

MXsecurity User Manual

Version 2.0, January 2024

www.moxa.com/product

MOXA®

© 2024 Moxa Inc. All rights reserved.

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

© 2024 Moxa Inc. All rights reserved.

Trademarks

The MOXA logo is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

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	6
Key Features	6
Centralized Management	6
Unified, Error-free Mass Deployment	6
Real-time Visibility and Monitoring	6
Event Logs and Alert Notifications	6
Interactive Map View	6
Comprehensive Reports	6
System Requirements	7
2. Installation	8
Setting Up the Virtual Machine	8
Installing MXsecurity on a VMware Workstation	8
Installing MXsecurity on a VMware ESXi System	11
Configuring the MXsecurity system	16
3. Migration	19
Migrating to a Newer Version of MXsecurity (VMware Workstation)	19
Migrating to a Newer Version of MXsecurity (ESXi)	23
4. Getting Started	27
Getting Started Task List	27
Opening the Management Console	27
Connecting Secure Routers to MXsecurity	29
5. Dashboard and Widgets	30
Dashboard Widgets Overview	30
System Status	30
Node License Usage	30
Group Status	31
Top 5 Layer 3-7 Policy Events by Source IP	32
Top 5 Layer 3-7 Policy Events by Destination IP	33
Top 5 Layer 3-7 Policy Events by Severity	34
Top 5 Protocol Filter Policy Events by Source IP	35
Top 5 Protocol Filter Policy Events by Destination IP	35
Top 5 Protocol Filter Policy Events by Severity	36
Top 5 ADP Events by Source IP	37
Top 5 ADP Events by Destination IP	37
Top 5 IPS Events by Source IP	38
Top 5 IPS Events by Destination IP	39
Top 5 IPS Events by Severity	41
Top 5 IPS Events by Category	41
Connection Interface (Cellular Router)	42
Signal Quality (Cellular Router)	42
Widget Management	44
Adding a Widget to the Dashboard	44
Removing a Widget from the Dashboard	45
Resizing a Widget	45
Moving the Widget Position	46
6. Management	47
Device Group Management	48
Creating a New Device Group	48
Deleting a Device Group	49
Editing a Device Group	50
Firmware Management	50
Uploading a New Firmware	50
Deleting a Firmware	51
Exporting Firmware	52
Software Package Management	52
Uploading a New Software Package	52
Deleting a Software Package	53
Exporting Software Packages	53

Viewing Detailed Information of a Software Package.....	53
Object Management.....	54
Creating a New Filter Object.....	54
Creating a New Interface Object.....	56
Editing an Object.....	56
Deleting an Object.....	57
Policy Profile Management.....	57
Creating a New Layer 3-7 Policy Profile.....	57
Creating a New Session Control Policy Profile.....	60
Creating a New DoS Policy Profile.....	61
Creating a New IPS Policy Profile.....	63
Editing a Policy Profile.....	64
Deleting a Policy Profile.....	64
Device Configuration Management.....	64
Uploading a Device Configuration File From a Local Host.....	64
Uploading a Configuration From a Device.....	65
7. Deployment.....	67
Rebooting a Managed Device.....	67
Scheduling a Managed Device Reboot.....	68
Deleting a Managed Device Reboot Schedule.....	69
Sending a Control SMS.....	69
Removing a Managed Device.....	71
Deploying Policy Profiles to Managed Devices.....	72
Scheduling a Policy Profile Deployment for Managed Devices.....	72
Deleting a Policy Profile Deployment Schedule.....	74
Upgrading the Software Package of Managed Devices.....	74
Scheduling a Software Package Deployment for Managed Devices.....	75
Deleting a Software Package Deployment Schedule.....	77
Upgrading the Firmware of Managed Devices.....	77
Scheduling a Firmware Deployment for Managed Devices.....	78
Deleting a Firmware Deployment Schedule.....	79
Deploying a Configuration to Managed Devices.....	80
Scheduling a Configuration Deployment for Managed Devices.....	81
Deleting a Configuration Deployment Schedule.....	82
8. Map View.....	84
Viewing Detailed Device Information.....	85
Editing the Location of a Device.....	86
9. Report.....	88
Inventory Reports.....	88
Generating a Current Inventory Report.....	88
Scheduling an Inventory Report.....	89
Cellular Signal Reports.....	91
Scheduling a Cellular Signal Report.....	91
Data Usage Reports.....	92
Generating a Cellular Data Usage Report.....	92
Scheduling a Cellular Data Usage Report.....	94
Trail Reports.....	95
Generating a Trail Report.....	95
Scheduling a Trail Report.....	96
Viewing GPS Trajectories.....	97
Report Settings.....	98
Configure Report Time Zone Settings.....	98
Editing a Report Schedule.....	99
10. Logging.....	100
Event Log.....	100
Device Log.....	100
Firewall Log.....	102
VPN Log.....	106
Audit Log.....	108
Event Log Settings.....	110

Notifications.....	111
Adding a Notification.....	111
11. Administration.....	114
User Accounts	114
User Roles.....	114
Account Input Format	116
Adding a User Account	117
Editing an Existing User Account	118
Deleting a User Account	119
Configuring the Password Policy	119
Changing Your Account Password	120
Licenses	121
Introduction to Licenses	121
Viewing Your Product License Information	121
Alert Messages.....	122
Adding a New License	123
Settings.....	125
Configuring Preferences	125
Configuring the System Time.....	125
Editing Email Settings	126
Editing Syslog Settings	127

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

2. Installation

Setting Up the Virtual Machine

Installing MXsecurity on a VMware Workstation

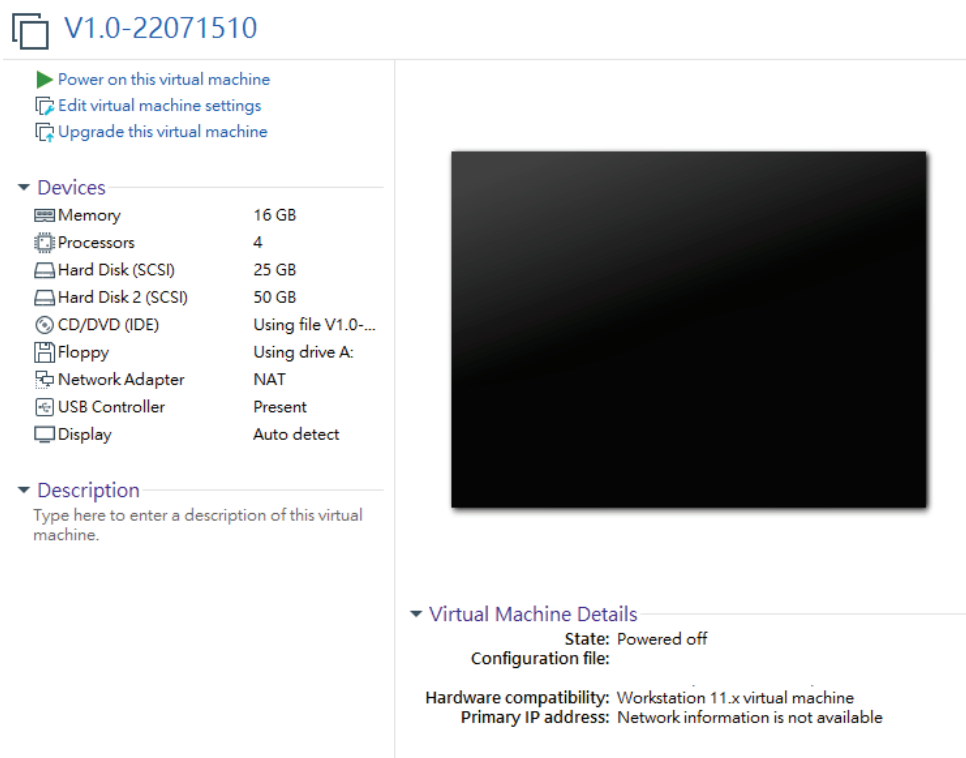
This section describes how to deploy MXsecurity to a VMware Workstation system.

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.



The screenshot displays the VMware Workstation interface for a virtual machine named "V1.0-22071510". The interface is divided into several sections:

- Actions:** Power on this virtual machine, Edit virtual machine settings, Upgrade this virtual machine.
- Devices:**

Memory	16 GB
Processors	4
Hard Disk (SCSI)	25 GB
Hard Disk 2 (SCSI)	50 GB
CD/DVD (IDE)	Using file V1.0-...
Floppy	Using drive A:
Network Adapter	NAT
USB Controller	Present
Display	Auto detect
- Description:** Type here to enter a description of this virtual machine.
- Virtual Machine Details:**
 - State: Powered off
 - Configuration file:
 - Hardware compatibility: Workstation 11.x virtual machine
 - Primary IP address: Network information is not available

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**.

V1.0-22071510

[Power on this virtual machine](#)
[Edit virtual machine settings.](#)
[Upgrade this virtual machine](#)

▼ **Devices**

Memory	16 GB
Processors	4
Hard Disk (SCSI)	25 GB
Hard Disk 2 (SCSI)	50 GB
CD/DVD (IDE)	Using file V1.0-...
Floppy	Using drive A:
Network Adapter	NAT
USB Controller	Present
Display	Auto detect

▼ **Description**
Type here to enter a description of this virtual machine.

▼ **Virtual Machine Details**

State: Powered off
Configuration file:
Hardware compatibility: Workstation 11.x virtual machine
Primary IP address: Network information is not available

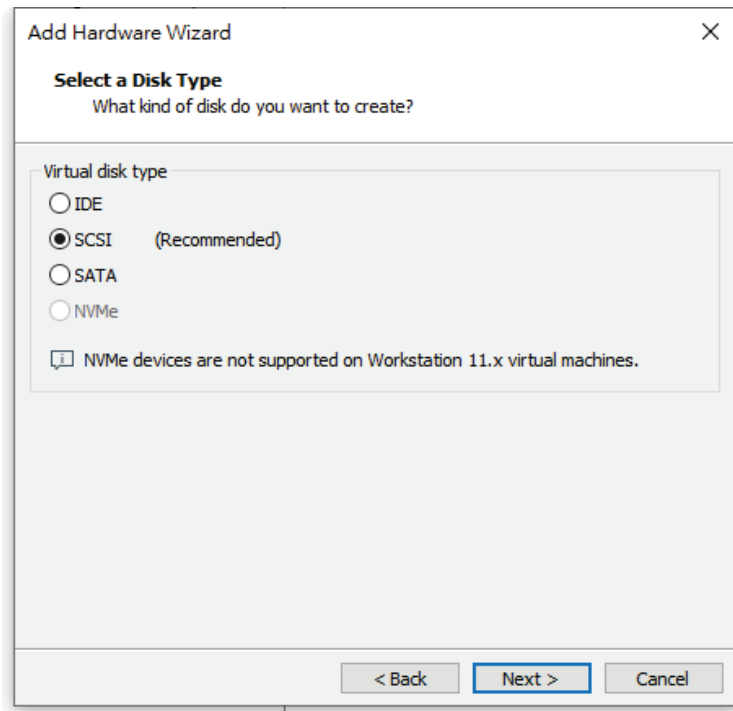
b. Click **Add**, then choose **Hard Disk**.

Add Hardware Wizard

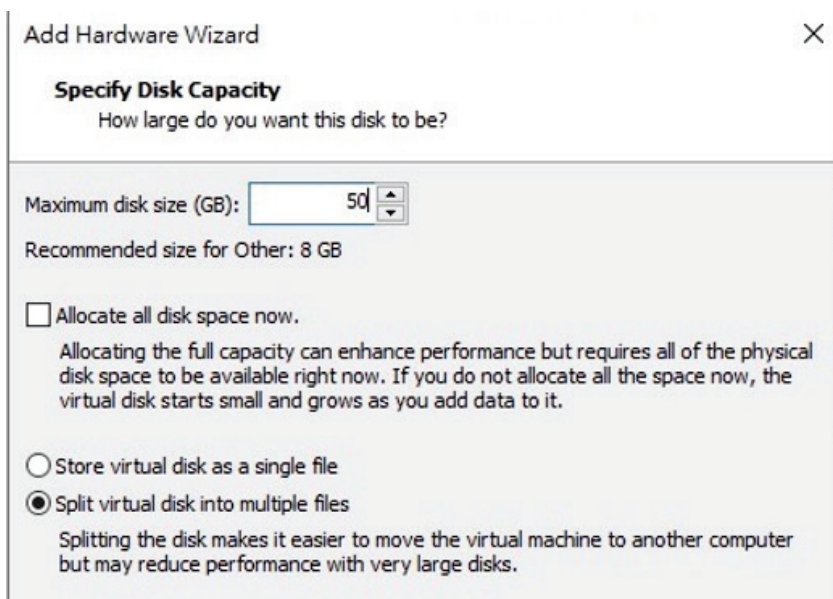
Hardware Type
What type of hardware do you want to install?

Hardware types:	Explanation
<input checked="" type="checkbox"/> Hard Disk	Add a hard disk.
<input type="checkbox"/> CD/DVD Drive	
<input type="checkbox"/> Floppy Drive	
<input type="checkbox"/> Network Adapter	
<input type="checkbox"/> USB Controller	
<input type="checkbox"/> Sound Card	
<input type="checkbox"/> Parallel Port	
<input type="checkbox"/> Serial Port	
<input type="checkbox"/> Printer	
<input type="checkbox"/> Generic SCSI Device	

- 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:
- Power off the MXsecurity instance.
 - Increase the external disk size based on your requirements.
 - 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).
- Click **Edit virtual machine settings**.
 - Configure the amount of memory.
 - 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

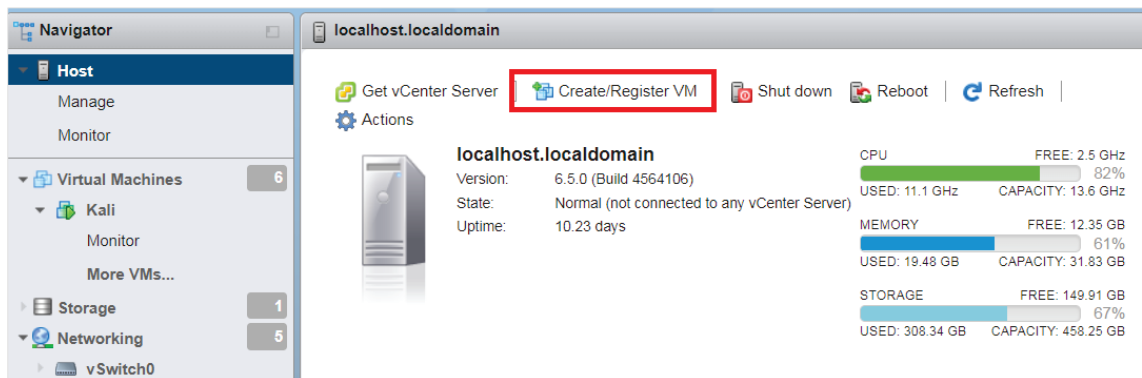
This section describes how to deploy MXsecurity to a VMware ESXi system.

Prerequisites

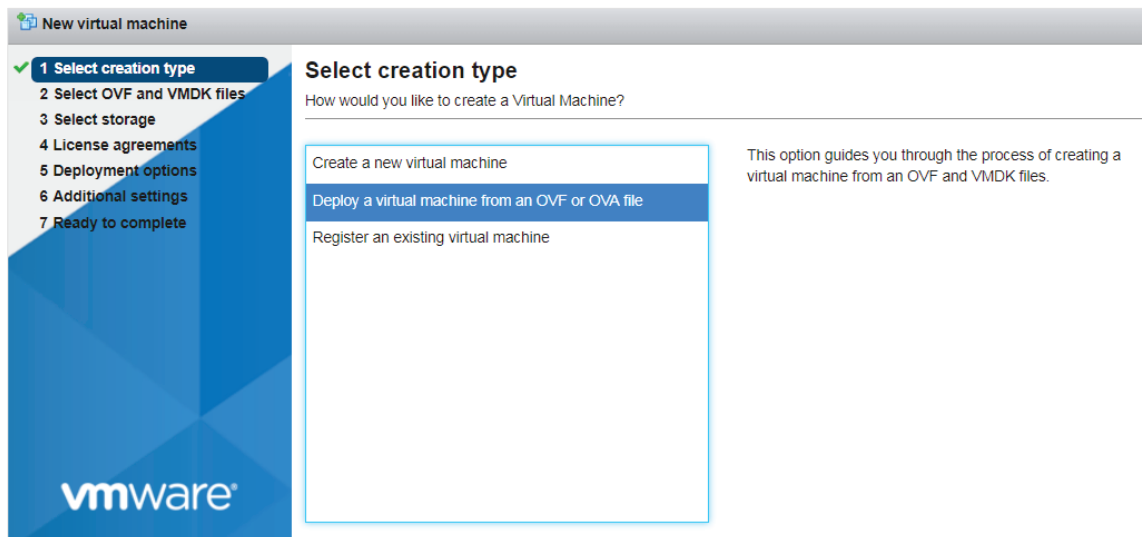
- The OVA packages provided by Moxa must be available and accessible to VMware ESXi.
- ESXi version 6 or above with the required specifications.
- The necessary networks have been properly created in ESXi.

Steps:

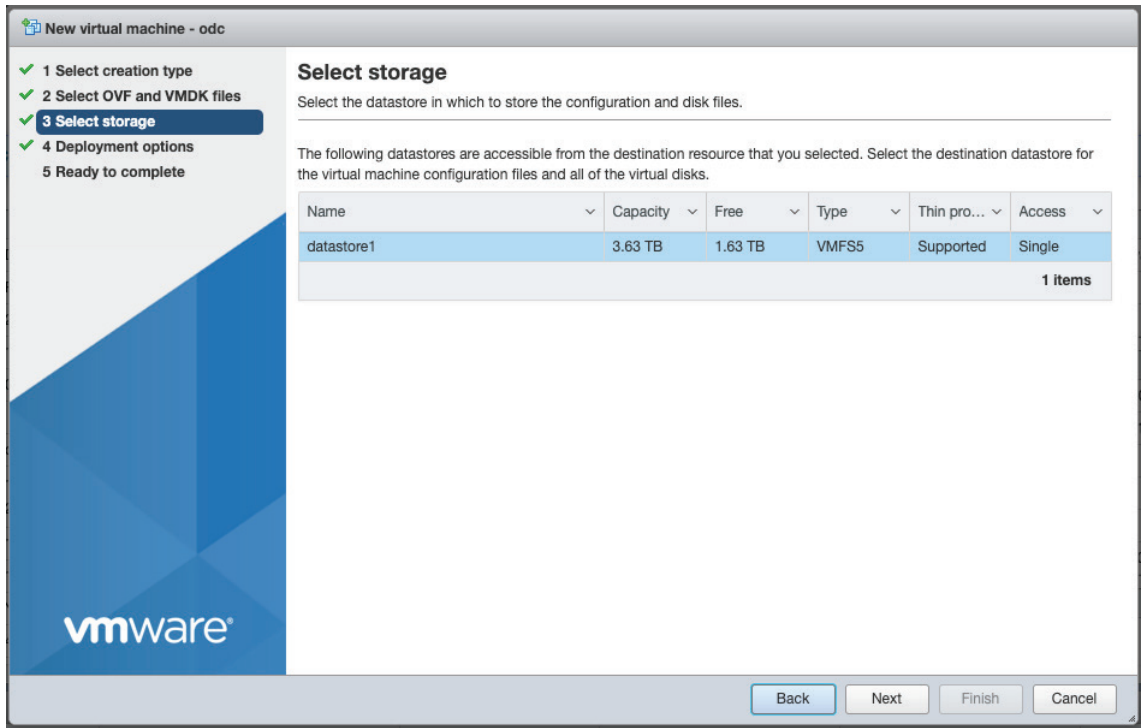
1. Log in to the VMware vSphere web client.
2. Under **Navigator**, click **Host** and then click **Create/Register VM**.



