.



   Click the button to configure advanced filters. Check the box of the specific event(s) you want to filter. Click **APPLY**. The logs will renew immediately to reflect the selected criteria.

   b. Click the button to export the current search results as a CSV file.

   c. Click the button to renew the search results.

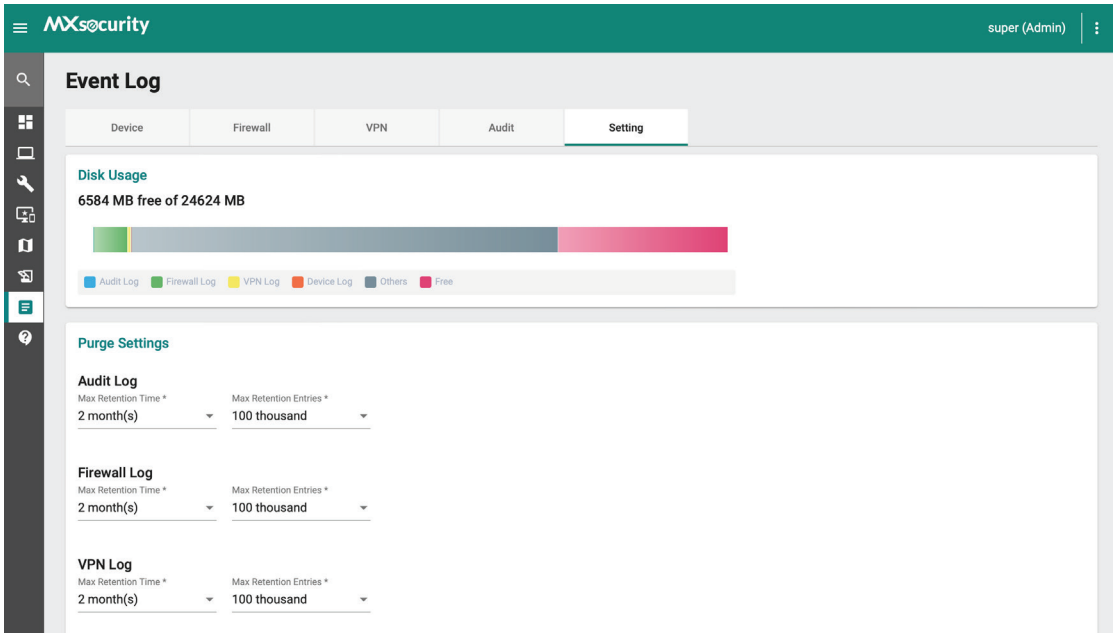
The following table describes the log's fields.

Field	Description
Time	The time the log entry was created.

Field	Description
Severity	The severity level assigned to the system event.
Event	The category of the system event.
Device Hostname	The host name of the device that generated the log.
Username	The username of the user that generated the log.
Group Name	The group name of the device group that generated the log.

Event Log Settings

From the Setting tab, users can check the status of event logs stored on the local drive and configure log purging settings.



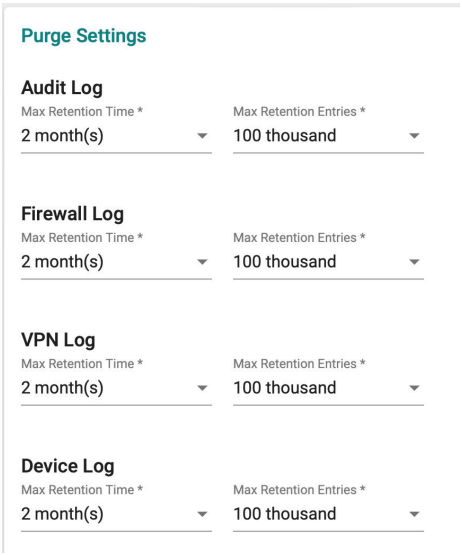
Purging Event Logs

The log purging function allows users to configure automatic log purging based on the specified retention time and log amount. Purging logs may be useful when the system generates a lot of event logs, which may affect network performance.

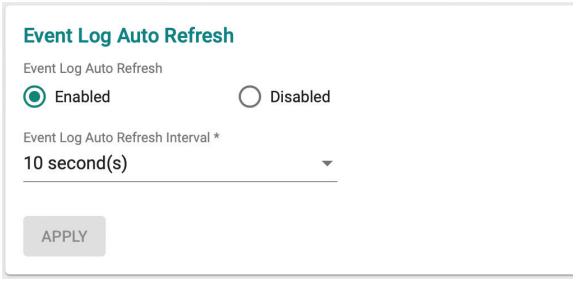
When the retention time or the number of entries for a log type exceeds the set threshold, MXsecurity will start clearing the logs, starting with the oldest records.

1. Navigate to **Logging > Event Log > Setting**.
2. In the Disk Usage section, check the current used and available disk space.

3. In the Purge Settings section, select the retention time and number of entries to retain for each log type.



4. (**Optional**) In the Event Log Auto Refresh section, disable or select the interval at which the event log data will refresh.



5. Click **APPLY**.

Notifications

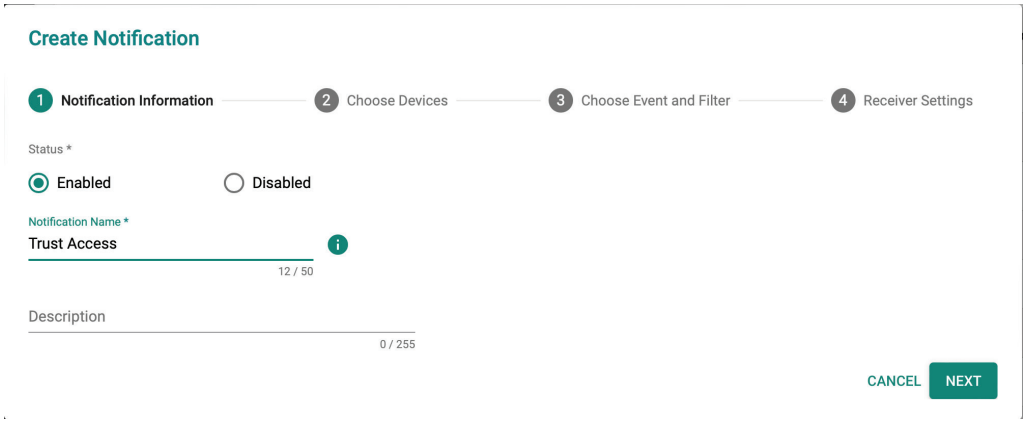
The Notification tab allows users to set up notifications for specific events. Users can configure these notifications to be sent by email or sent to a Syslog server.