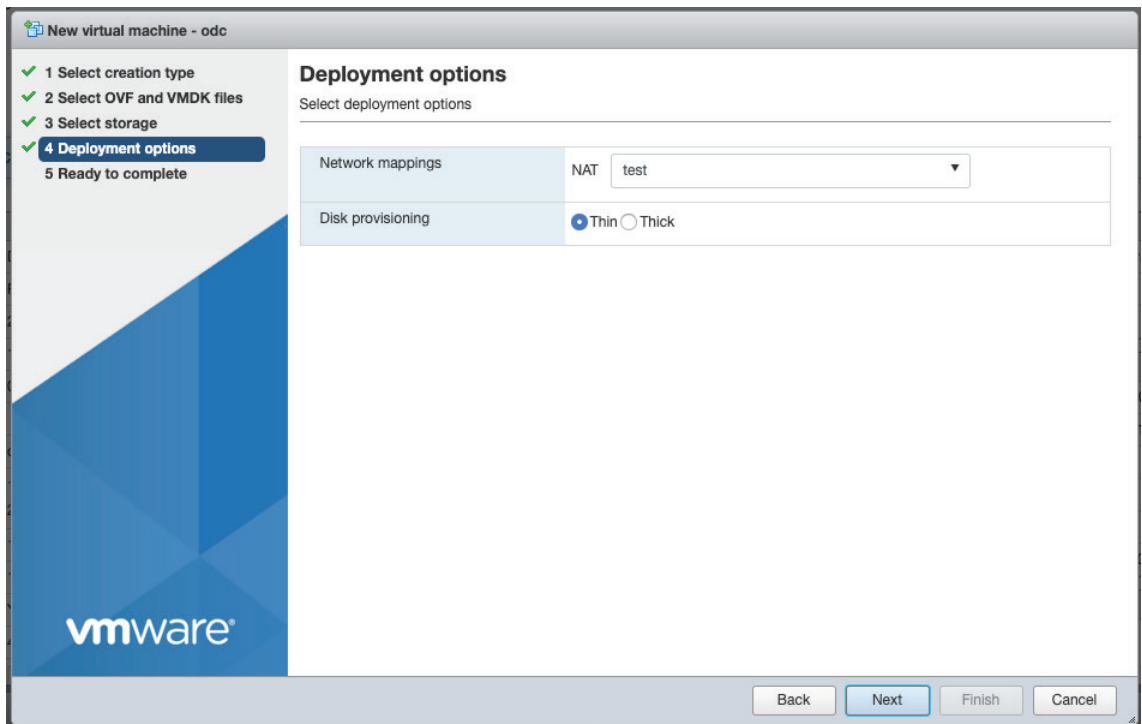
3. Select **Deploy a virtual machine from an OVF or OVA file**.



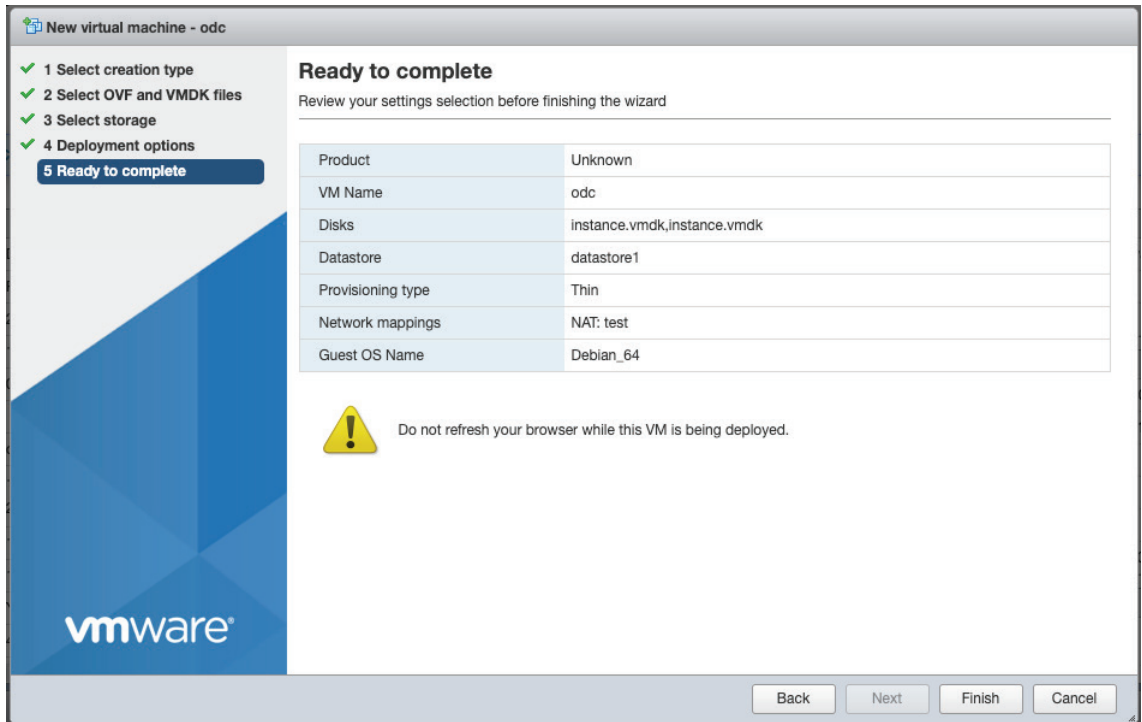
4. Enter a name for your MXsecurity instance and then select an MXsecurity image to upload.
5. Choose a storage location for the MXsecurity virtual machine.



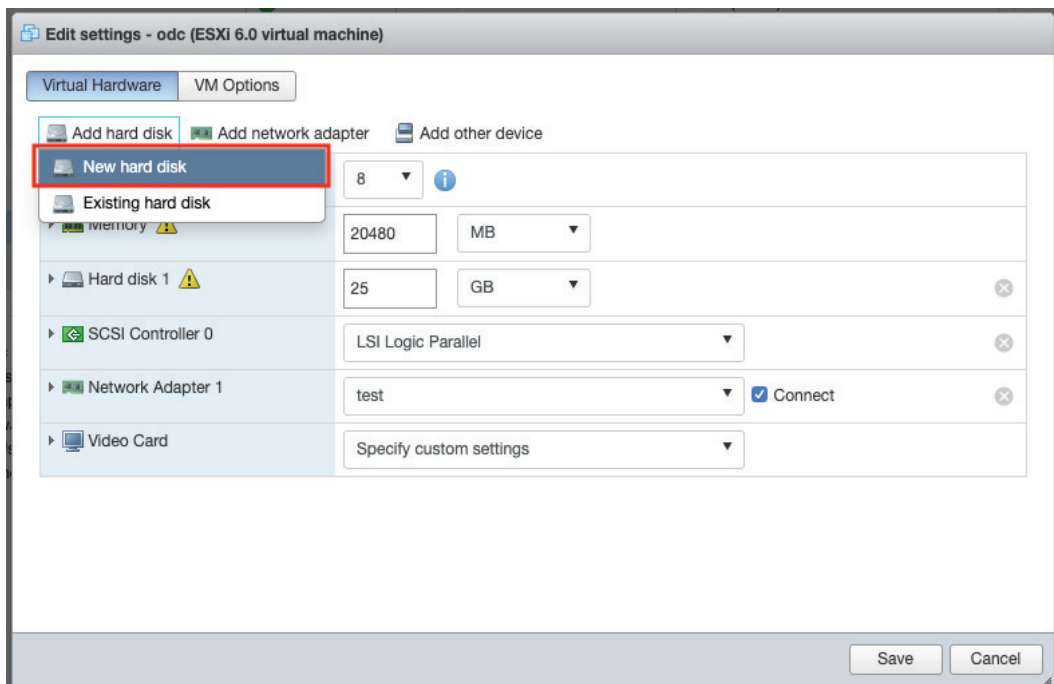
6. Select the deployment options.



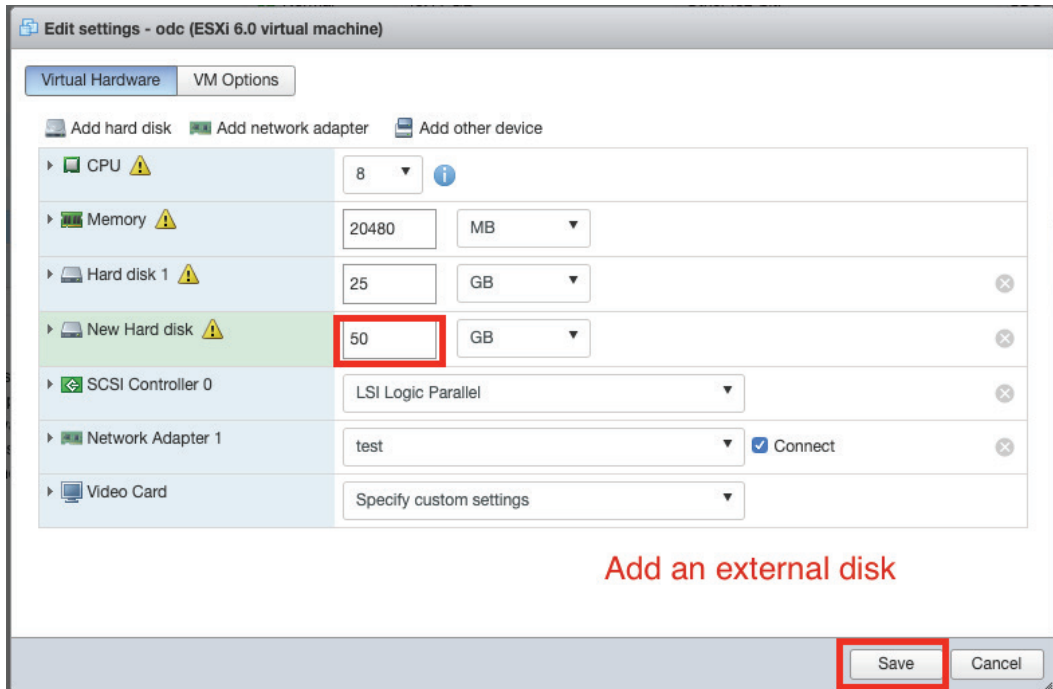
When you see the **Ready to complete** screen, click **Finish** to start the deployment.



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:
- Power off the MXsecurity instance.
 - Increase the external disk size based on your requirements.
 - Power the MXsecurity instance back on.

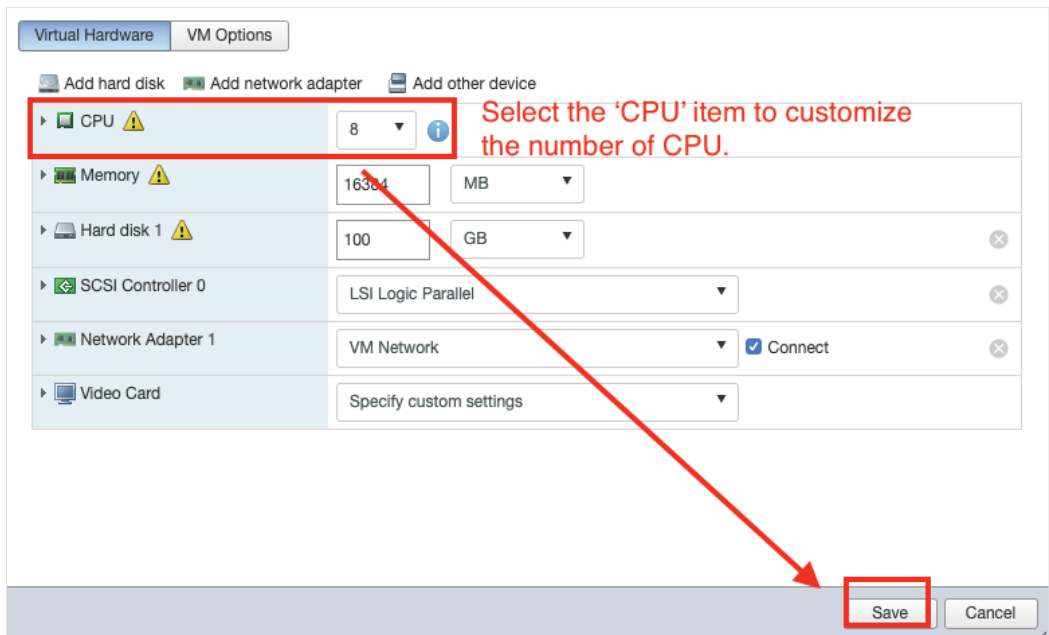
If you want to migrate the existing MXsecurity settings to the newly launched VM, please refer to [Migration](#).



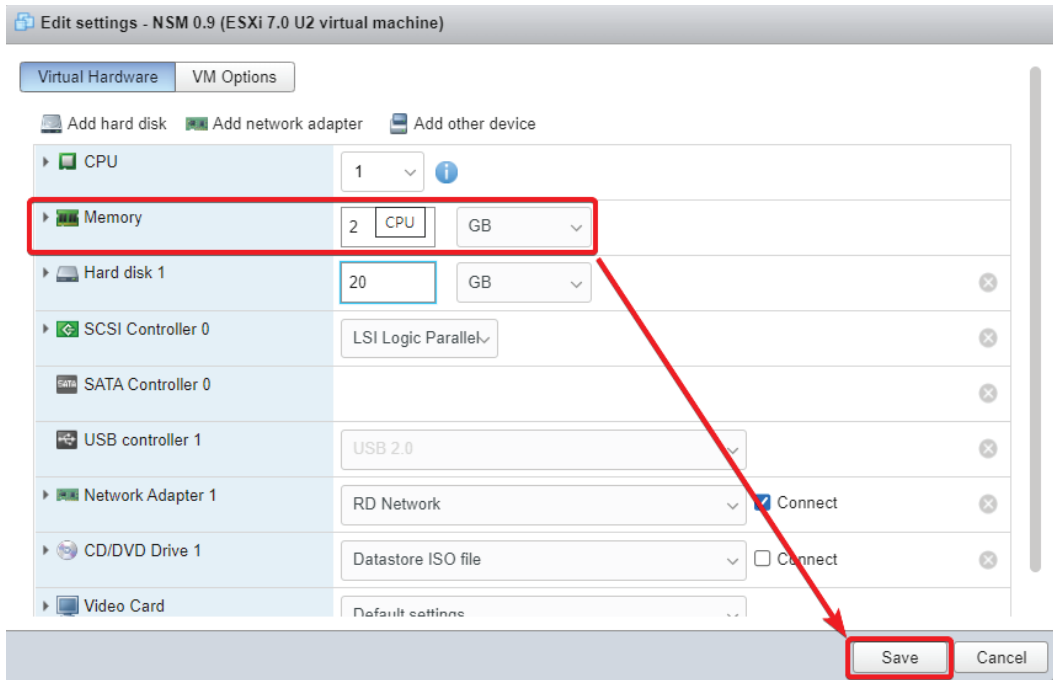
NOTE

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.

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

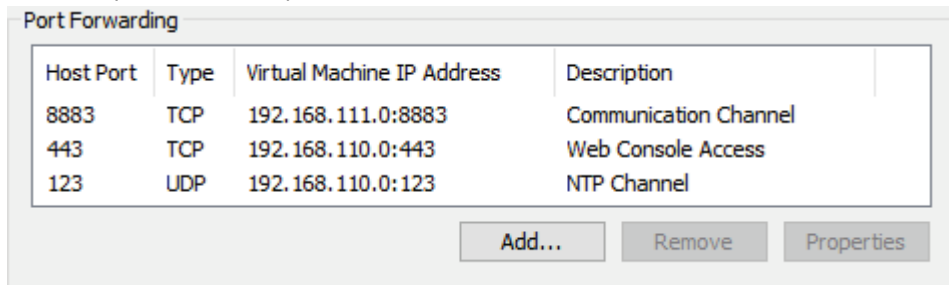
- b. Log in to the MXsecurity again with your new password.
4. **(Optional)** After logging in to the MXsecurity, type the "help" command to see a list of available commands.

```
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.



Host Port	Type	Virtual Machine IP Address	Description
8883	TCP	192.168.111.0:8883	Communication Channel
443	TCP	192.168.110.0:443	Web Console Access
123	UDP	192.168.110.0:123	NTP Channel



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
```

3. Migration

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

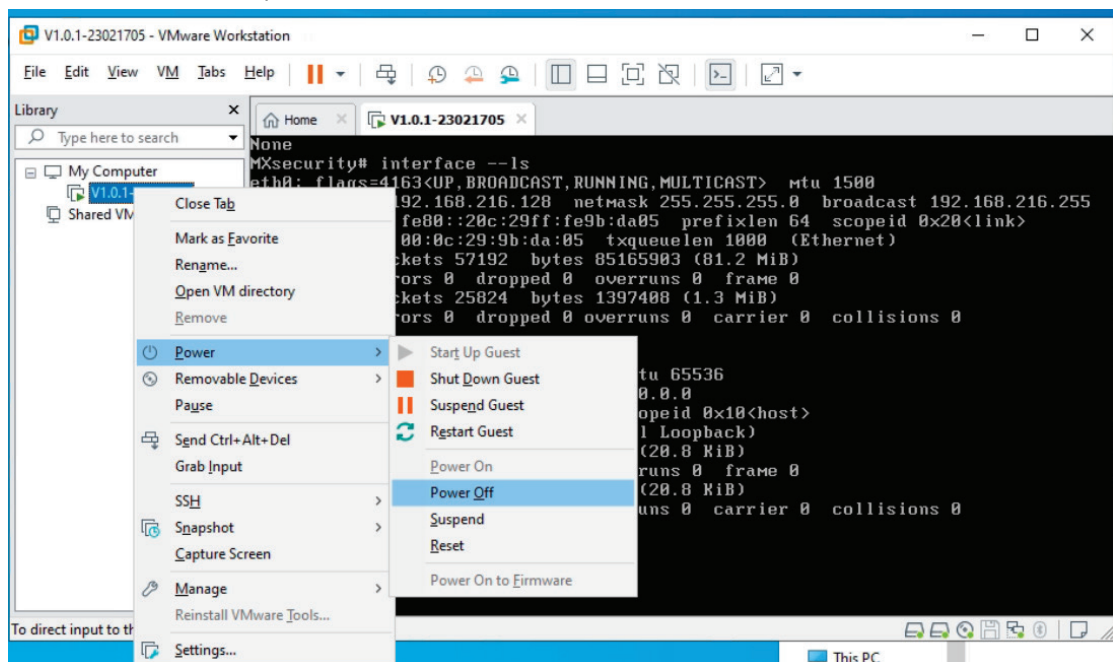
MXsecurity v1.1.0 has implemented enhanced connection security measures. To avoid issues, managed devices should be upgraded to a firmware version and MXsecurity Agent Package which is compatible with MXsecurity v1.1.0. The following device firmware versions are compatible with MXsecurity v1.1.0:

- 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.