Adding a Notification

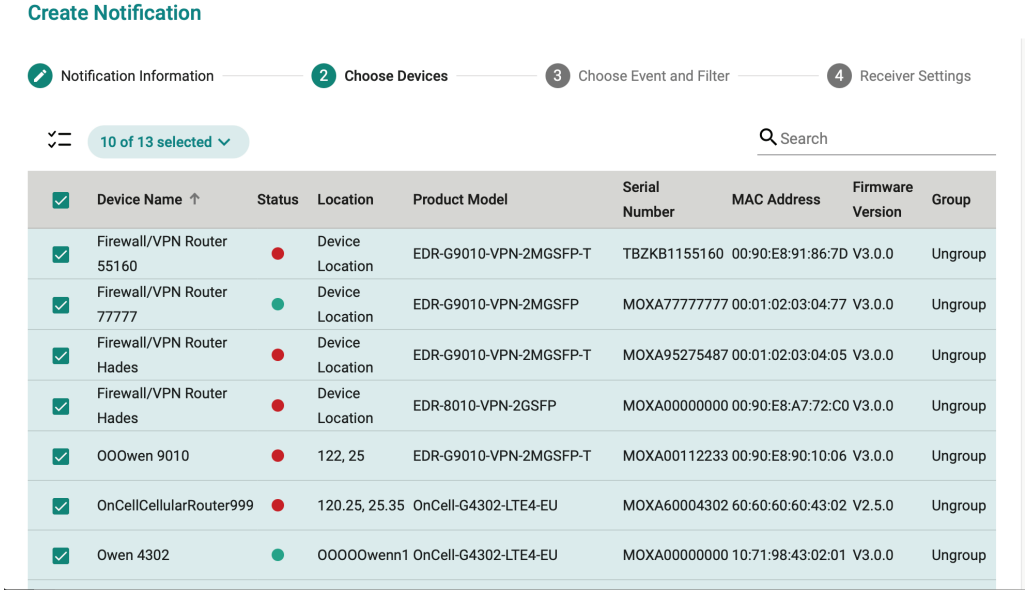
Steps:

1. Navigate to **Logging > Notifications**.
2. Click the  icon to add a notification.

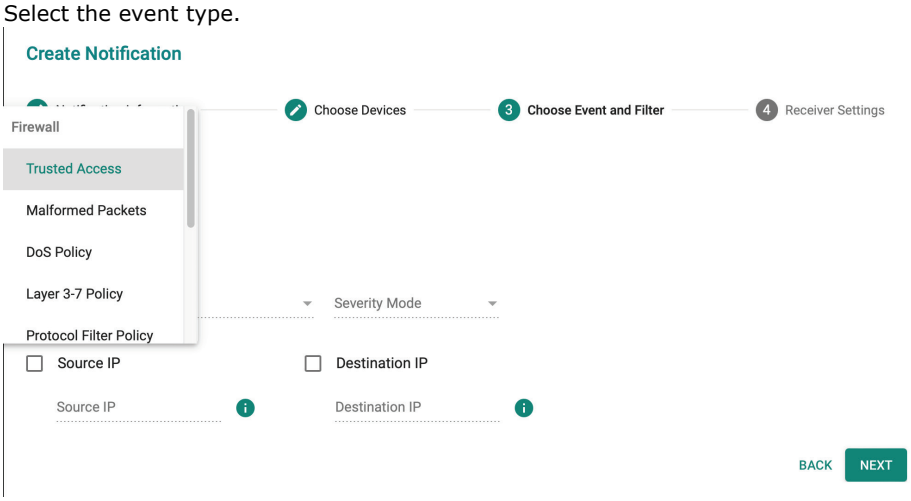
3. Enter a name and description for the notification.



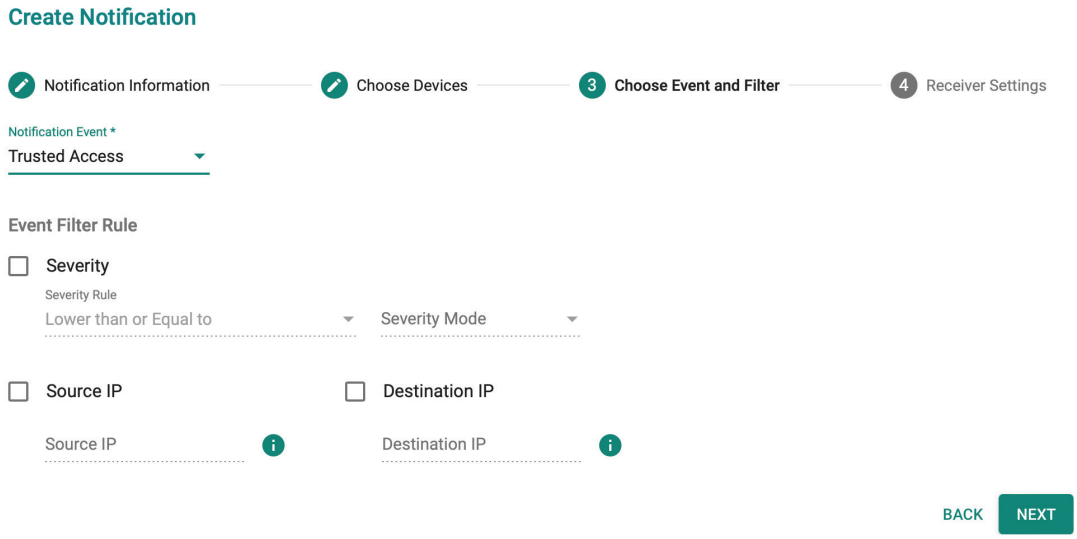
4. Click **NEXT**.
5. Select the device(s) that will send notifications for the specified events.



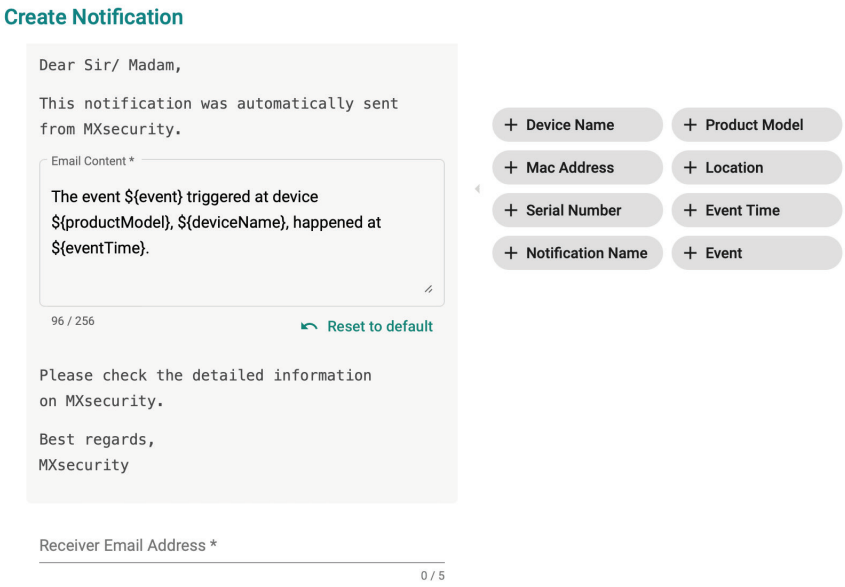
6. Select the event types and configure filter rules:
   a. Select the event type.



b. Specify the notification filter rules to determine when the device will send a notification for the event. Depending on the select notification event, filter rule options will be different.

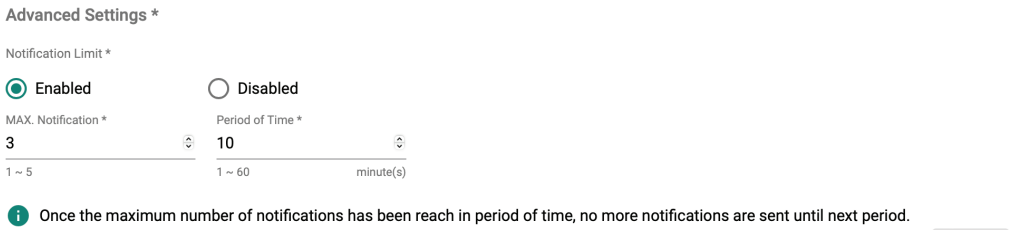


7. Configure the notification content and recipient settings.



a. Select the notification delivery method. Multiple methods can be selected.
b. Edit the notification content using the predefined variables.
c. If Email is selected, specify the email recipients. You can add up to 5 recipients separated by a comma.