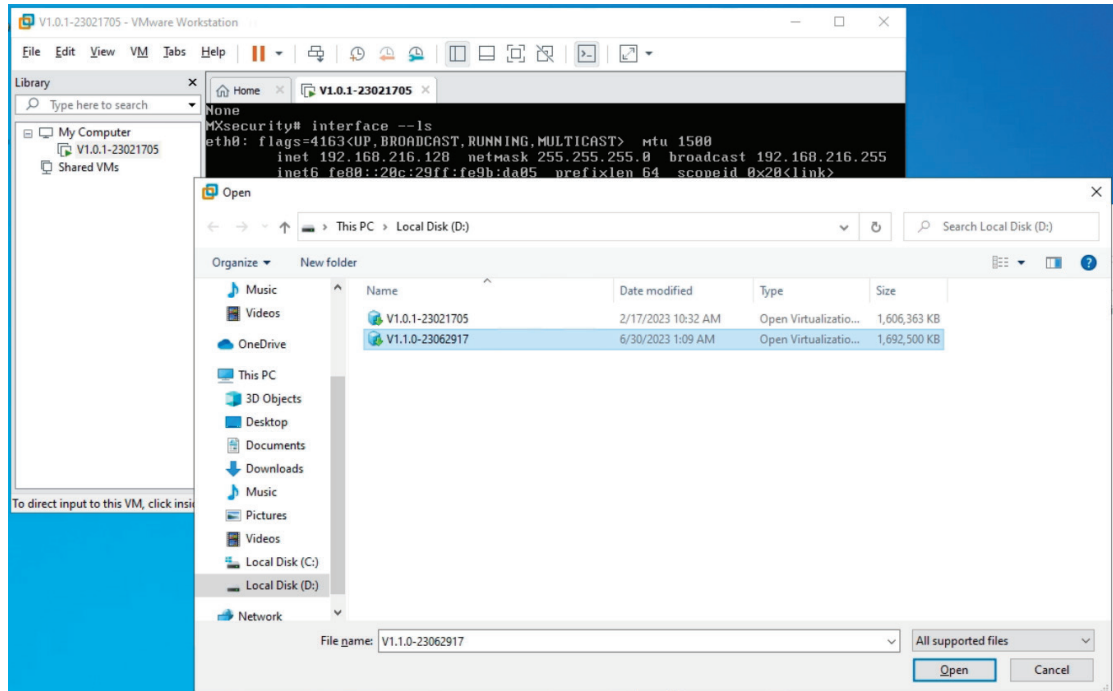
Steps:

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

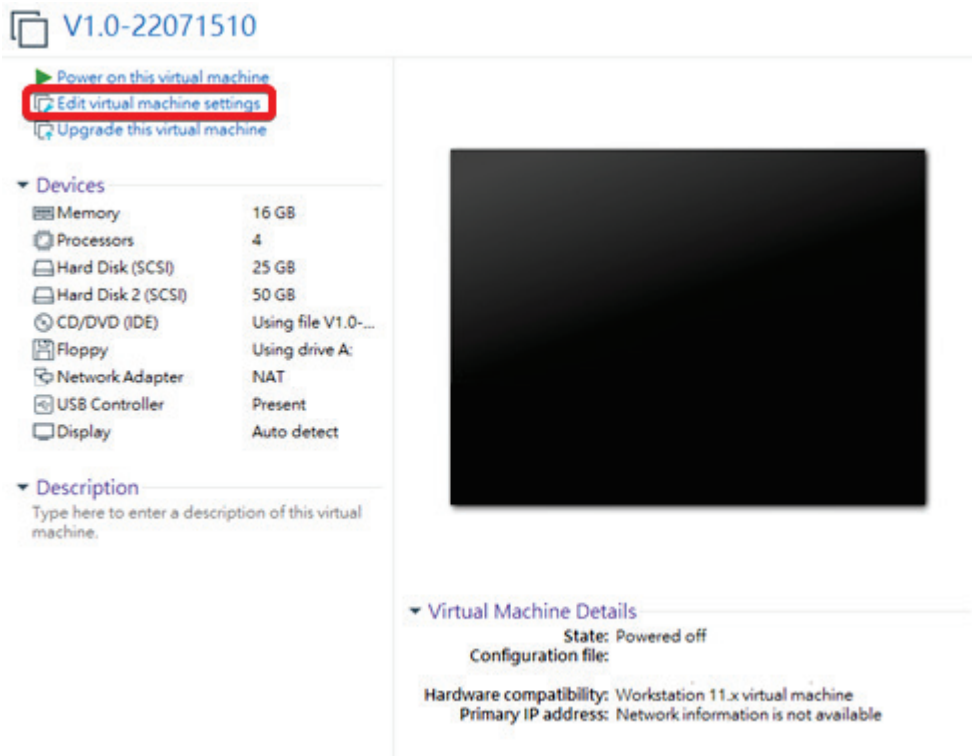


3. Go to **File > Open** in the menu bar.

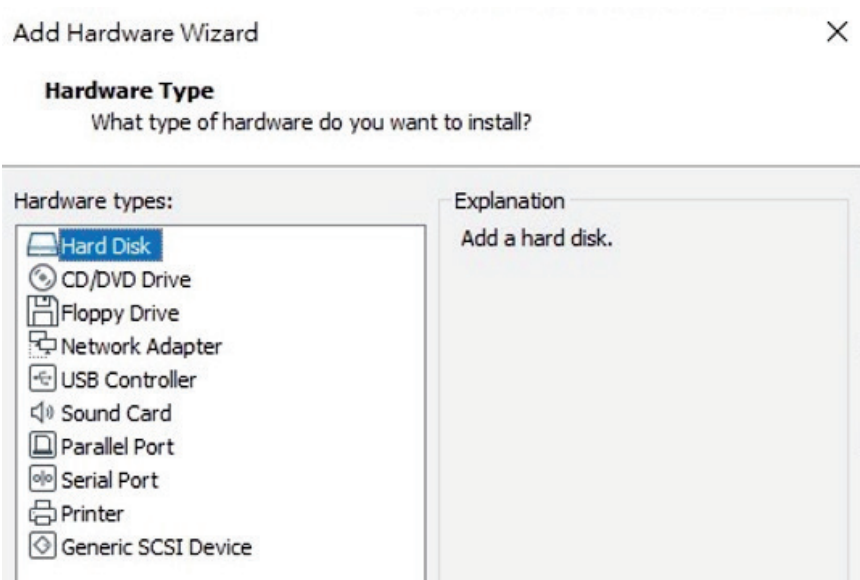
4. Select the VM image file (*.ova) of the new MXsecurity version from your localhost file path and click **Open**.



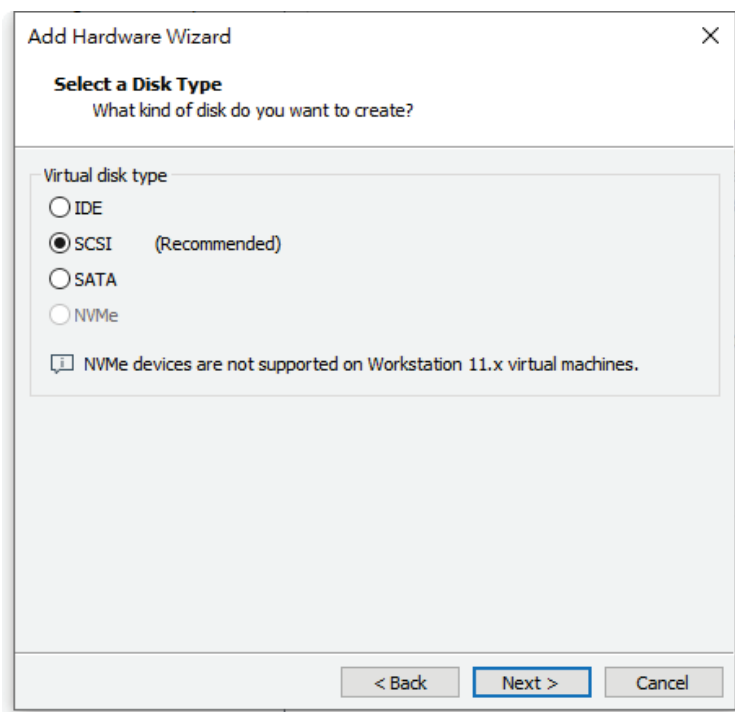
5. Add an existing Hard Disk.
a. Click **Edit virtual machine settings**.



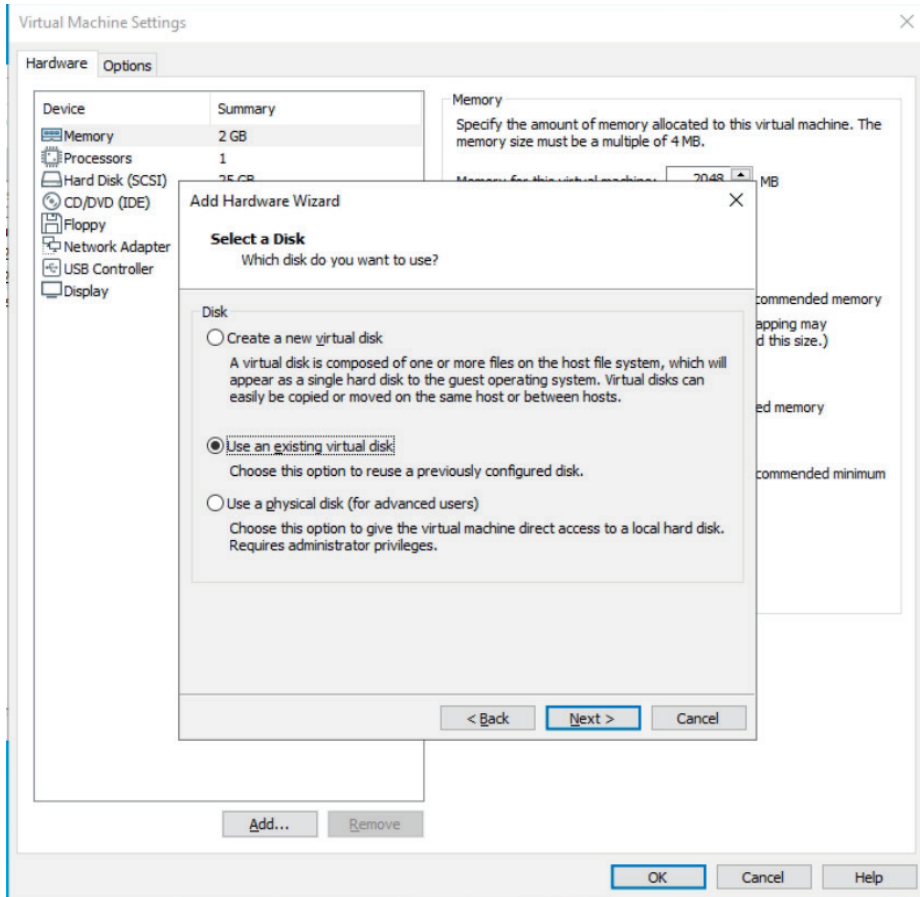
- b. Click **Add**, then choose **Hard Disk**.



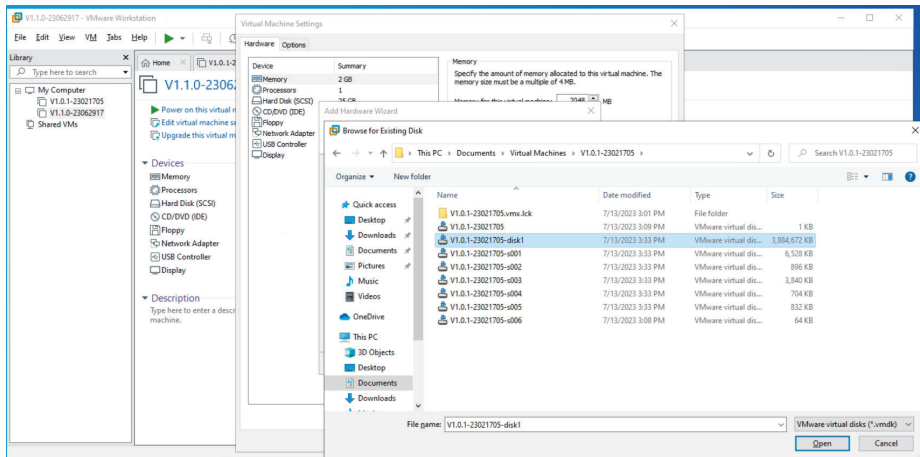
c. Select a disk type and click **Next**.



- 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**.
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

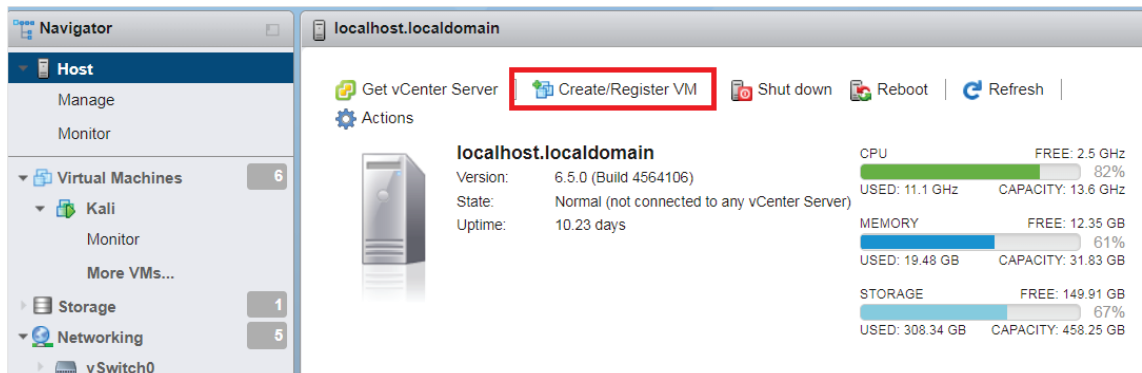
MXsecurity v1.1.0 has implemented enhanced connection security measures. To avoid issues, managed devices should be upgraded to a firmware version and MXsecurity Agent Package which is compatible with MXsecurity v1.1.0. The following device firmware versions are compatible with MXsecurity v1.1.0:

- 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

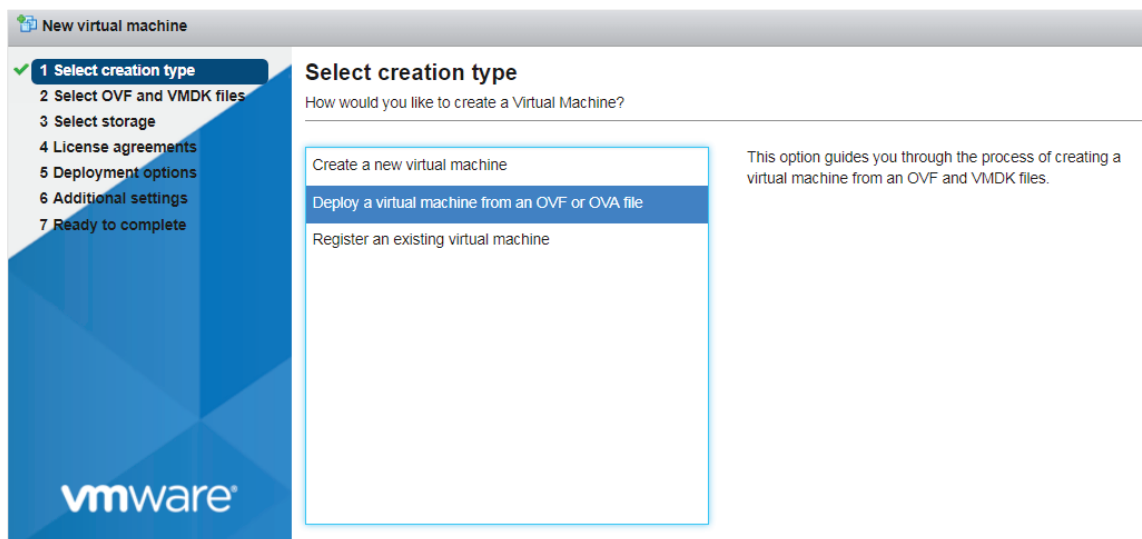
If you have an older version of the MXsecurity Agent Package installed, you will need to manually upgrade it to v2.0.13 on the managed device first. To manually upgrade the software package, navigate to **System > System Management > Software Package Management > MXsecurity Agent Package** in the Secure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

Steps:

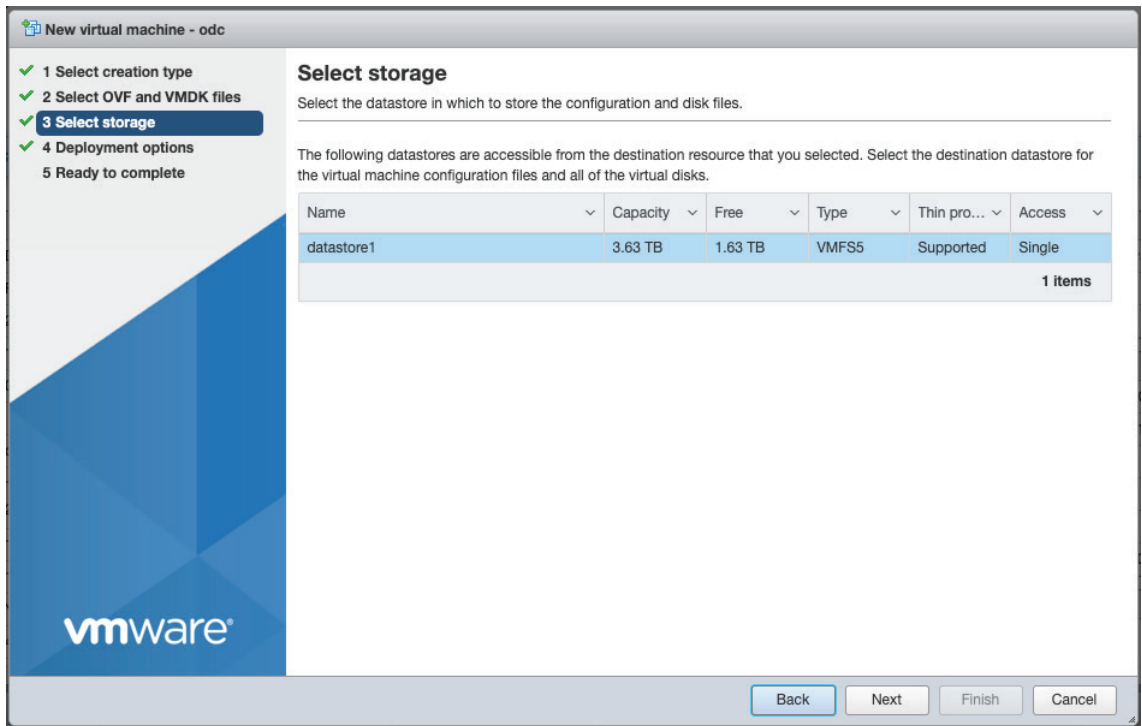
1. Start the VMware ESXi.
2. Power off the MXsecurity instance.
3. Under **Navigator**, click **Host** and then click **Create/Register VM**.



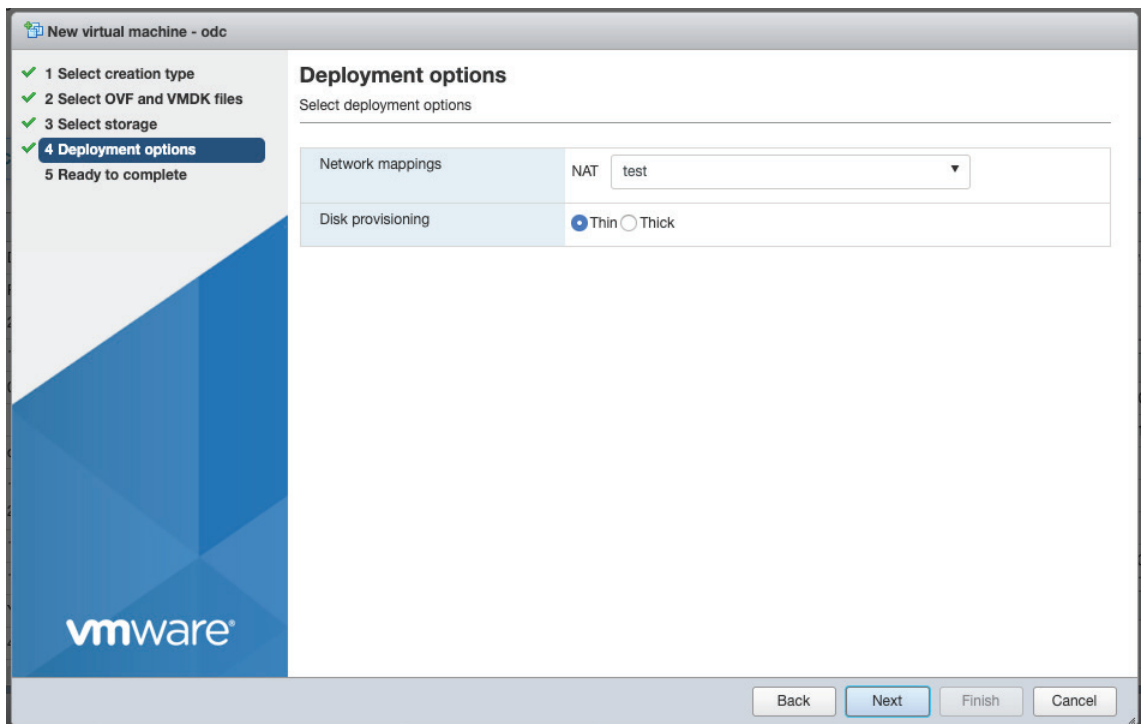
4. Select **Deploy a virtual machine from an OVF or OVA file**.



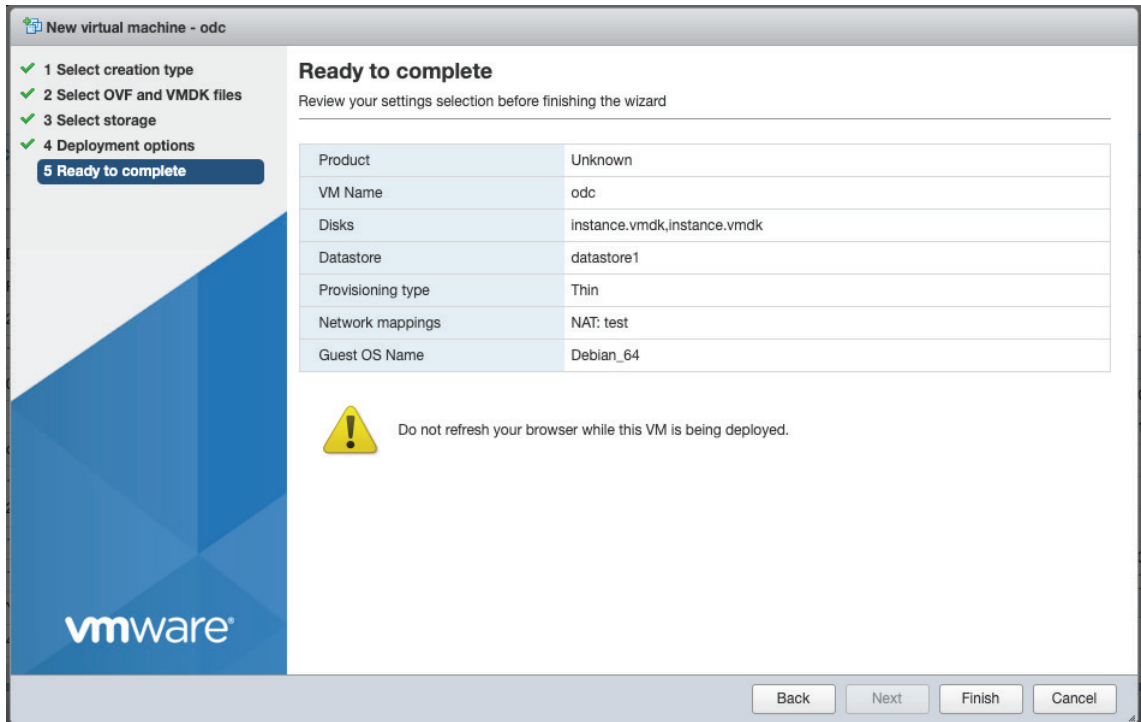
5. Enter a name for your MXsecurity instance and then the image file of the new MXsecurity version to upload.
6. Choose a storage location for the MXsecurity virtual machine.



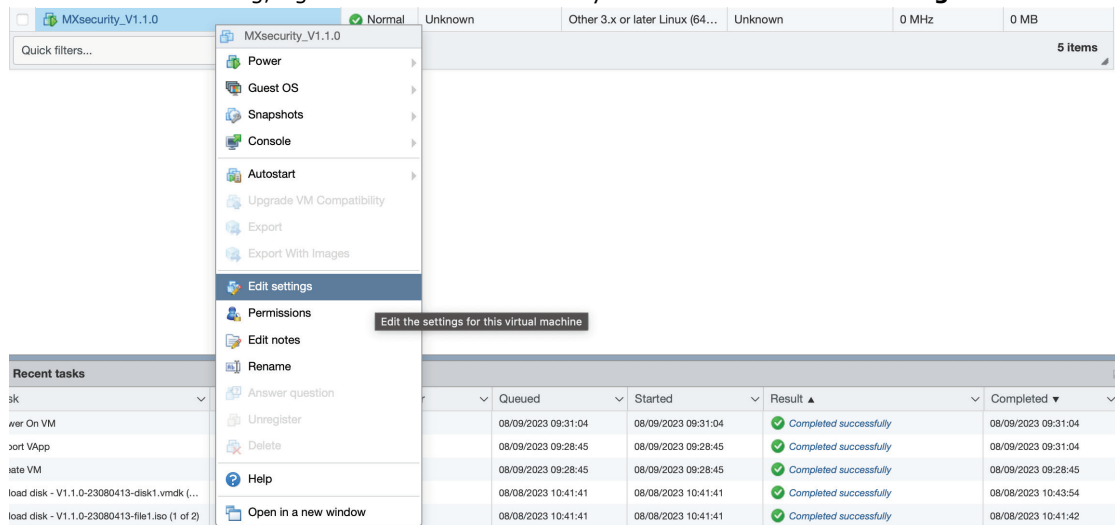
7. Select the deployment options.



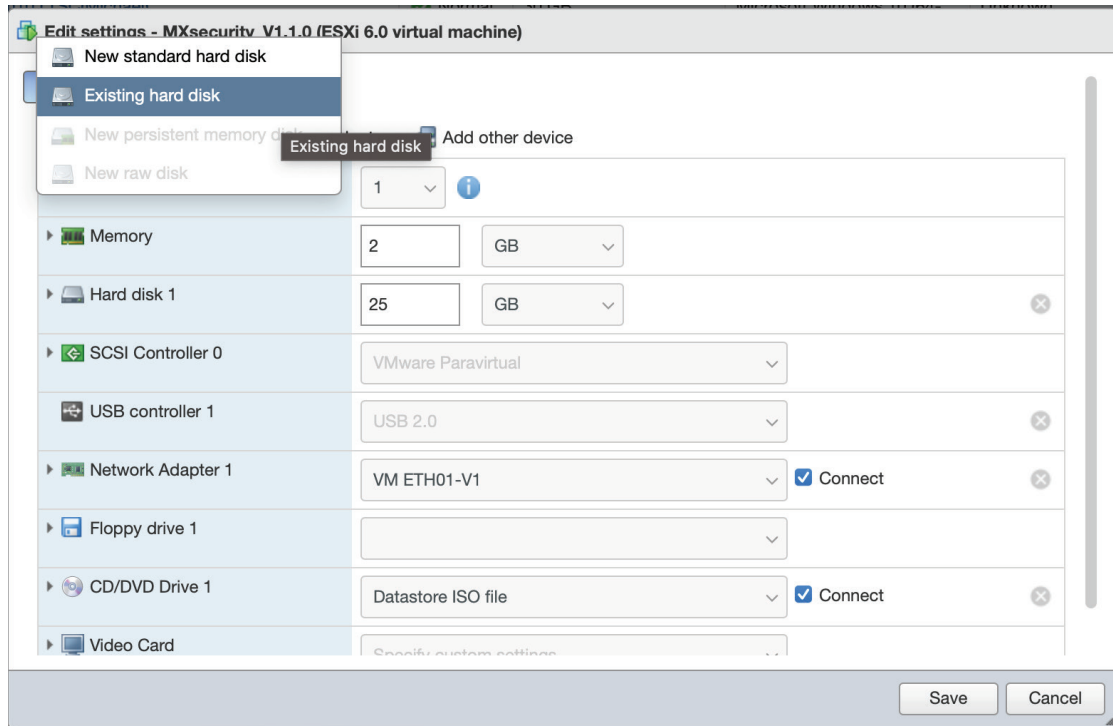
When you see the **Ready to complete** screen, click **Finish** to start the deployment.



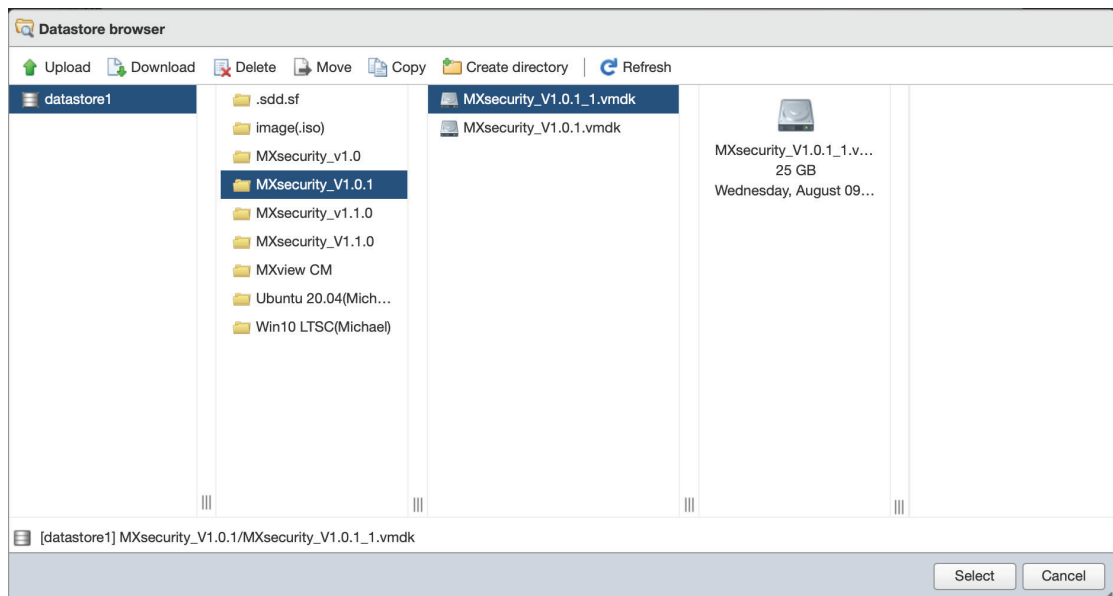
8. Under the **Recent tasks** pane, you will see a progress bar indicating that the MXsecurity image is being uploaded. Wait until the upload has finished.
9. When finished installing, right-click the new MXsecurity instance and click **Edit Settings**.



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



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



12. Click **Save**.
13. Log in to the MXsecurity web console and confirm the migration was successful.

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.



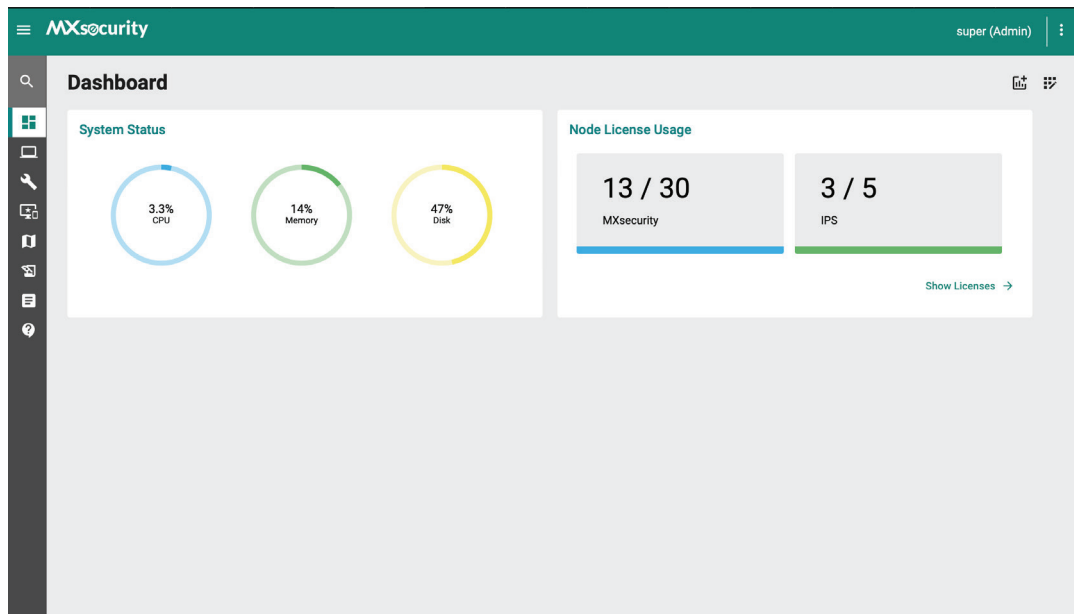
NOTE

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.

The screenshot shows the MXsecurity configuration page. At the top, there is a 'Connection Status' section with a refresh icon. Below it, a table displays the current status: Status is 'Connecting', Package Version is '1.0.0017', Service Address is '192.168.127.1', and Profile Synchronization is '---'. Below this is a 'New Connection' form with input fields for Service Address (with a character count of 0 / 64), HTTPS Port (set to 443), and Communication Port (set to 8883). A 'CONNECT' button is located at the bottom of the form.

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.

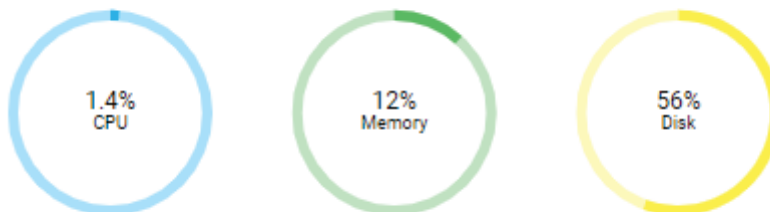
Dashboard Widgets Overview

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.

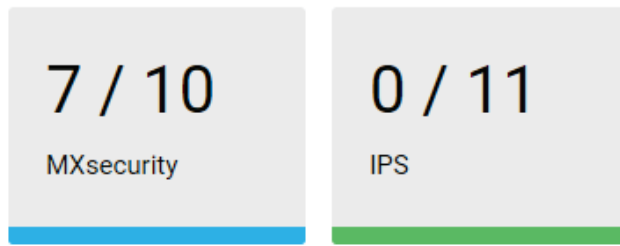
System Status



Node License Usage

This widget displays the number of registered devices and the number of unused node licenses.

Node License Usage



[Show Licenses →](#)

Group Status

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

Group Status

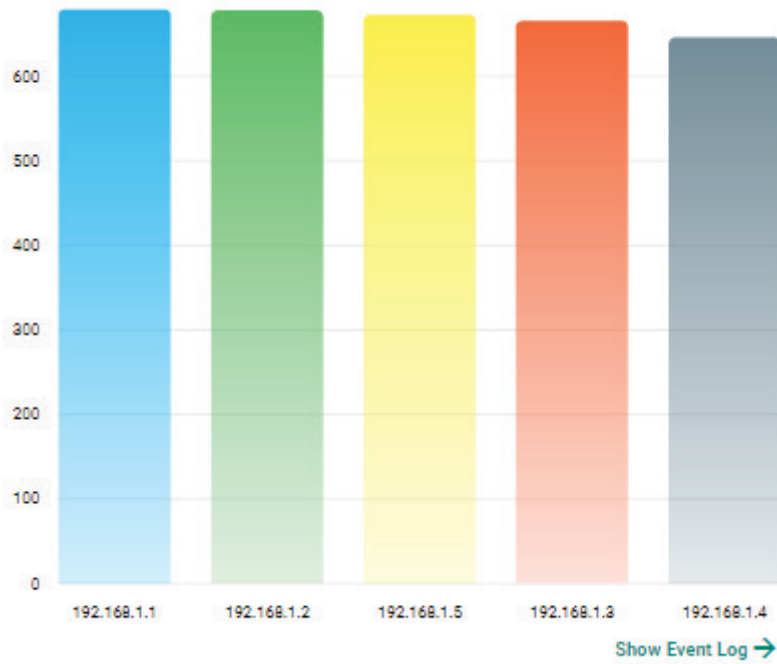


[Show Device Group →](#)

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.