8. Configure Advanced Settings. To prevent an influx of messages in a short period, users can configure a limit on the number of notifications for a specified interval. When exceeded, all additional notifications will be discarded until the next interval begins.



a. Enable or disable the notification limit.
b. Specify the maximum number of notifications.

c. Specify the interval duration.

9. Click **APPLY**.

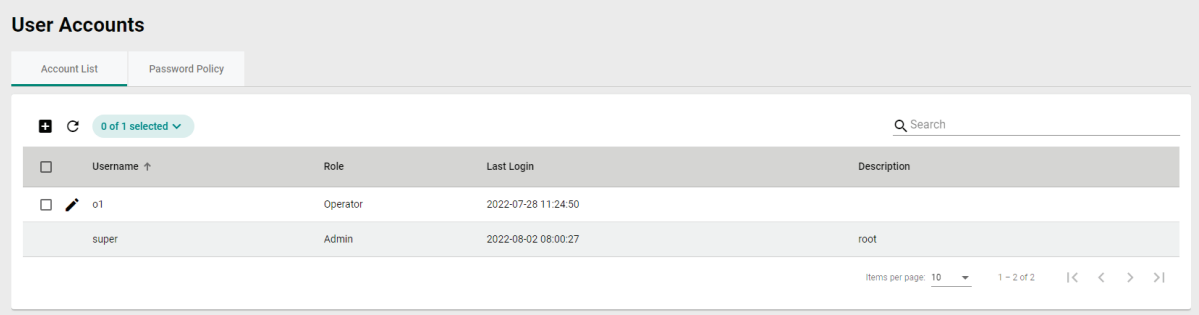
11. Administration

This chapter describes the available administrative settings for MXsecurity.

User Accounts

> **NOTE**
>
> Log in to the management console using the default administrator account ("admin") or any account with administrator privileges to access the User Accounts screens.

MXsecurity uses role-based administration to grant and control access to the management console. Use this feature to assign specific management console privileges to user accounts and present them with only the tools and permissions necessary to perform specific tasks. Each account is assigned a specific role. A role defines the level of access to the management console. Users can log in to the management console using custom user accounts.



The following table outlines the tasks available on the **User Accounts** tab.

Task	Description
Add a user account	Click the icon to create a new user account. For more information, see Adding a User Account.
Delete an existing account	Select one or more existing user accounts and click the icon. For more information, see Deleting a User Account.
Edit an existing account	Click the icon next to an existing user account to view or modify the current account settings. For more information, see Editing an Existing User Account.
Configure the password policy	Click **Password Policy** to adjust password restrictions. For more information, see Configuring the Password Policy.

User Roles

The following table describes the permissions matrix for user roles.

Dashboard

		User Roles		
Configuration Screen	**Action**	**Admin**	**Operator**	**Viewer**
Dashboard	View	Yes	VG	VG
	All operations	Yes	VG	VG

System Tab

		User Roles		
Configuration Screen	**Action**	**Admin**	**Operator**	**Viewer**
User Accounts	View	Yes	No	No
	All operations	Yes	No	No
Licenses	View	Yes	No	No
	All operations	Yes	No	No
Settings	View	Yes	No	No
	All operations	Yes	No	No

Management Tabs

		User Roles		
Configuration Screen	**Action**	**Admin**	**Operator**	**Viewer**
Device Group	View	Yes	VG	No
	All operations	Yes	No	No
Firmware	View	Yes	Yes	No
	All operations	Yes	No	No
Software Packages	View	Yes	Yes	No
	All operations	Yes	No	No
Objects	View	Yes	Yes	No
	All operations	Yes	No	No
Policy Profiles	View	Yes	Yes	No
	All operations	Yes	No	No
Device Configuration	View	Yes	VG	No
	All operations	Yes	No	No

NOTE

VG denotes that if the administrator has assigned/shared the device group permissions with a specific user account, then that user can view the information for that device group on the Management/Device Groups pages.

Device Deployment

		User Roles		
Configuration Screen	**Action**	**Admin**	**Operator**	**Viewer**
Device Deployment	View	Yes	VG	No
	All operations	Yes	VG	No

NOTE

VG denotes that if the administrator has assigned/shared the device group permissions with a specific user account, then that user can view the information for that device group on the Device Deployment page.

Map View

		User Roles		
Configuration Screen	**Action**	**Admin**	**Operator**	**Viewer**
Map View	View	Yes	VG	VG
	All operations	Yes	VG	No

Report

		User Roles		
Configuration Screen	**Action**	**Admin**	**Operator**	**Viewer**
Reports	View	Yes (All users)	VG (Self)	VG (Self)
	All operations	Write (Self) Delete (All users)	VG (Self)	VG (Self)

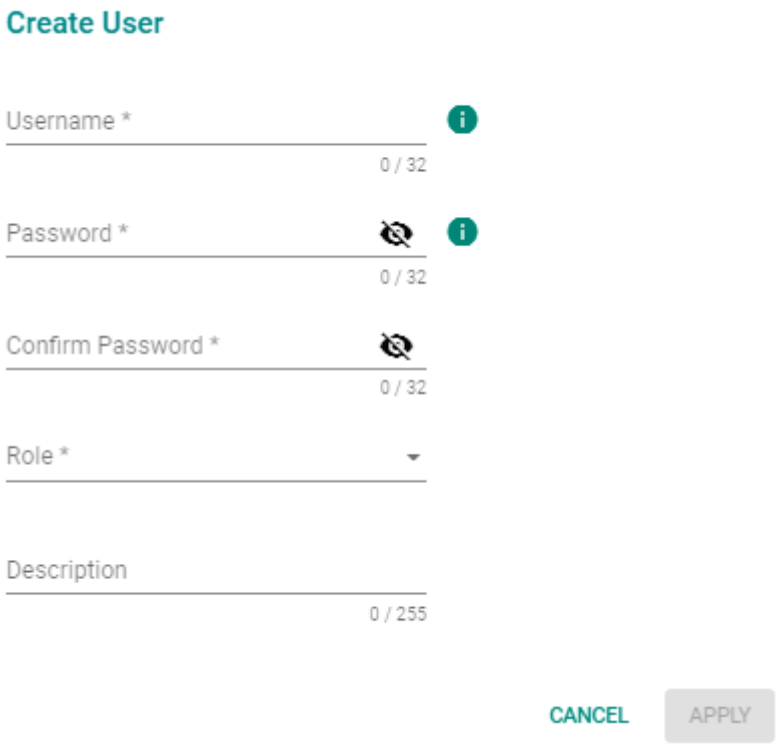
Logging

		User Roles		
Configuration Screen	**Action**	**Admin**	**Operator**	**Viewer**
Event Log	View	Yes	VG	VG
	All operations	Yes	VG	No
Notification	View	Yes	VG (Self)	VG (Self)
	All operations	Write (Self) Delete (All users)	VG (Self)	VG (Self)

> **NOTE**
>
> VG denotes that if the administrator has assigned/shared the device group permissions with a specific user account, then that user can view the information for that device group on the Logging/Event Log pages.

Account Input Format

Input format validation will apply to the account management form text fields. The following table describes the format restrictions for user input.