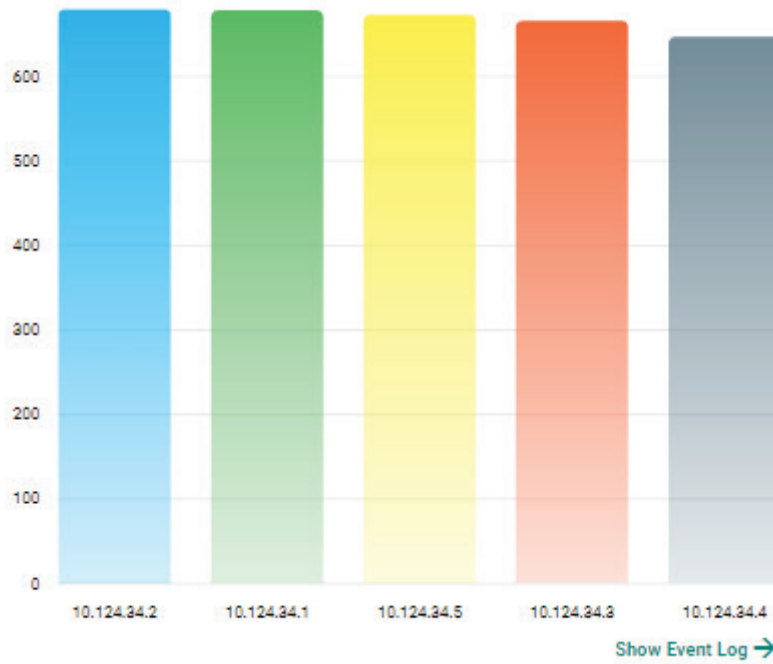
Top 5 Layer 3-7 Policy Events by Source IP



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.

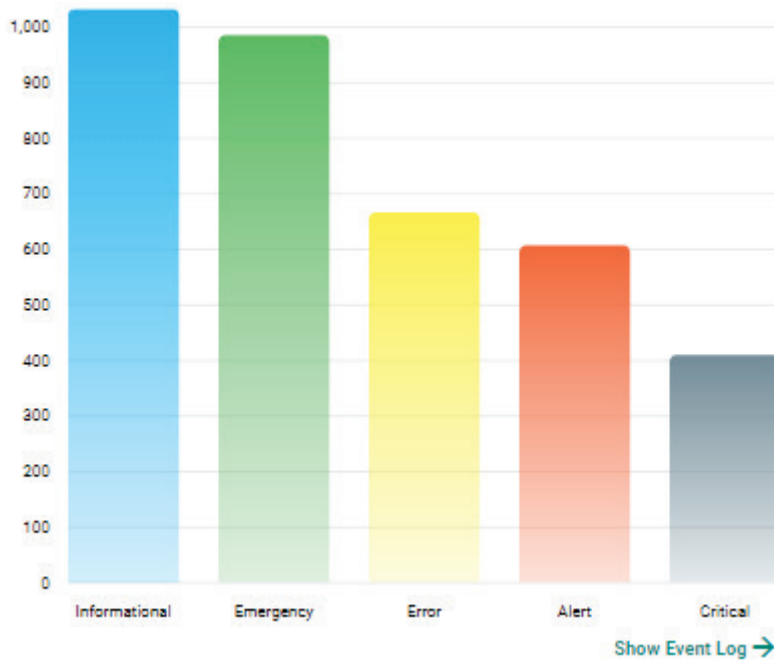
Top 5 Layer 3-7 Policy Events by Destination IP



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.

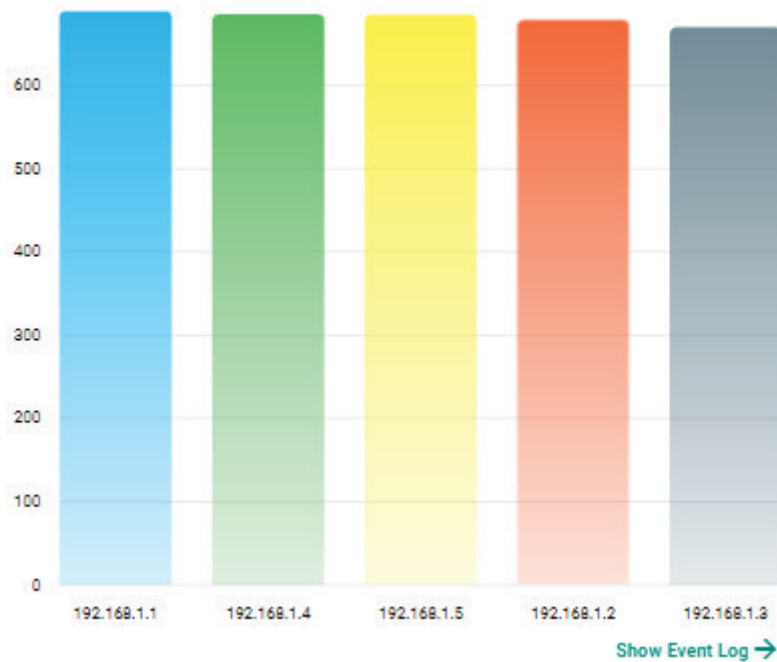
Top 5 Layer 3-7 Policy Events by Severities



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

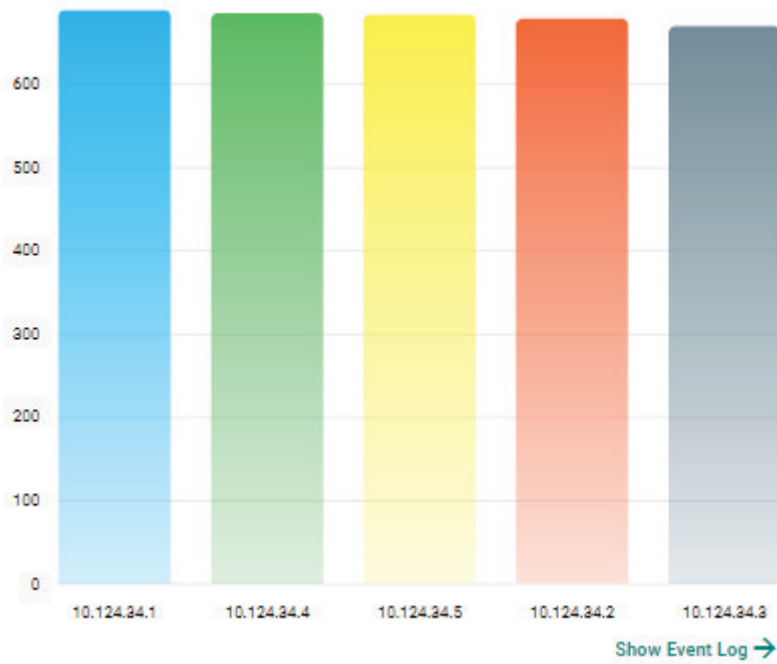
Top 5 Protocol Filter Policy Events by Source IP



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.

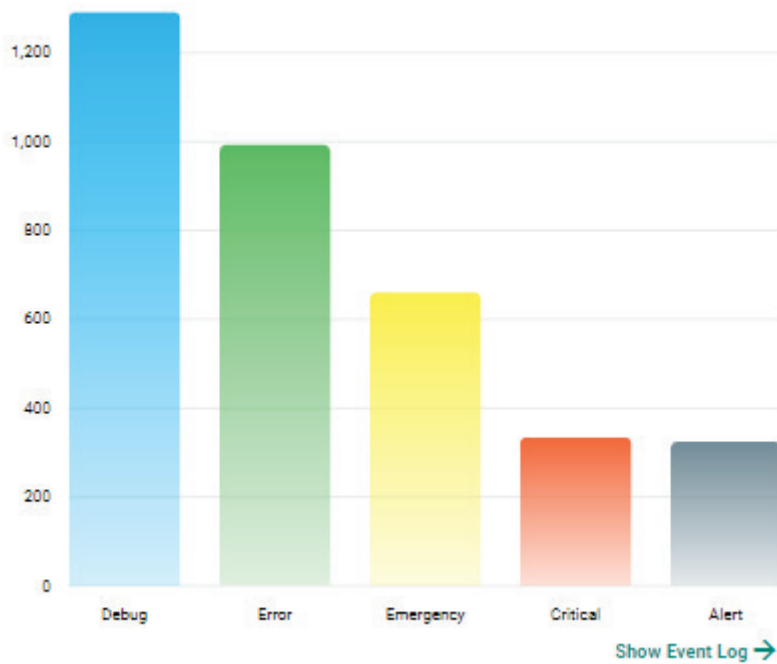
Top 5 Protocol Filter Policy Events by Destination IP



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.

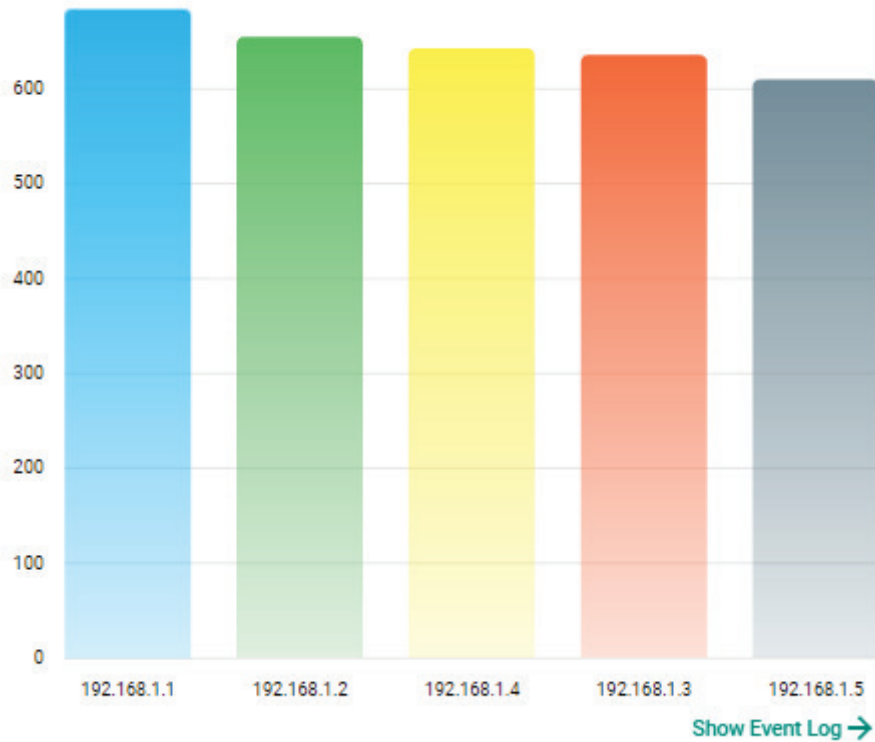
Top 5 Protocol Filter Policy Events by Severities



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.

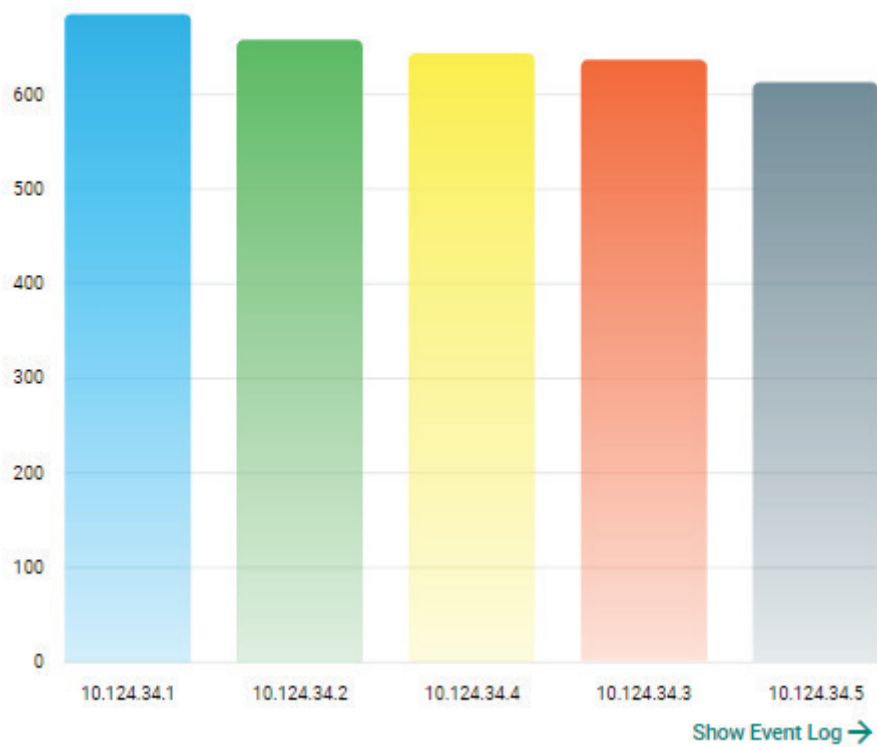
Top 5 ADP Policy Events by Source IP



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.

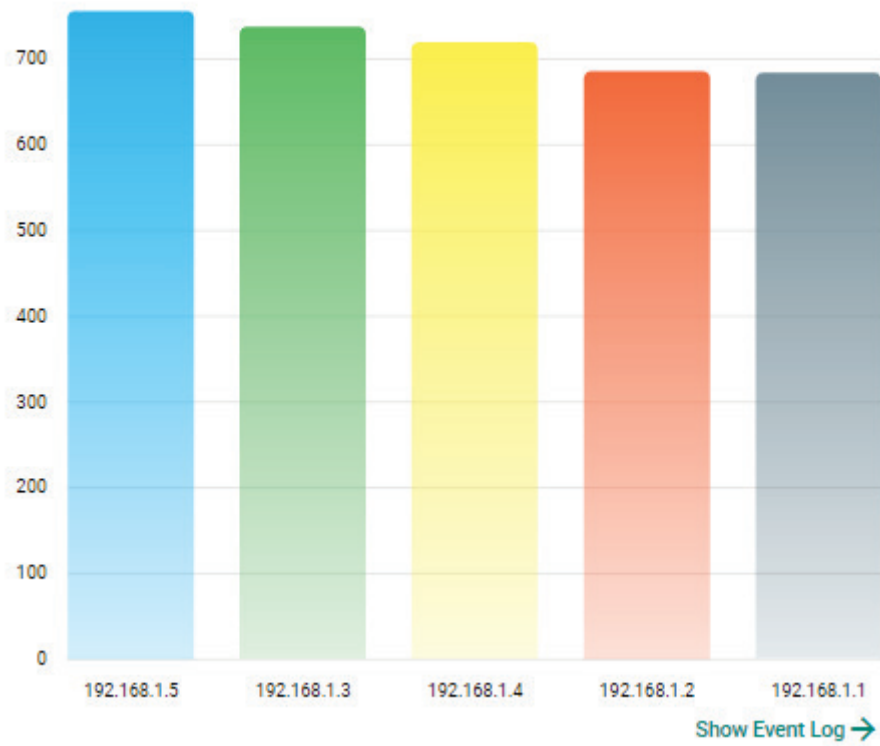
Top 5 ADP Policy Events by Destination IP



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.

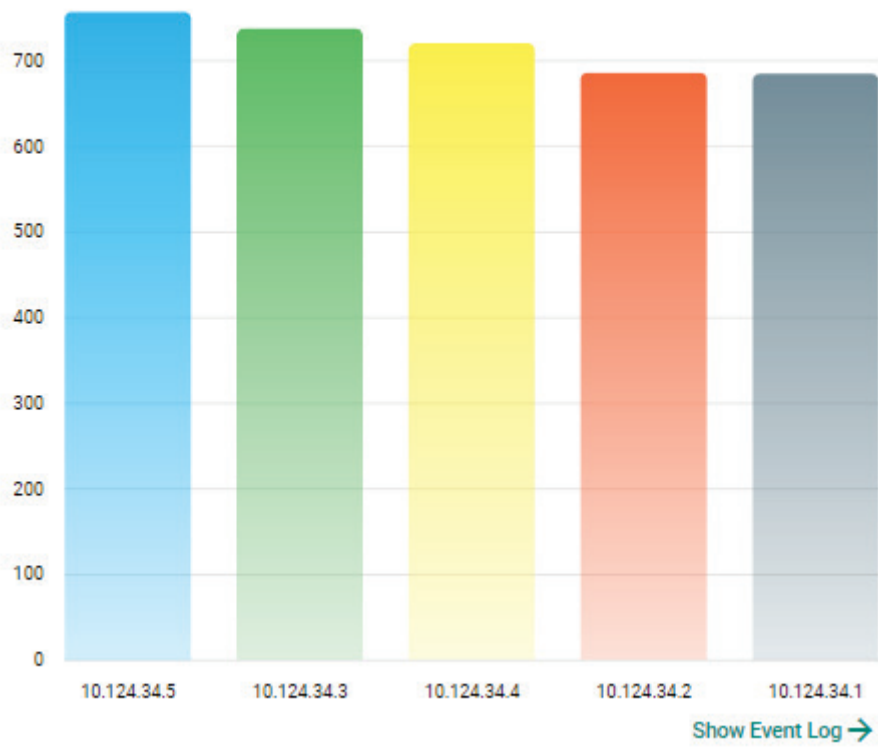
Top 5 IPS Policy Events by Source IP



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.

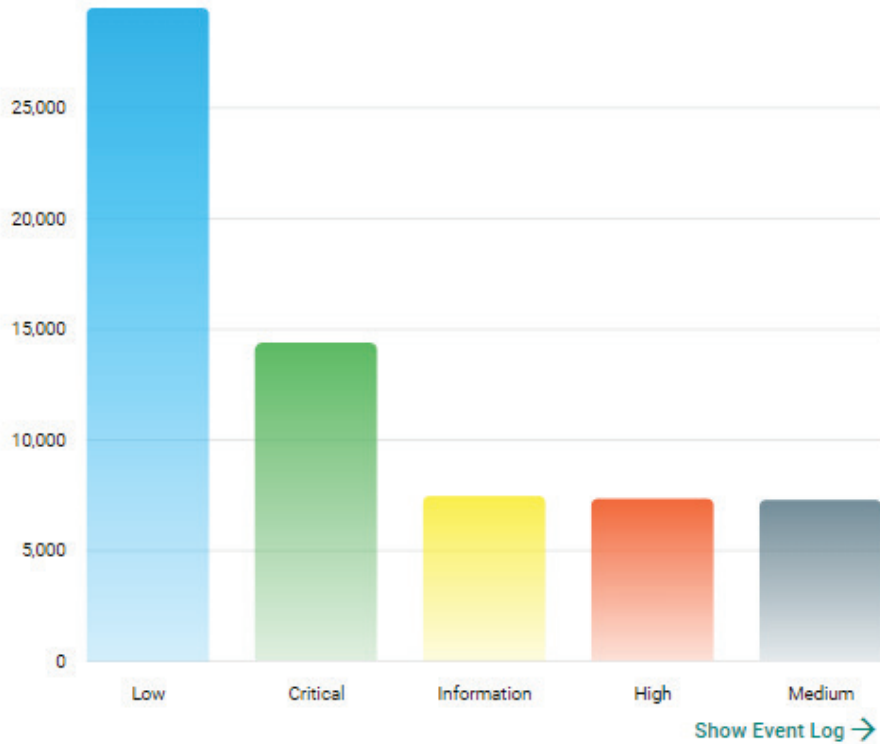
Top 5 IPS Policy Events by Destination IP



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.

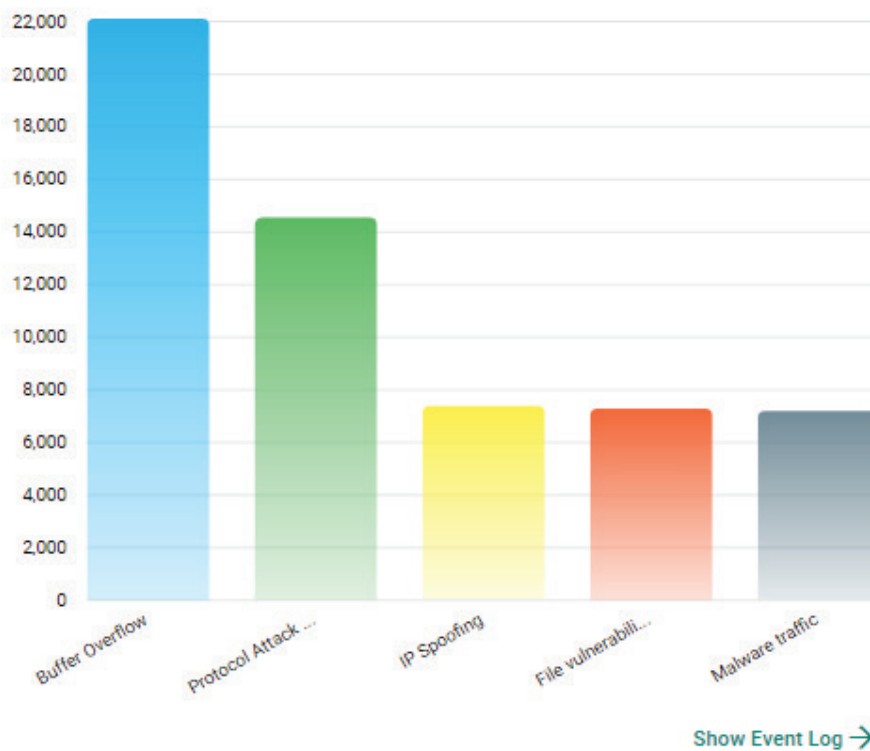
Top 5 IPS Policy Events by Severities



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.

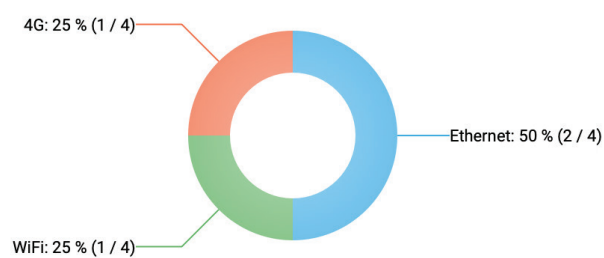
Top 5 IPS Policy Events by Category



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.

Connection Interface (Cellular Router)

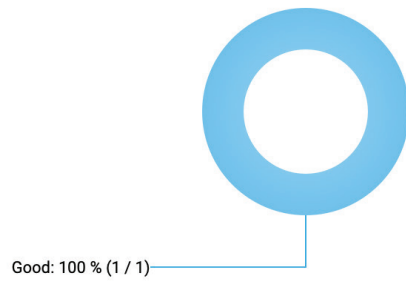


[Show Map View →](#)

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.

Signal Quality (Cellular Router)



[Show Map View →](#)

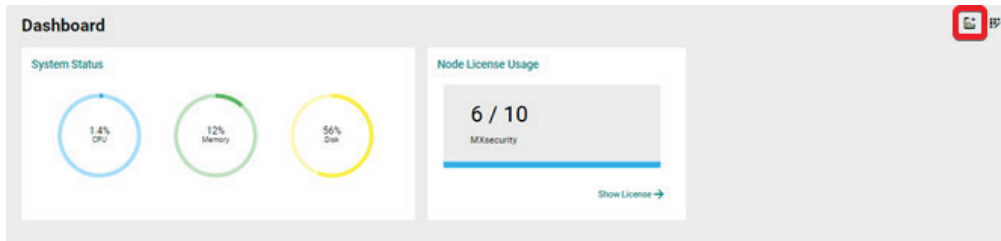
Widget Management

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

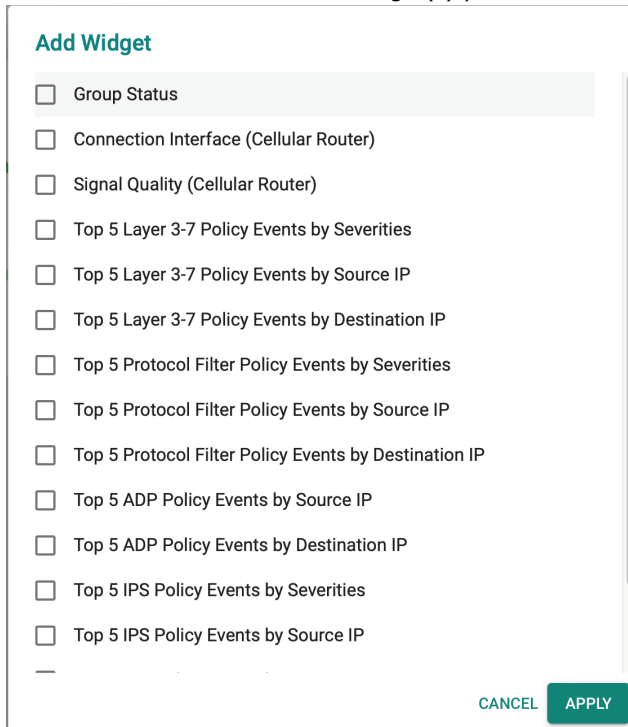
Adding a Widget to the Dashboard

Steps:

1. Click the  icon to add widgets.




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

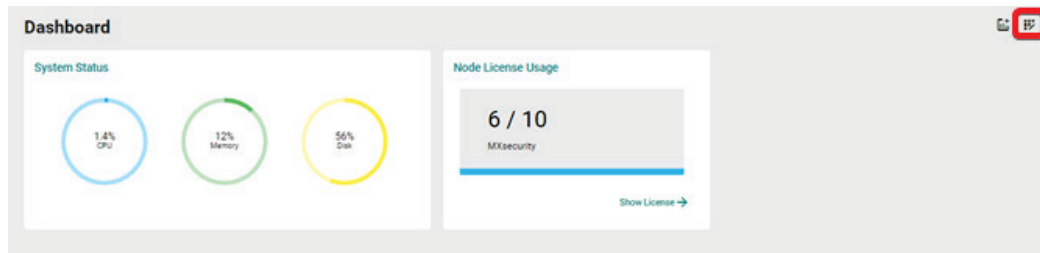


3. Click **APPLY** to add the selected widget(s) to the tab.

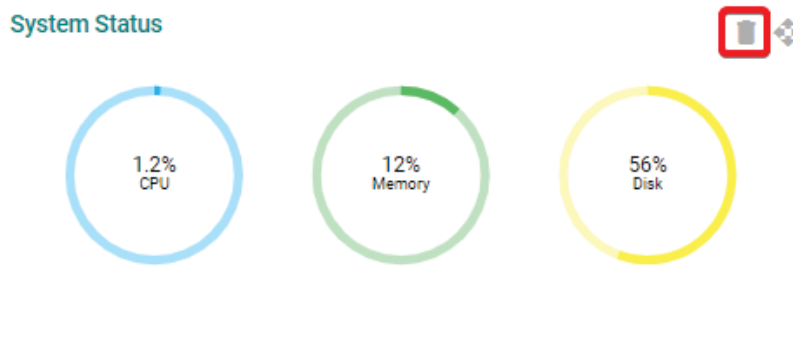
Removing a Widget from the Dashboard


Steps:

1. Click the  icon to edit the dashboard.




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

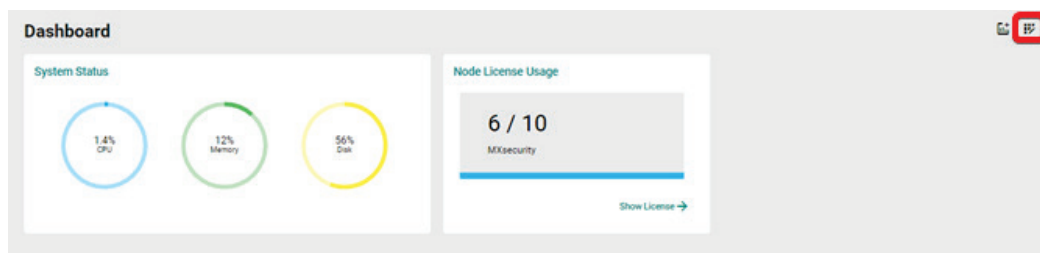


3. Click the  icon again to save your changes and leave edit mode.

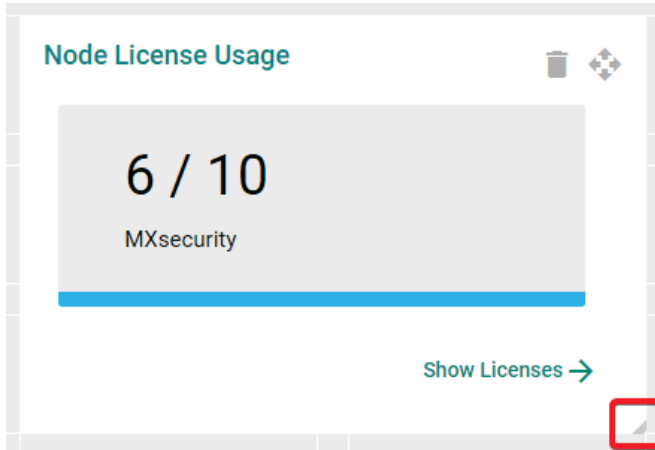
Resizing a Widget


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.

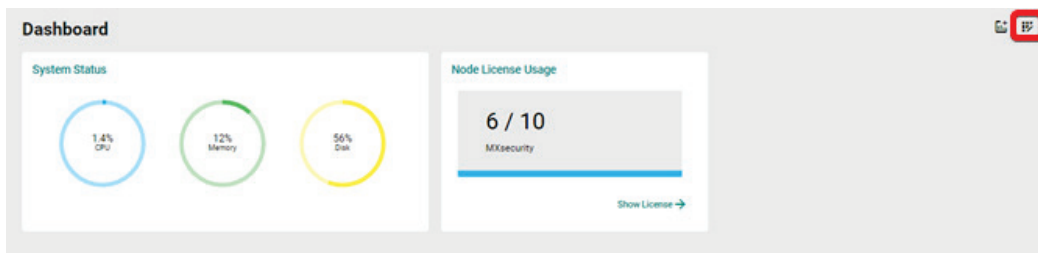



3. Click and drag the corner of the widget to the desired size, then release the mouse. The dark grey area in the Dashboard background indicates the final size of the widget.
4. Click the  icon again to save your changes and leave edit mode.

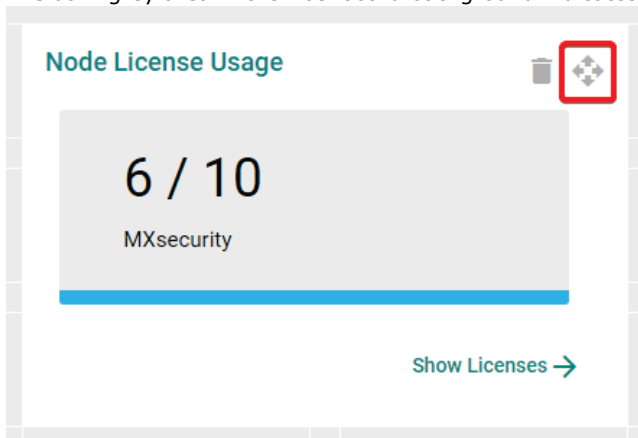
Moving the Widget Position


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 the 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.

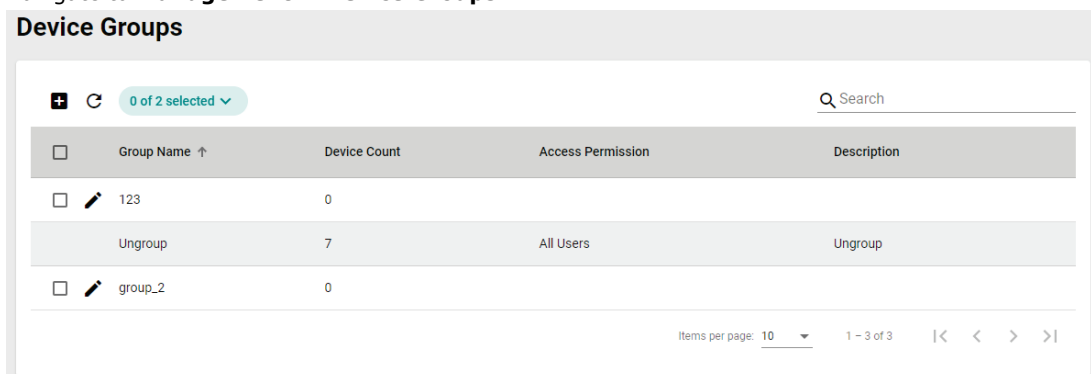
The configurations and policies that can be shared are:


- 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 (_).

Create Group

1 Enter Group Information — 2 Add Devices — 3 Grant Access Permission

Group Name *  0 / 32

Description 0 / 255

[CANCEL](#) [NEXT](#)

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

Create Group

1 Enter Group Information — 2 Add Devices — 3 Grant Access Permission

0 of 6 Selected Search

<input type="checkbox"/>	Host Name ↑	Status	Location	Model Name	Serial Number	MAC	Firmware Version	Group
<input type="checkbox"/>	Firewall/VPN Router 00000	●	Device Location	EDR-G9010-VPN-2MGSFP	MOXA00000000	00:33:11:22:33:44	V2.0	Ungroup
<input type="checkbox"/>	device_1	●	location_1	EDR-G9010-VPN-2MGSFP	1	00:00:00:00:00:01	V1.0	Ungroup
<input type="checkbox"/>	device_2	●	location_2	EDR-G9010-VPN-2MGSFP	2	00:00:00:00:00:02	V1.0	Ungroup
<input type="checkbox"/>	device_3	●	location_3	EDR-G9010-VPN-2MGSFP	3	00:00:00:00:00:03	V1.0	Ungroup
<input type="checkbox"/>	device_4	●	location_4	EDR-G9010-VPN-2MGSFP	4	00:00:00:00:00:04	V1.0	Ungroup
<input type="checkbox"/>	xxx	●	aaa	EDR-G9010-VPN-2MGSFP-T	MOXA00000000	00:01:02:03:04:05	V2.0	Ungroup

Items per page: 10 1 - 6 of 6 |< < > >|

[BACK](#) [NEXT](#)

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

Create Group

1 Enter Group Information — 2 Add Devices — 3 Grant Access Permission

0 of 2 Selected Search


<input type="checkbox"/>	Username ↑	Role	Description
<input type="checkbox"/>	_kk	Viewer	kkk pokjpo opkpk_...--())
<input type="checkbox"/>	super	Admin	root
<input type="checkbox"/>	test	Operator	123

Items per page: 10 1 - 3 of 3 |< < > >|

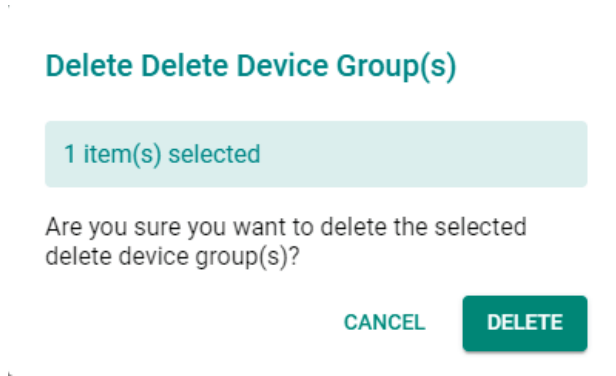
[BACK](#) [APPLY](#)

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).

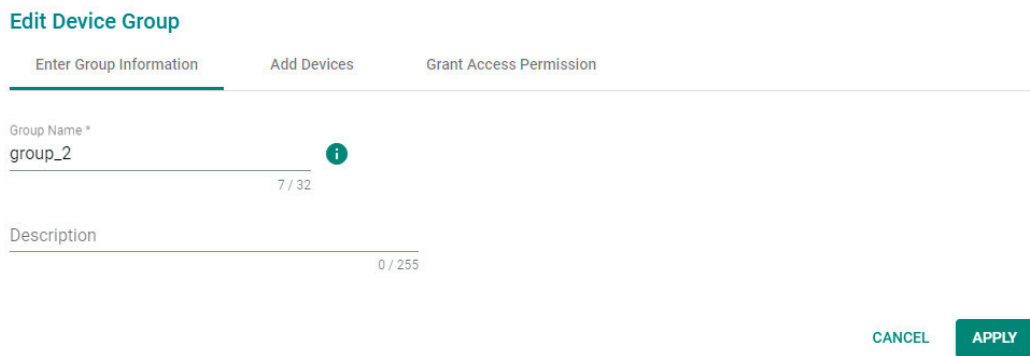
- When prompted to confirm, click **DELETE**.



Editing a Device Group

Steps:

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



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


Firmware Management

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



Uploading a New Firmware




Steps:

- Navigate to **Management > Firmwares**.

2. Click the  icon to add a new firmware.

Firmwares

  0 of 3 selected 🔍 Search

<input type="checkbox"/>	Model Series ↑	Version	Build Time	Description	Schedule In Use
<input type="checkbox"/>	 EDR-G9010	V2.1	2021-05-19 16:00:00		Yes
<input type="checkbox"/>	 EDR-G9010	V3.1	2021-05-19 16:00:00		Yes
<input type="checkbox"/>	 OnCell G4302	V1.1	2021-05-19 16:00:00		

Items per page: 10 1 - 3 of 3 |< < > >|



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.

Upload Firmware

Description 0 / 255

Upload a firmware file (.rom)


 Drag and drop a file here, or [browse](#).

CANCEL UPLOAD

4. Click **UPLOAD**.

Deleting a 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**.

Delete Firmware(s)

1 item(s) selected

Are you sure you want to delete the selected firmware(s)?


CANCEL

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 local software package database from MXsecurity.

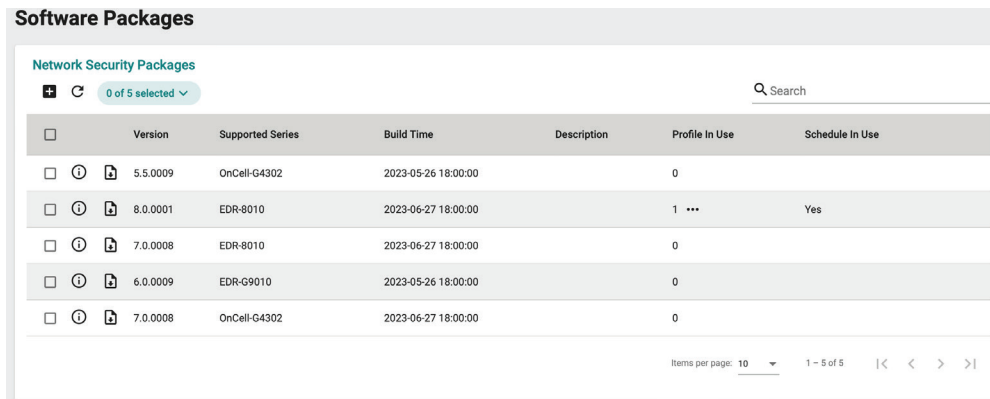
The following packages can be managed in MXsecurity:

- Network Security Package

Uploading a New Software Package

Steps:

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



The screenshot shows the 'Software Packages' management interface. At the top, there is a search bar and a selection indicator showing '0 of 5 selected'. Below this is a table with the following columns: Version, Supported Series, Build Time, Description, Profile In Use, and Schedule In Use. The table contains five rows of data, each with a checkbox and a download icon in the first column.