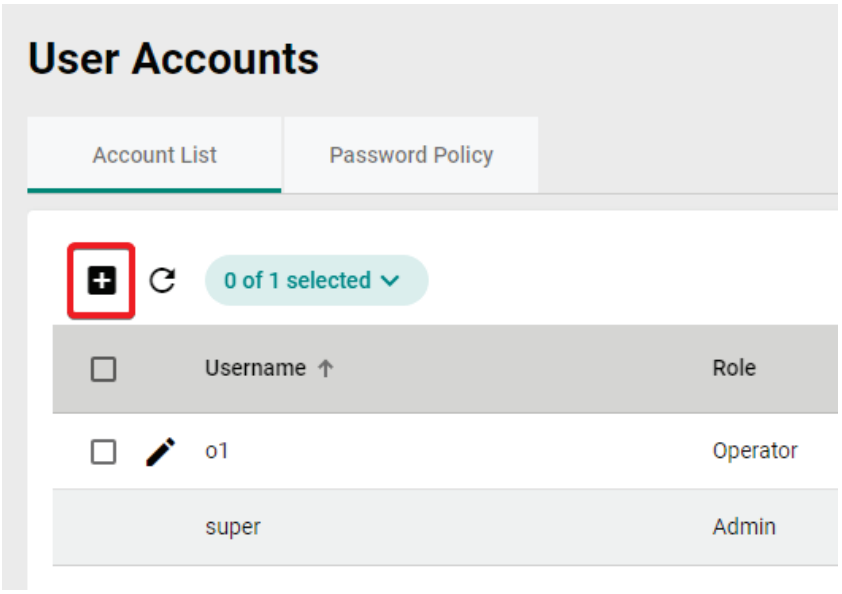
Type	Length	Format	Reserved Name
Username	1 to 32 characters	Letters: a-z, A-Z Numbers: 0-9 Special characters: periods (.), underscores (_)	admin administrator viewer operator root auditor
Description	0 to 255 characters	Letters: a-z, A-Z Numbers: 0-9 Special characters: periods (.), underscores (_), spaces, parenthesis [(,)], hyphens (-)	

Adding a User Account

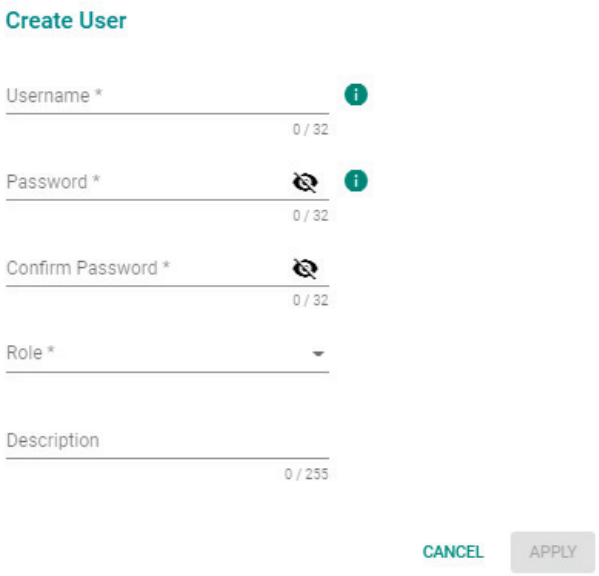
When logging in with an administrator account, you can create new user accounts for accessing MXsecurity.

Steps:

1. Navigate to **System > User Accounts > Account List**.
2. Click the  icon.



The **Create User** screen will appear.

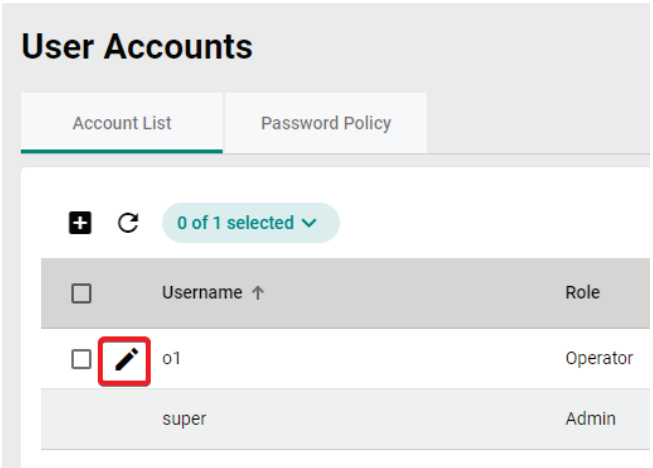


3. Configure the following settings:
   a. **Username**: Enter the username used to log in to the management console.
   b. **Password**: Enter the account password.
   c. **Confirm Password**: Enter the account password again to confirm.
   d. **Role**: Select a user role for this account. For more information, see User Roles.
   e. **Description**: Enter a description for this account.
4. Click **APPLY**.

Editing an Existing User Account

Steps:

1. Navigate to **System > User Accounts > Account List**.
2. Click the icon next to the user account you want to modify.

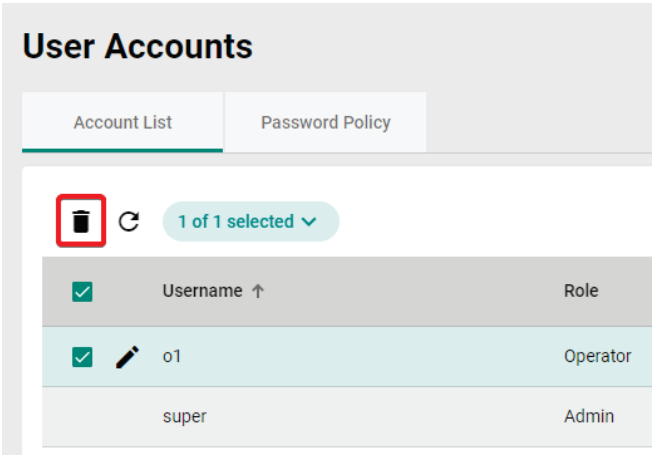


3. Modify the user account settings. Refer to Adding a User Account for more information.
4. Click **APPLY**.

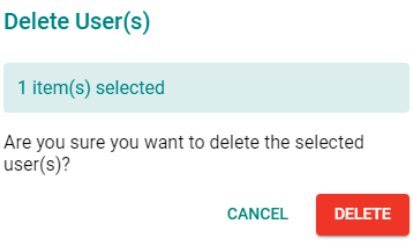
Deleting a User Account

Steps:

1. Navigate to **System > User Accounts > Account List**.
2. Check the box of the user account(s) you want to delete.
3. Click the icon to delete the selected user account(s).



4. When prompted to confirm, click **DELETE**.



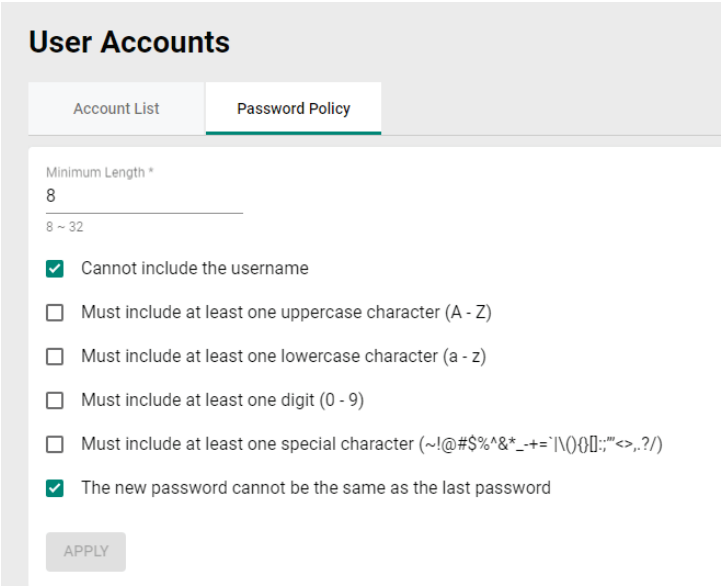
Configuring the Password Policy

To improve password strength, the administrator can customize the password policy from the **Password Policy** screen.