<input type="checkbox"/>	Version	Supported Series	Build Time	Description	Profile In Use	Schedule In Use
<input type="checkbox"/>	5.5.0009	OnCell-G4302	2023-05-26 18:00:00		0	
<input type="checkbox"/>	8.0.0001	EDR-8010	2023-06-27 18:00:00		1 ...	Yes
<input type="checkbox"/>	7.0.0008	EDR-8010	2023-06-27 18:00:00		0	
<input type="checkbox"/>	6.0.0009	EDR-G9010	2023-05-26 18:00:00		0	
<input type="checkbox"/>	7.0.0008	OnCell-G4302	2023-06-27 18:00:00		0	

At the bottom of the table, there is a pagination control showing 'Items per page: 10' and '1 - 5 of 5'.



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.

Upload Package

Description 0 / 255

Upload a package file (.pkg)


 Drag and drop a file here, or [browse](#).

CANCEL UPLOAD

4. Click **UPLOAD**.

Deleting a Software Package

Steps:

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

Delete Software Package(s)

1 item(s) selected

Are you sure you want to delete the selected software package(s)?


CANCEL

DELETE

Exporting Software Packages

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

Steps:


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

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

Software Packages

Network Security Packages

0 of 6 selected

Search

<input type="checkbox"/>	Version	Supported Series	Build Time	Description	Profile In Use	Schedule In Use
<input type="checkbox"/>	5.5.0007	OnCell-G4302	2023-04-12 02:00:00		0	Yes
<input type="checkbox"/>	5.5.0012	OnCell-G4302	2023-06-28 02:00:00		0	
<input type="checkbox"/>	6.0.0012	EDR-G9010	2023-06-09 02:00:00		1 ...	Yes
<input type="checkbox"/>	6.0.0013	EDR-G9010	2023-06-28 02:00:00		0	
Supported Functions: Modbus/TCP, DNP3, IEC-104, MMS, IPS						
<input type="checkbox"/>	7.0.0001	EDR-8010	2023-04-22 02:00:00		0	
<input type="checkbox"/>	6.0.0006	EDR-8010	2023-04-27 02:00:00		0	Yes

Items per page: 10 | 1 - 6 of 6 | < > >>



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.

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.

- Click the  icon to create a new object.

Objects

Filter | Interface

 0 of 13 selected Q Search

<input type="checkbox"/>	Object Name ↑	Type	Details	References
<input type="checkbox"/>	44	IP Address and Subnet	192.168.127.1	0
<input type="checkbox"/>	123	IP Address and Subnet	192.168.1.0	0
<input type="checkbox"/>	02	IP Address and Subnet	1.1.1.1	0
<input type="checkbox"/>	03	IP Address and Subnet	2.2.2.2	0
<input type="checkbox"/>	04	User-defined Service	TCP 3	1 ...

- Enter a name for the object.

Create Object

Object Name * i
0 / 32

Object Type * v

CANCEL CREATE

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

Create Object

Object Name * i
0 / 32

Object Type * v

IP Address & Subnet

Network Service

Industrial Application Service


User-defined Service

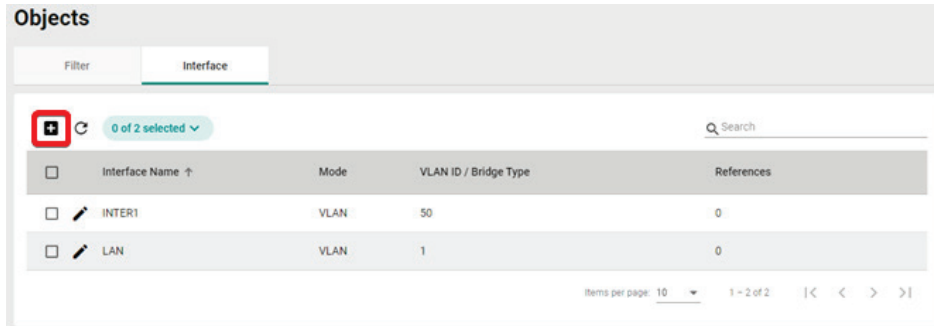
CANCEL CREATE

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

Create Interface

Interface Name 0 / 32 ⓘ

Mode

VLAN Bridge

VLAN *


1 ~ 4094

CANCEL APPLY

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**.

Delete Interface(s)

2 item(s) selected

Are you sure you want to delete the selected interface(s)?

CANCEL

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**.

- Click the  icon to create a policy profile.

Policy Profiles

0 of 11 selected Search

<input type="checkbox"/>	Profile Name ↑	Description	Device In Use	Schedule In Use
<input type="checkbox"/>	 Dos		0	
<input type="checkbox"/>	 Dos2		0	
<input type="checkbox"/>	 abcd		1 ...	Yes
<input type="checkbox"/>	 br-test		0	
<input type="checkbox"/>	 fsafdfad		4 ...	Yes
<input type="checkbox"/>	 ips		0	
<input type="checkbox"/>	 test321	123321	0	
<input type="checkbox"/>	 testprofile2222		0	
<input type="checkbox"/>	 testseste		0	
<input type="checkbox"/>	 testsesterfdrd		0	

Items per page: 10 1 - 10 of 11 |< < > >|



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.

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


Layer 3 - 7 ^

Policy Global Setting		Policy Event Global Setting	
Enforcement	Default Action	Log	
Disabled	Deny All	Enabled	

0 of 0 Selected Search

<input type="checkbox"/>	Index	Enforce	Policy Name	Event	Incoming Interface	Outgoing Interface	Filter Mode	Source Address	Source Port	Destination Address	Destination Port or Protocol	Action	Description
--------------------------	-------	---------	-------------	-------	--------------------	--------------------	-------------	----------------	-------------	---------------------	------------------------------	--------	-------------

Items per page: 10 0 of 0 |< < > >|

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

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

Create Layer 3-7 Policy

Index *
1
1 ~ 1024

Status *
Enabled

Name *
0 / 32

Description
0 / 128

Log *
Disabled

Severity *
<4> Warning

Log Destination
Local Storage

Incoming Interface *
Any

Outgoing Interface *
Any

Action *
Allow

Filter Mode *
IP and Port Filtering

Source IP Address *
Any

Source Port *
Any

Destination IP Address *
Any

Destination Port or Protocol *
Any

- 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](#).

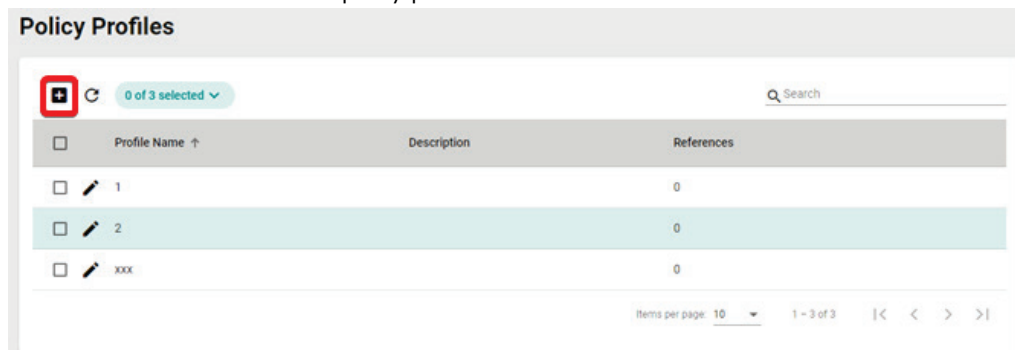
Source MAC Filtering:

- i. Source MAC Address: Specify the source MAC address.
8. Click **CREATE** to create the Layer 3-7 Policy Profile.
9. Click **APPLY**.

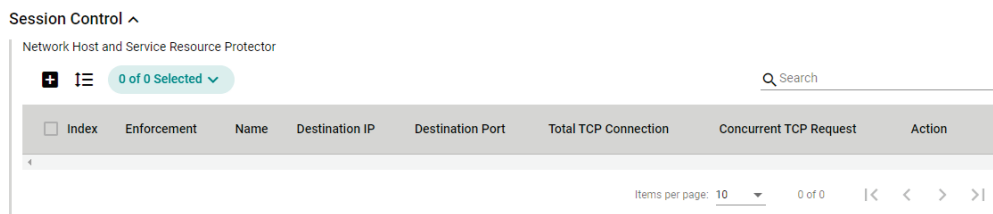
Creating a New Session Control Policy Profile


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:

Create Session Control Policy


Index *
1
1 ~ 1024


Status *
Enabled


Name *
0 / 32


Severity * <4> Warning Log Destination Local Storage

Action *
Drop

TCP Destination * 

IP Address * 

Port * 

TCP Connection Limitation * 


Total TCP Connections 1 ~ 65535 connections Concurrent TCP Reques... 1 ~ 512 connections/s

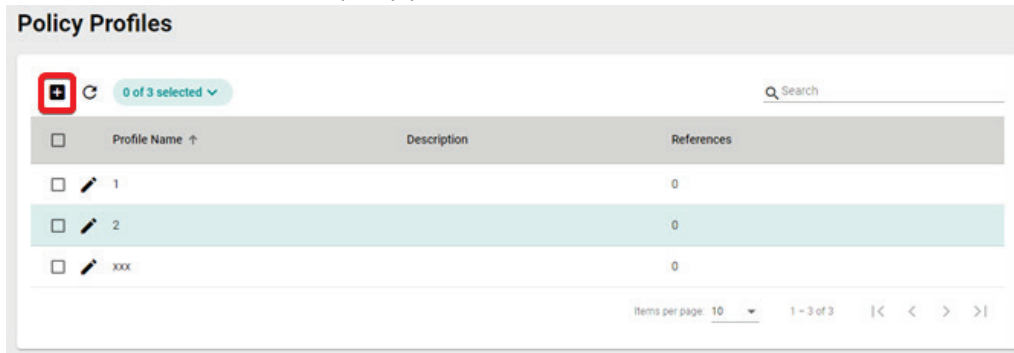
- a. **Index:** Specify the index for the policy profile.
 - b. **Status:** Enable or disable the policy profile.
 - c. **Name:** Enter a description for the policy profile.
 - d. **Severity:** Select the log severity level.
 - e. **Log Destination:** If logging is enabled, choose where the logs will 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**.

- Click the  icon to create a policy profile.




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

DoS ^

DoS Settings

All

Session SYN Protection

TCP-Without-SYN Scan 

Port-Scan Protection **Flood Protection**

Null Scan ICMP-Flood
Limit: 1000
1 - 4000 pkt/s

Xmas Scan

NMAP-Xmas Scan

SYN/FIN Scan SYN-Flood
Limit: 1000
1 - 4000 pkt/s

FIN Scan

NMAP-ID Scan

SYN/RST Scan ARP-Flood
Limit: 1000
1 - 2000 pkt/s

DoS Log Settings


Log * Severity * Log Destination

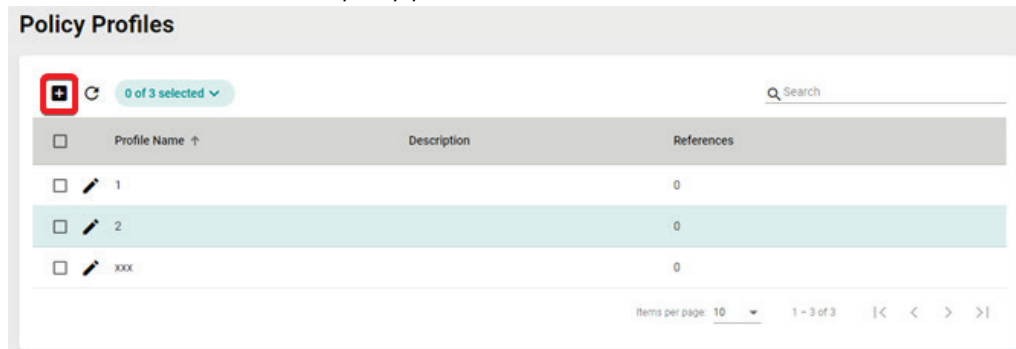
Disabled Emergency [Dropdown]

- 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.
 - Log:** Enable or disable event logs.
 - Severity:** Select the log severity level.
 - Log Destination:** If logging is enabled, choose where the logs will be stored. Multiple options can be selected.
- 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.

IPS ^


Package Version *


 Before configuring any policies, please make sure the Intrusion Prevention System (IPS) function is enabled on the Firewall > Advanced Protection > Configuration screen in the device's web interface.

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).

IPS ^

Package Version *
5.0.0023

 Before configuring any policies, please make sure the Intrusion Prevention System (IPS) function is enabled on the Firewall > Advanced Protection > Configuration screen in the device's web interface.

  1 of 4013 selected

<input type="checkbox"/>	ID	Name	Status	Category	Severity	Action
<input checked="" type="checkbox"/>	4026531840	TCP SYN Flood	Enabled	Flooding & Scan	High	Reset
<input type="checkbox"/>	4026531842	UDP Flood	Enabled	Flooding & Scan	High	Reset
<input type="checkbox"/>	4026531844	ICMP Flood	Enabled	Flooding & Scan	High	Reset
<input type="checkbox"/>	4026531846	IGMP Flood	Enabled	Flooding & Scan	High	Reset

8. Configure the following settings:


Rule Settings

Status
Enabled

Action
Reset


- 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**.

Delete Profile(s)

1 item(s) selected

Are you sure you want to delete the selected profile(s)?

CANCEL


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.

EDR-G9010-VPN-2MGSFP ^

<input type="checkbox"/>	Configure Name ↑	Last Modified Time	Description	Schedule In Use
<input type="checkbox"/>	 20230101_configure	2023-07-15 18:24:15	First version of PoC	Yes
<input type="checkbox"/>	 20230201_configure	2023-07-15 18:22:52		
<input type="checkbox"/>	 20230301_configure	2023-07-15 18:23:30	Network setting ok	

1 - 3 of 3

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

The screenshot shows a form titled "Upload Device Configuration File" with two steps. Step 1, "Enter Configuration File Information", is active. It includes a "Configuration Model" dropdown set to "EDR-G9010-VPN-2MGSFP", a "Configure Name" field with the value "20230601_configure" (18 / 50 characters), and a "Description" field with the value "PoC complete" (12 / 255 characters). Step 2, "Select Configuration File", is inactive. At the bottom right, there are "CANCEL" and "NEXT" buttons.


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.

The screenshot shows the same form, now at step 2, "Select Configuration File". Step 1 is completed. The "Upload Configuration Method" dropdown is set to "Upload Configuration from Local". Below it is a dashed box for "Upload Configuration File (.ini)" with the instruction "Drag and drop a file here, or browse.". At the bottom right, there are "BACK" and "APPLY" buttons.


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.

EDR-G9010-VPN-2MGSFP ^

 0 of 3 selected

Search

<input type="checkbox"/>	Configure Name ↑	Last Modified Time	Description	Schedule In Use
<input type="checkbox"/>	 20230101_configure	2023-07-15 18:24:15	First version of PoC	Yes
<input type="checkbox"/>	 20230201_configure	2023-07-15 18:22:52		
<input type="checkbox"/>	 20230301_configure	2023-07-15 18:23:30	Network setting ok	

1 - 3 of 3

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

Upload Device Configuration File

1 Enter Configuration File Information 2 Select Configuration File

Configuration Model
EDR-G9010-VPN-2MGSFP

Configure Name *
20230601_configure 18 / 50

Description
PoC complete 12 / 255

CANCEL **NEXT**

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.

Upload Device Configuration File

1 Enter Configuration File Information 2 Select Configuration File

Upload Configuration Method *
Upload Configuration from Device

Search

	Device Name ↑	Status	Location	Product Model	Serial Number	MAC Address	Firmware Version	Group
<input type="checkbox"/>	Firewall/VPN Router 55160	●	Device Location	EDR-G9010-VPN- 2MGSFP-T	TBZKB1155160	00:90:E8:91:86:7D	V3.0.0	Ungroup
<input checked="" type="checkbox"/>	Firewall/VPN Router 77777	●	Device Location	EDR-G9010-VPN- 2MGSFP	MOXA77777777	00:01:02:03:04:77	V3.0.0	Ungroup
<input type="checkbox"/>	Firewall/VPN Router Hades	●	Device Location	EDR-G9010-VPN- 2MGSFP-T	MOXA95275487	00:01:02:03:04:05	V3.0.0	Ungroup
<input type="checkbox"/>	OOOwen 9010	●	122, 25	EDR-G9010-VPN- 2MGSFP-T	MOXA00112233	00:90:E8:90:10:06	V3.0.0	Ungroup
<input type="checkbox"/>	device_1	●	120.0, 20.5	EDR-G9010-VPN- 2MGSFP	TEST-DEV-1	90:10:00:00:00:01	V1.0.0	Ungroup
<input type="checkbox"/>	device_2	●	125.0, 25.5	EDR-G9010-VPN- 2MGSFP	TEST-DEV-2	90:10:00:00:00:02	V1.0.0	Ungroup

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).

Device Deployment

General | Policy Profiles | Software Packages | Firmware | Device Configuration

0 group(s) selected | 1 device(s) selected

Device Name	Status	Location	Product Model	Serial Number	MAC	Firmware Version	Scheduling Reboot	Last Reboot Time
Ungroup								
<input type="checkbox"/> OnCellCellularRouter999	●	120.25, 25.35	OnCell-G4302-LTE4-EU	MOXA60004302	60:60:60:43:02	V2.5.0		
<input type="checkbox"/> Owen 4302	●	00000wenn1	OnCell-G4302-LTE4-EU	MOXA00000000	10:71:98:43:02:01	V3.0.0		
<input type="checkbox"/> device_4	●	location_4	OnCell G4302-LTE4-AU	TEST-DEV-4	43:00:00:00:00:04	V1.0.0	Weekly Mon. Tue. 07:55	Manually 2023-04-26 17:37:05
<input type="checkbox"/> Firewall/VPN Router 55160	●	Device Location	EDR-G9010-VPN-2MGSFP-T	TBZKB1155160	00:90:E8:91:86:7D	V3.0.0		Schedule 2023-05-11 04:00:25
<input type="checkbox"/> 000wen 9010	●	122, 25	EDR-G9010-VPN-2MGSFP-T	MOXA00112233	00:90:E8:90:10:06	V3.0.0		Schedule 2023-07-12 16:10:24
<input checked="" type="checkbox"/> device_3	●	location_3	EDR-G9010-VPN-2MGSFP-T	TEST-DEV-3	90:10:00:00:00:03	V1.0.0	One Time 2023-07-12 16:10	Manually 2023-07-12 16:10:24
<input type="checkbox"/> Firewall/VPN Router Hades	●	Device Location	EDR-G9010-VPN-2MGSFP-T	MOXA95275487	00:01:02:03:04:05	V3.0.0		

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

Reboot Device(s)

1 item(s) selected

Are you sure you want to reboot the selected device(s)?