Steps:

1. Navigate to **System > User Accounts > Password Policy**.

2. Select the option(s) to apply to the password policy.

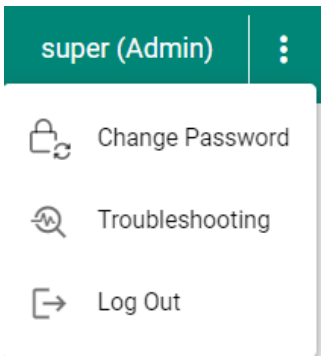


3. Click **APPLY**.

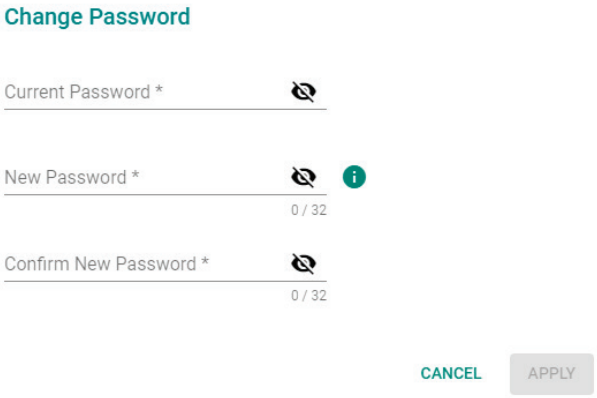
Changing Your Account Password

Steps:

1. Click the icon in the top-right of the management console banner.



2. Click **Change Password**.
   The **Change Password** screen will appear.



3. Configure the following settings:
   a. **Current Password**: Enter your current password.

b. **New Password**: Enter your new password.

c. **Confirm New Password**: Enter your new password again.

4. Click **APPLY**. This will automatically log you out and return you to the login screen.

Licenses

From the **License** tab you can view license information and manage license keys to enable specific functions within MXsecurity.

> **NOTE**
>
> Only user accounts with administrator privileges can access the Licenses screen.

Introduction to Licenses

MXsecurity supports two types of licenses:

- **MXsecurity licenses**: Determines the maximum number of nodes that can be managed by MXsecurity.
- **IPS licenses**: Point-based licenses that add IPS points to the total available IPS point balance. Each IPS-registered device consumes one point per day, which is deducted from the IPS point balance.

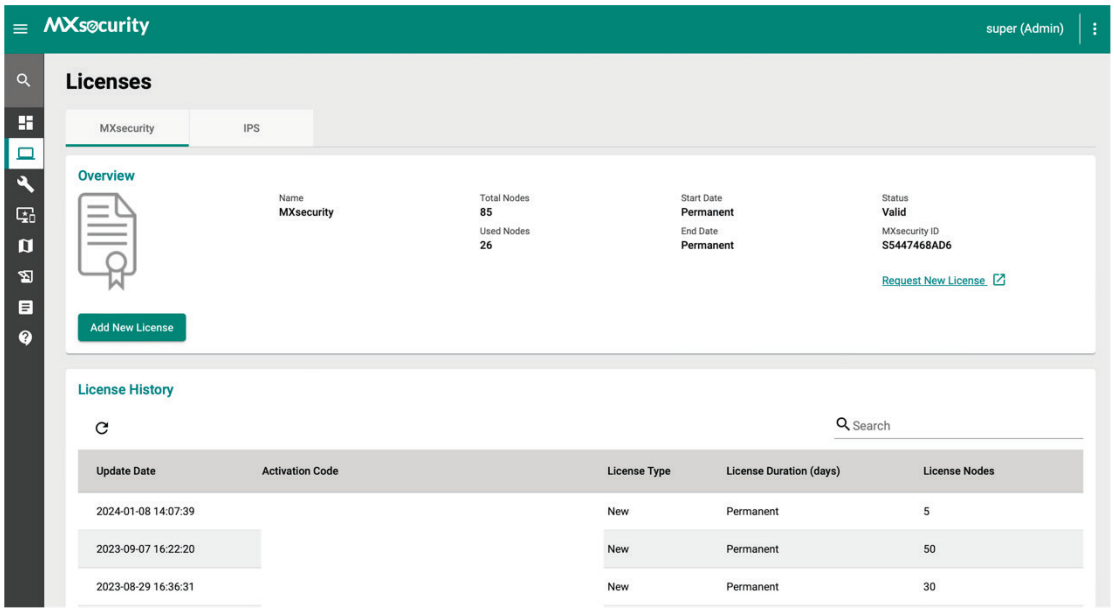
> **NOTE**
>
> As of MXsecurity v2.3.0, IPS licenses use the point-based format.

Viewing Your Product License Information

Steps:

1. Navigate to **System > Licenses**.

   The **Licenses** screen will appear.



2. Click the **MXsecurity** or **IPS** tab to view information for the respective license type.

The following tables describes the license information for each license type.

MXsecurity licenses

Field	Description
Name	The name of the license.
Total Nodes	The number of nodes that can be managed by this license.
Used Nodes	The number of used nodes on the license.
Start Date	The start date of the license.
End Date	The expiration date of the license.
Status	The status of the license.
UUID	The unique ID of this MXsecurity instance.

The following table describes the license history.

Message	Description
Create Date	The date of this license was entered.
Activation Code	The activation code of the license.
License Type	The type of license.
Valid for (days)	The duration of the license.
License Nodes	The number of nodes of the license.

IPS licenses

Field	Description
Name	The name of the license.
IPS Point Balance	The total number of available IPS license point.
Daily Point Usage	The total number of points consumed daily by IPS-registered devices.
Estimated Point Depletion Date	The estimated date the IPS point balance will be depleted.
Status	The status of the license.
UUID	The unique ID of this MXsecurity instance.

The following table describes the license history.

Message	Description
Create Date	The date of this license was entered.
Activation Code	The activation code of the license.
License Type	The type of license.
License Points	The number of points of the license.

Alert Messages

When a license is about to expire or has expired, alert messages will pop-up when the user logs in to the web management console.

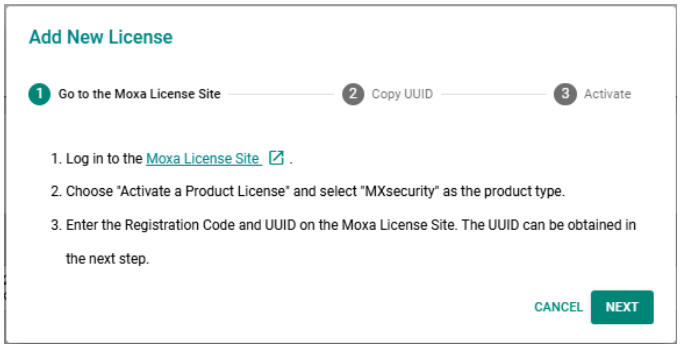
Message	Description
The (category) license expires in (days) days. To continue using all features, enter a new license code.	This message appears 30 days before the license expiration date. The (days) represent the days remaining before the license expires.
The (category) license has expired. To continue using all features, enter a valid license code.	The license has expired, and you will be required to purchase a new license to continue using the product.
The total points of all IPS licenses will deplete in (days) days.	This message appears 30 days before the IPS point balance is depleted. The (days) indicates the number of days remaining before the point balance runs out.
IPS license points depleted.	The IPS point balance license is depleted, and you will need to purchase a new IPS point license to continue using IPS pattern update services.

Adding a New MXsecurity License

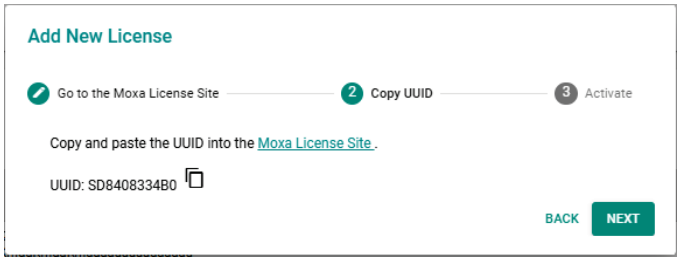
You can activate an MXsecurity license using a valid license activation code.

Steps:

1. Navigate to **System > Licenses > MXsecurity**.
2. Click the Add New License button.
   The **Add New License** screen will appear.



3. Follow the on-screen instructions for activating the license on the Moxa License Site.
4. Enter the activation code provided by the Moxa License Site into MXsecurity.



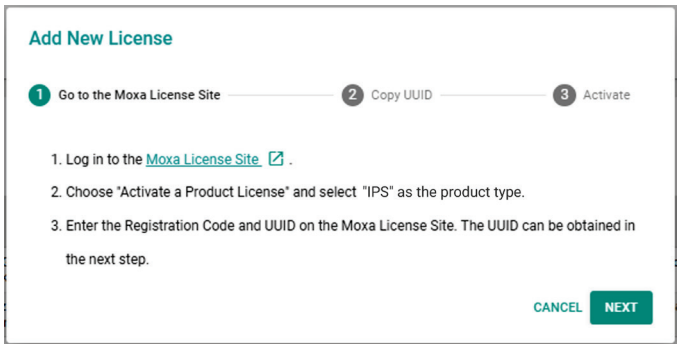
5. Click **APPLY**.
6. Verify the license information is correct.

Adding a New IPS License

You can activate an IPS license using a valid license activation code.

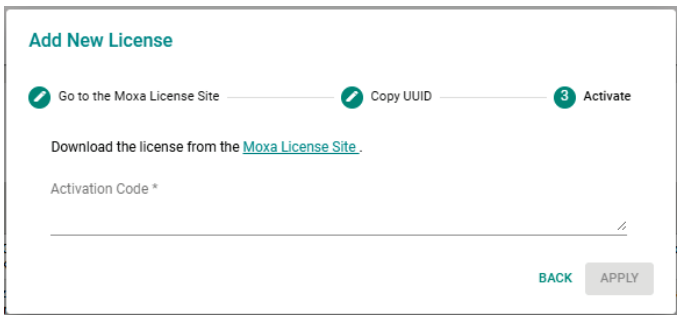
Steps:

1. Navigate to **System > Licenses > IPS**.
2. Click the Add New License button.
   The **Add New License** screen will appear.



3. Follow the on-screen instructions for activating the license on the Moxa License Site.

4. Enter the activation code provided by the Moxa License Site into MXsecurity.



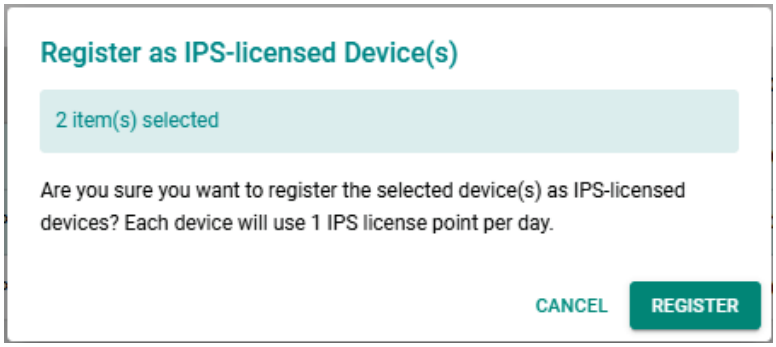
5. Click **APPLY**.
6. Verify the license information is correct.

Registering an IPS-licensed Device

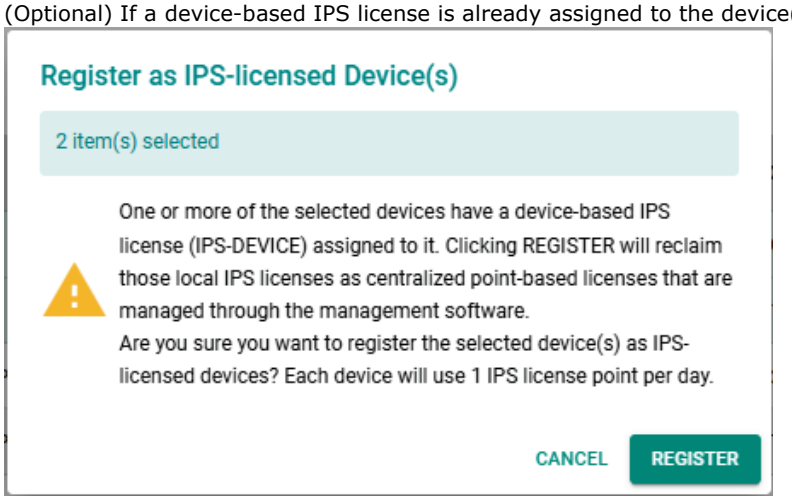
To enable full IPS functionality on a device, you must register the device as an IPS-license device. Once registered, the device will consume one IPS license point per day.

Steps:

1. Navigate to **System > Licenses**.
2. Click the **IPS** tab.
3. In the IPS License Management section, check of the box device(s) you want to register as IPS-licensed.
4. Click the  icon to register an IPS licenses to the selected device(s).
5. When prompted to confirm, click **REGISTER**.



6. (Optional) If a device-based IPS license is already assigned to the device(s), a notification will appear.



7. Click **REGISTER** to reclaim the device-based licenses and register the device(s) as IPS-licensed.

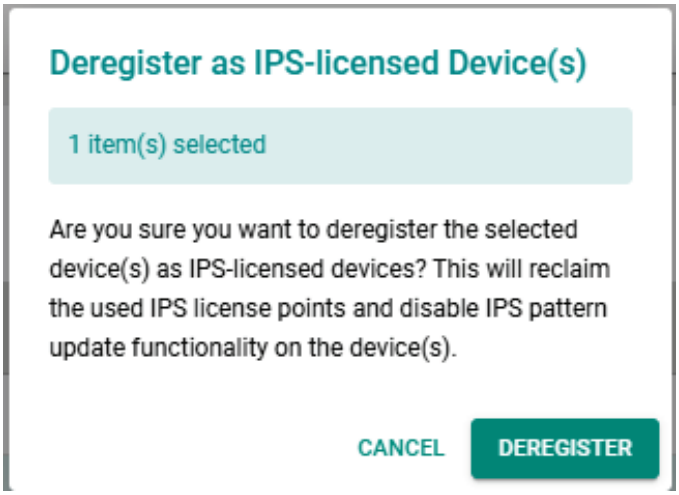
> **NOTE**
>
> When reclaiming a device-based IPS (IPS-DEVICE) license, the management software will reclaim and reassign the license as a centrally managed IPS license. The original license will be added to the total IPS point balance.

Deregistering an IPS-licensed Device

You can deregister an IPS license from a managed device to assign it to another device. Deregistering an IPS license will cause IPS pattern updates to become unavailable on that device until another IPS license is assigned to it.

Steps:

1. Navigate to **System > Licenses**.
2. Click the **IPS** tab.
3. In the IPS License Management section, check of the box device(s) you want to deregister the IPS license for.
4. Click the  icon to deregister the IPS licenses from the selected device(s).
5. When prompted to confirm, click **DEREGISTER**.



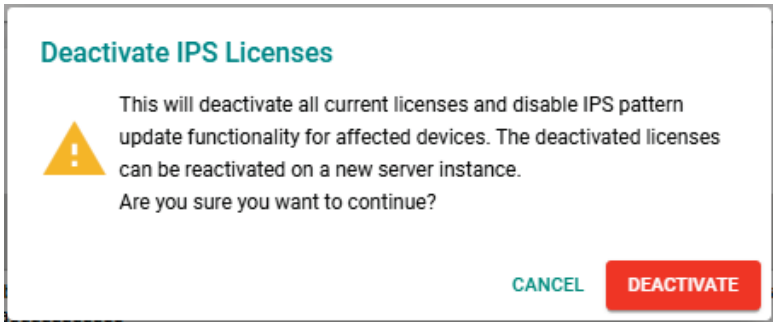
Transferring an IPS License

In some circumstances, you may need to migrate MXsecurity to a new host system. To transfer your IPS licenses to another instance of MXsecurity, you must deactivate them on the current system first and reactivate the license(s) on the new MXsecurity instance.

Steps:

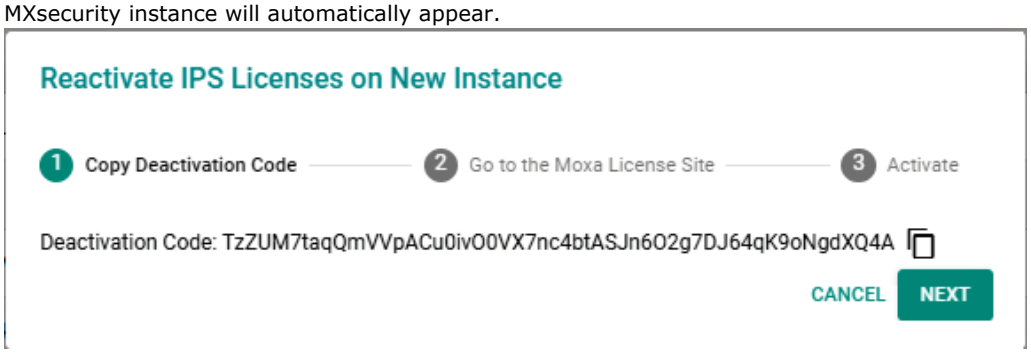
1. Navigate to **System > Licenses**.
2. Click the **IPS** tab.
3. In the License History section, click the  icon to deactivate all IPS licenses.

4. When prompted to confirm, click **DEACTIVATE**.



> **NOTE**
>
> If there were more than one active IPS license, clicking **DEACTIVATE** will combine the IPS license points of all these licenses into a single license.

5. The **Reactivate IPS Licenses on New Instance** window for activating the license on the new MXsecurity instance will automatically appear.



If you closed this window, you can reopen it by clicking the **Reactivate** button in the Deactivated Licenses section.

6. Follow the steps in the reactivation wizard to complete the license transfer process.

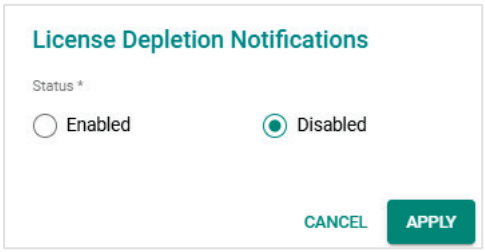
Configuring IPS License Depletion Notifications

You can set up notifications to inform you when your IPS license point balance is about to run out.

Steps:

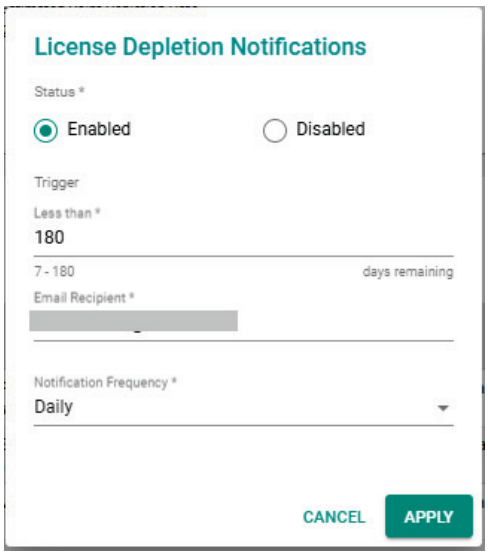
1. Navigate to **System > Licenses**.
2. Click the **IPS** tab.
3. Click the 

button.
The **License Depletion Notifications** screen will appear.



4. Change the status to **Enabled**. License notifications are disabled by default.

5. Configure the following settings:



   a. **Less than**: Specify the number of days before the IPS point balance is depleted. A notification will be sent when this threshold is reached. Days remaining are calculated based on the total available IPS point balance divided by the daily point usage.
   b. **Email Recipient**: Enter the email address of the notification recipient. SMTP settings must be configured first before notifications can be set up. Refer to Editing Email Settings.
   c. **Notification Frequency**: Select the notification frequency.
6. Click **APPLY**.

Settings

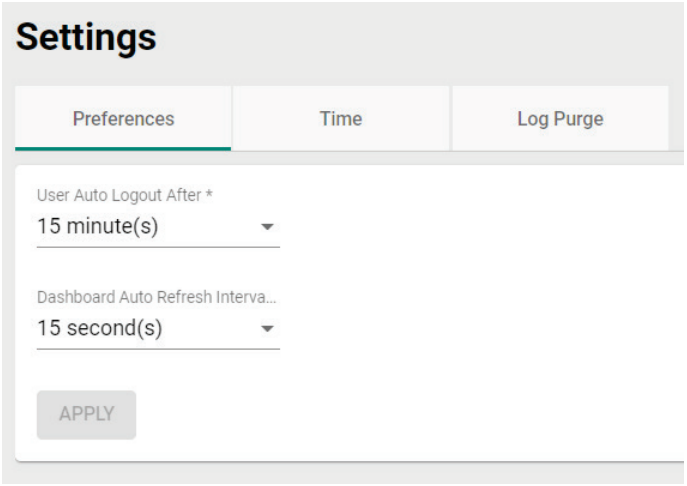
From the **Settings** page, you can configure system preferences, time, and log purge settings.

Configuring Preferences

From the Preferences screen, you can confirm basic settings for the MXsecurity instance.

Steps:

1. Navigate to **System > Settings > Preferences**.
2. Select the duration and interval for the auto logout and dashboard auto refresh functions respectively.



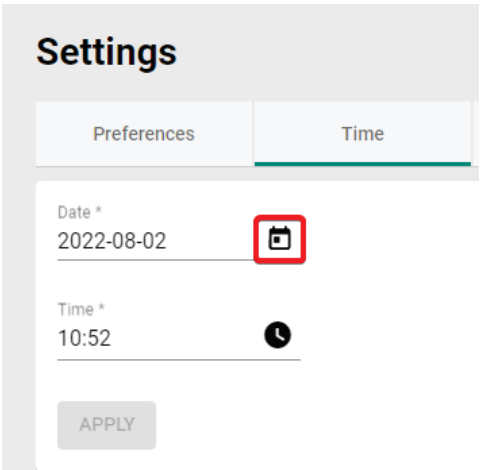
3. Click **APPLY**.

Configuring the System Time

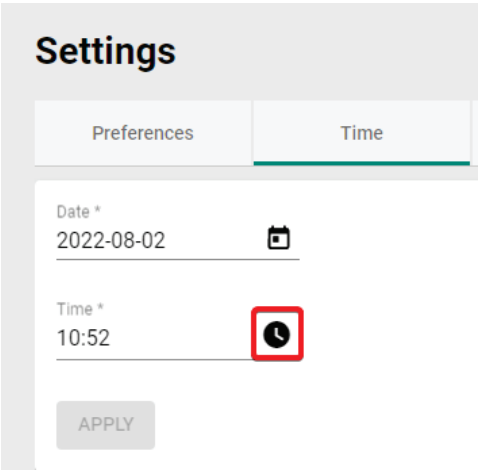
From the Time tab, you can manually set the system time. MXsecurity will automatically synchronize the system time with all managed nodes.

Steps:

1. Navigate to **System > Settings > Time**.
2. Click the icon to select the date.



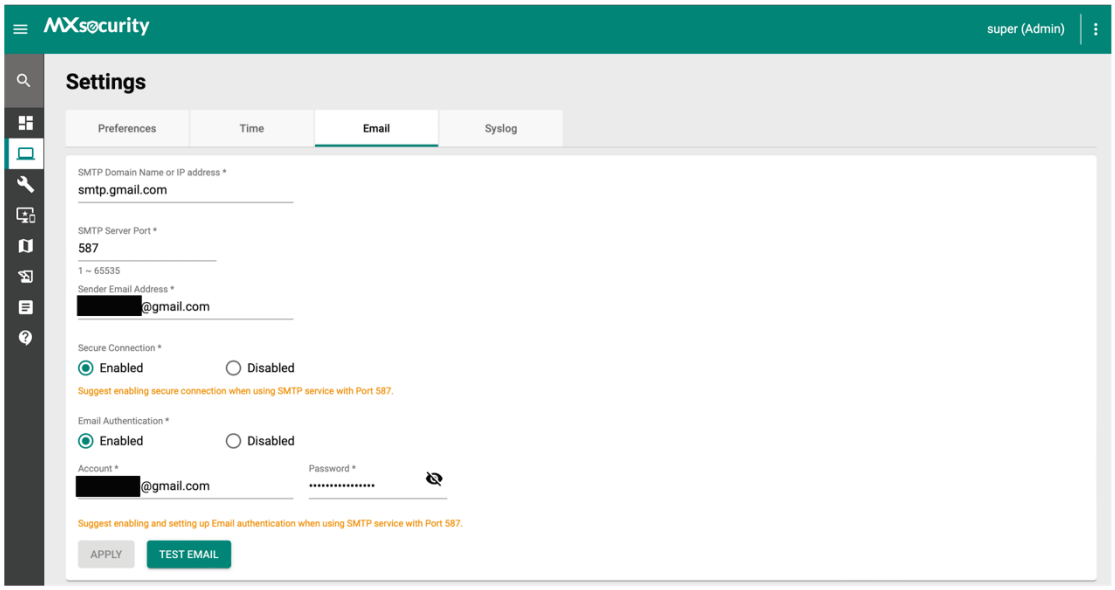
3. Click the icon to select the time.



4. Click **APPLY**.

Editing Email Settings

From the **Email** tab, you can configure email server settings. These settings must be configured to use certain functions, such as email notifications and scheduled report sending.



Refer to the table below for an overview of each setting.

Field	Description
SMTP Domain Name or IP address	The SMTP server domain name or IP address.
SMTP Server Port	The communication port of the SMTP server. The recommended port is 587.
Sender Email Address	The email address used to send notifications or reports.
Secure Connection	Enable or disable SSL (port 587) to establish a connection to the SMTP server. This function depends on the settings of the SMTP server. In most cases, servers require a secure connection.
Email Authentication	Enable or disable email authentication. If enabled, MXsecurity requires an account and password for email authentication with the SMTP server.
Account	If email authentication is enabled, enter email account name.
Password	If email authentication is enabled, enter the authentication account password.

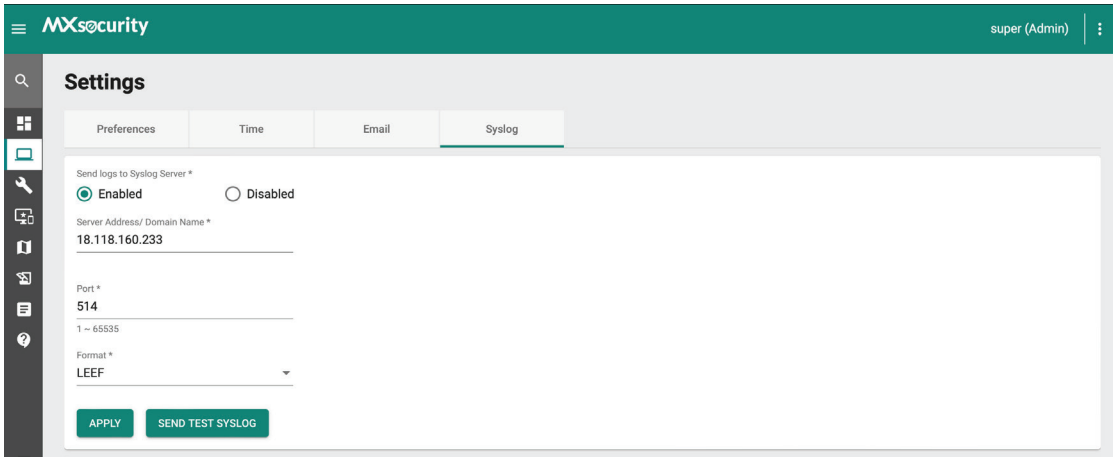
> **NOTE**
>
> If you set a Gmail account as the sender address, we highly recommend enabling "2-step verification" and getting a 16-bit application password. For details, refer "Gmail-Help center - Sign in with Passwords" for more information.

Click **TEST EMAIL** to test the configuration.

When finished, click **APPLY**.

Editing Syslog Settings

From the **Syslog** tab, you can configure the syslog server to which MXsecurity will send syslog messages to.



Refer to the table below for an overview of each setting.

Field	Description
Send logs to Syslog server	Enable or disable sending syslog messages to the Syslog server.
Server Address/ Domain Name	The IP address or domain name of the syslog server.
Port	The port number of the syslog server. The default port is 514.
Format	The syslog event format used for the syslog server. The default format is LEEF. Available options include: CEF.

Click **SEND TEST SYSLOG** to test the configuration.

When finished, click **APPLY**.