CANCEL

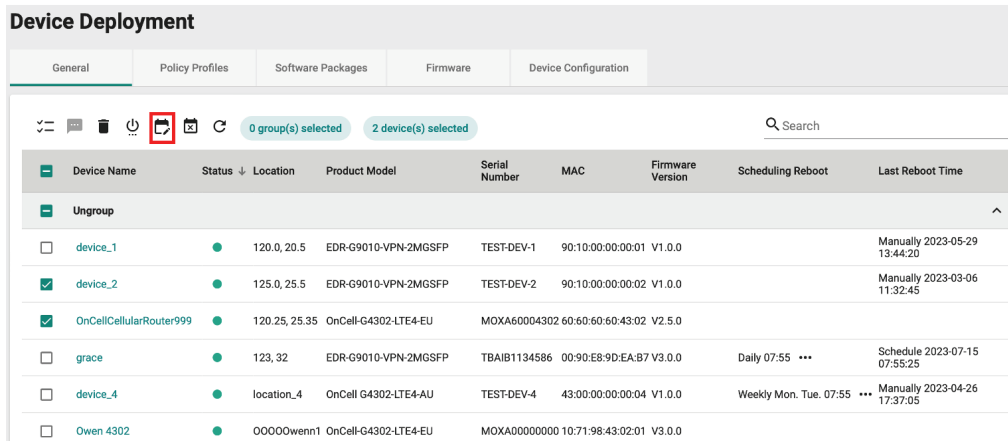
REBOOT

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:

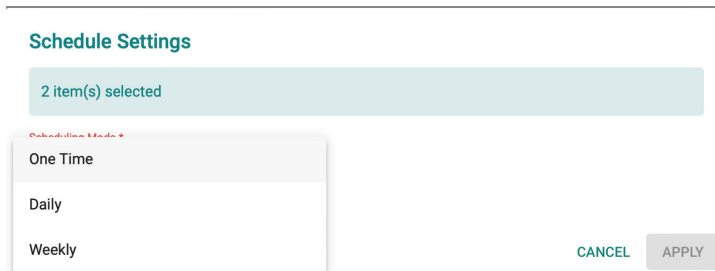
1. Navigate to **Device Deployment > General**.
2. Check the box of the device(s) you want to reboot.
3. Click the  icon to configure a reboot schedule for the selected device(s).



The screenshot shows the 'Device Deployment' interface with the 'General' tab selected. A table lists several devices. The 'Scheduling Reboot' column shows various schedules. A red box highlights the reboot icon in the top toolbar.

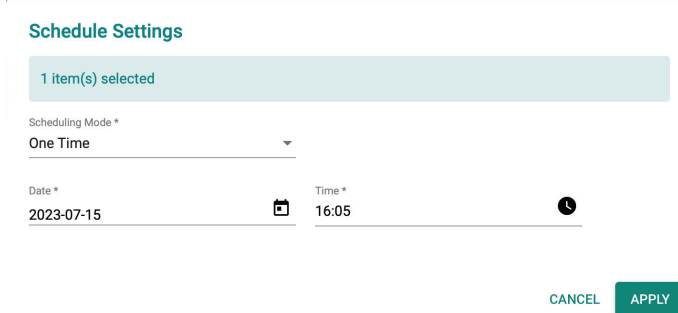
Device Name	Status	Location	Product Model	Serial Number	MAC	Firmware Version	Scheduling Reboot	Last Reboot Time
device_1	●	120.0, 20.5	EDR-G9010-VPN-2MGSFP	TEST-DEV-1	90:10:00:00:00:01	V1.0.0		Manually 2023-05-29 13:44:20
device_2	●	125.0, 25.5	EDR-G9010-VPN-2MGSFP	TEST-DEV-2	90:10:00:00:00:02	V1.0.0		Manually 2023-03-06 11:32:45
OnCellCellularRouter999	●	120.25, 25.35	OnCell-G4302-LTE4-EU	MOXA60004302	60:60:60:60:43:02	V2.5.0		
grace	●	123, 32	EDR-G9010-VPN-2MGSFP	TBAIB1134586	00:90:E8-9D:EA:B7	V3.0.0	Daily 07:55 ...	Schedule 2023-07-15 07:55:25
device_4	●	location_4	OnCell G4302-LTE4-AU	TEST-DEV-4	43:00:00:00:00:04	V1.0.0	Weekly Mon, Tue, 07:55 ...	Manually 2023-04-26 17:37:05
Owen 4302	●	00000wenn1	OnCell-G4302-LTE4-EU	MOXA00000000	10:71:98:43:02:01	V3.0.0		

4. Select a scheduling mode:



The screenshot shows the 'Schedule Settings' dialog box with '2 item(s) selected'. The 'Scheduling Mode' dropdown menu is open, showing options: One Time, Daily, and Weekly. 'CANCEL' and 'APPLY' buttons are visible at the bottom right.

- 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.



The screenshot shows the 'Schedule Settings' dialog box with '1 item(s) selected'. The 'Scheduling Mode' is set to 'One Time'. The 'Date' is set to '2023-07-15' and the 'Time' is set to '16:05'. 'CANCEL' and 'APPLY' buttons are visible at the bottom right.

- 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.

Schedule Settings

1 item(s) selected

Scheduling Mode *
Daily

Time *
05:00

Period *
2023-07-15 – 2023-10-13

CANCEL APPLY

- 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.

Schedule Settings

1 item(s) selected

Scheduling Mode *
Weekly

Weekly Day *
Mon. Wed. Fri.

Time *
05:00


Period *
2023-07-15 – 2023-10-13

CANCEL APPLY

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**.

Delete Scheduling

2 item(s) selected

Are you sure you want to delete the selected scheduling?

CANCEL DELETE

Sending a Control SMS

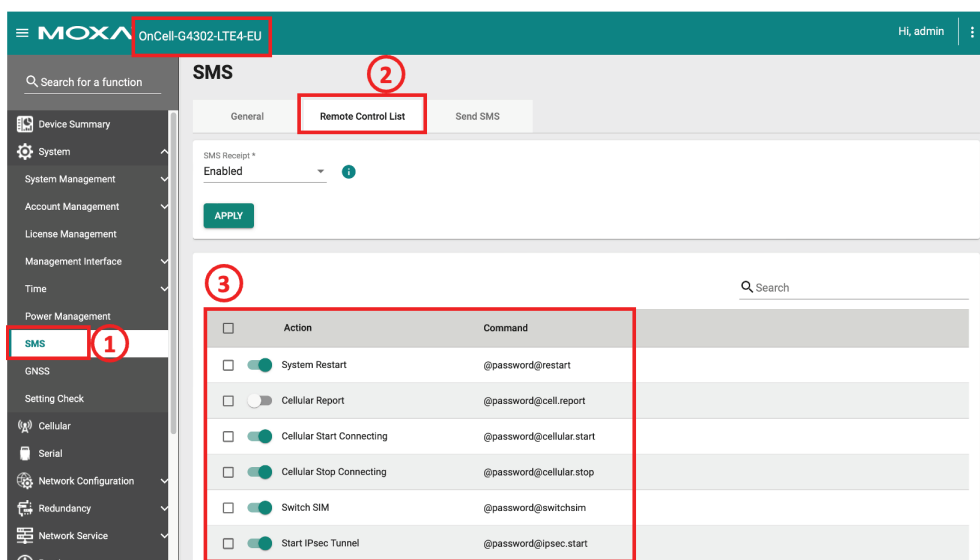
The OnCell Series routers may be installed in areas outside the range of the base station coverage. If a connection can be established, the signal may be extremely weak, leading to interruptions for applications. It also makes it challenging for users to restore the device's external network connection via the web console or SSH.


However, if the cellular router's SIM card can receive SMS messages, MXsecurity can remotely control the cellular router by sending SMS commands. Refer to the table below for an overview of available SMS commands.

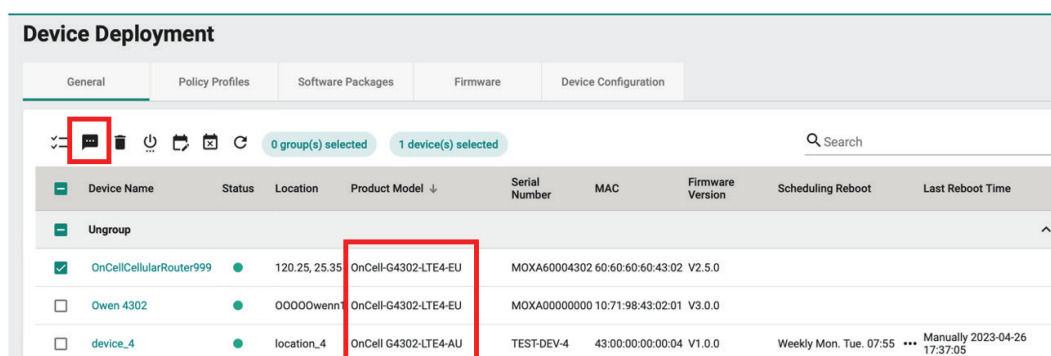
Command	Description
System Restart	The device will reboot.
Cellular Start Connecting	The device will enable the cellular data connection.
Cellular Stop Connecting	The device will disable the cellular data connection.
Start IPsec Tunnel	The device will establish the IPsec tunnel.
Stop IPsec Tunnel	The device will disconnect the IPsec tunnel.
Set DO On	The device will turn the status of the relay output to On.
Set DO Off	The device will turn the status of the relay output to Off.
Switch SIM	The device will restart the cellular module and switch to the SIM card installed in the other SIM slot.

Steps:

1. Enable remote control functions on the OnCell secure router:
 - a. Log in to the OnCell secure router's web console.
 - b. Navigate to **System > SMS > Remote Control List**.
 - c. Enable the function(s) that you want to remotely control by SMS through MXsecurity. For security reasons, all functions are disabled by default.



2. In MXsecurity, navigate to **Device Deployment > General**.
3. Check the box of an OnCell secure router.
4. Click the  icon to send a control SMS.



5. Select the SMS command you want to execute.
6. Click **Send**.



NOTE

There is a one-minute wait timer between each SMS message. Once the wait timer expires runs out, another SMS message can be sent.



NOTE

MXsecurity can send a maximum of 200 SMS control messages per device each month. A counter in the top-right of Remote SMS Control page shows the number of sent messages.


Removing a Managed Device

Steps:

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

The screenshot shows the 'Device Deployment' interface with the 'General' tab selected. At the top, there are four tabs: 'General', 'Policy Profiles', 'Software Packages', and 'Firmware'. Below the tabs, there are several icons: a filter icon, a trash can icon (highlighted with a red box), a power icon, and a refresh icon. To the right of these icons, there are two status indicators: '0 group(s) selected' and '2 device(s) selected'. Below this is a table with the following columns: Host Name, Status, Location, and Model Name. The table contains three rows of data, with the first two rows having their checkboxes checked.

Host Name	Status	Location	Model Name
device_1	●	location_1	ONCELL-G4300-OWEN-ABC
device_1	●	location_1	EDR-G9010-VPN-2MGSFP
device_2	●	location_2	ONCELL-G4300-OWEN-ABC

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

Delete Device(s)

1 item(s) selected

Are you sure you want to delete the selected device(s)?

CANCEL

DELETE


Deploying Policy Profiles to Managed Devices

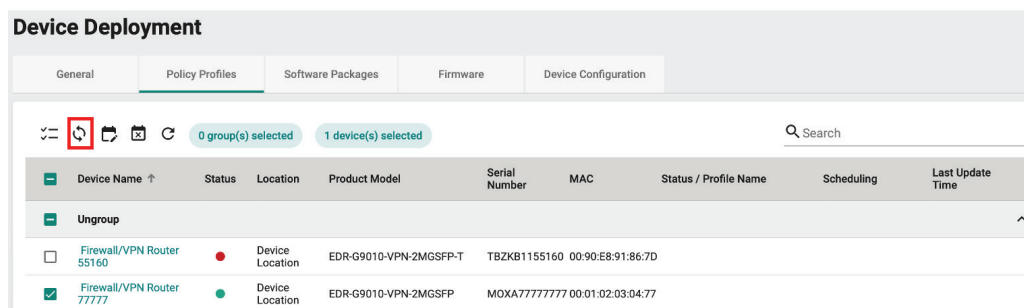
You can deploy specific policy profiles to managed devices and check the synchronization status between the device and MXsecurity.

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).

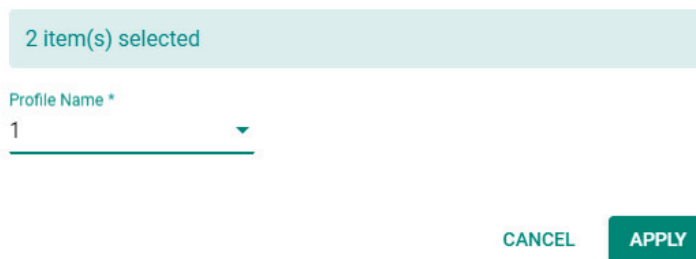


The screenshot shows the 'Device Deployment' interface with the 'Policy Profiles' tab selected. A table lists two devices, both of which are selected with checkboxes. The table columns are: Device Name, Status, Location, Product Model, Serial Number, MAC, Status / Profile Name, Scheduling, and Last Update Time.

Device Name	Status	Location	Product Model	Serial Number	MAC	Status / Profile Name	Scheduling	Last Update Time
Firewall/VPN Router 55160	Not Sync	Device Location	EDR-G9010-VPN-2MGSFP-T	TBZKB1155160	00:90:E8:91:86:7D			
Firewall/VPN Router 77777	Sync	Device Location	EDR-G9010-VPN-2MGSFP	MOXA77777777	00:01:02:03:04:77			

4. Select a previously configured policy profile.
Refer to [Policy Profile Management](#) for instructions on how to create policy profiles.

Sync Profile To Device(s)




The dialog box shows '2 item(s) selected' and a 'Profile Name' dropdown menu with '1' selected. There are 'CANCEL' and 'APPLY' buttons at the bottom.

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).

Device Deployment

General | Policy Profiles | Software Packages | Firmware | Device Configuration

0 group(s) selected | 2 device(s) selected

Device Name	Status	Location	Product Model	Serial Number	MAC	Firmware Version	Scheduling Reboot	Last Reboot Time
Ungroup								
<input type="checkbox"/> device_1	●	120.0, 20.5	EDR-G9010-VPN-2MGSFP	TEST-DEV-1	90:10:00:00:00:01	V1.0.0		Manually 2023-05-29 13:44:20
<input checked="" type="checkbox"/> device_2	●	125.0, 25.5	EDR-G9010-VPN-2MGSFP	TEST-DEV-2	90:10:00:00:00:02	V1.0.0		Manually 2023-03-06 11:32:45
<input checked="" type="checkbox"/> OnCellCellularRouter999	●	120.25, 25.35	OnCell-G4302-LTE4-EU	MOXA60004302 60:60:60:60:43:02		V2.5.0		
<input type="checkbox"/> grace	●	123, 32	EDR-G9010-VPN-2MGSFP	TBAIB1134586	00:90:E8:9D:EA:B7	V3.0.0	Daily 07:55 ...	Schedule 2023-07-15 07:55:25
<input type="checkbox"/> device_4	●	location_4	OnCell G4302-LTE4-AU	TEST-DEV-4	43:00:00:00:00:04	V1.0.0	Weekly Mon. Tue. 07:55 ...	Manually 2023-04-26 17:37:05
<input type="checkbox"/> Owen 4302	●	00000wenn1	OnCell-G4302-LTE4-EU	MOXA00000000	10:71:98:43:02:01	V3.0.0		

4. Select a scheduling mode:

Schedule Settings

2 item(s) selected

Scheduling Mode *

- One Time
- Daily
- Weekly

CANCEL APPLY

- 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.

Schedule Settings

1 item(s) selected

Scheduling Mode *

One Time

Date * 2023-07-15

Time * 16:05

CANCEL APPLY

- 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.

Schedule Settings

1 item(s) selected

Scheduling Mode *

Daily

Time * 05:00

Period * 2023-07-15 – 2023-10-13

CANCEL APPLY

- 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.

Schedule Settings

1 item(s) selected


Scheduling Mode *	Weekly	Weekly Day *	Mon. Wed. Fri.
Time *	05:00	Period *	2023-07-15 – 2023-10-13

CANCEL APPLY

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**.

Delete Scheduling

2 item(s) selected

Are you sure you want to delete the selected scheduling?

CANCEL DELETE

Upgrading the Software Package of Managed Devices


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

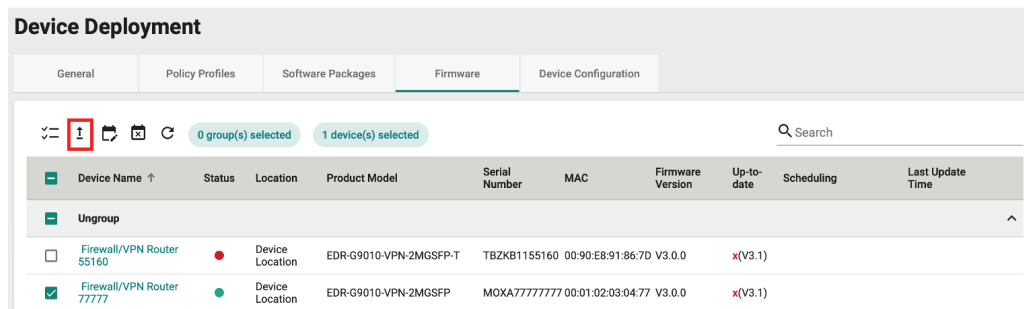
You can check the following software package information:

- **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.

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



Device Deployment

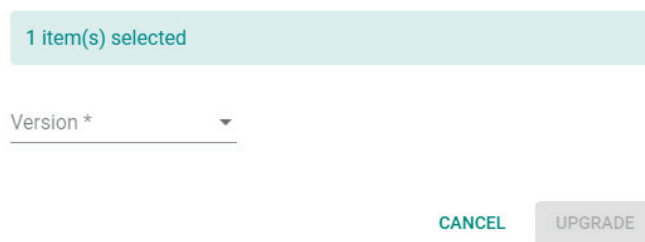
General Policy Profiles Software Packages **Firmware** Device Configuration

0 group(s) selected 1 device(s) selected

Device Name ↑	Status	Location	Product Model	Serial Number	MAC	Firmware Version	Up-to-date	Scheduling	Last Update Time
Ungroup									
<input type="checkbox"/> Firewall/VPN Router 55160	●	Device Location	EDR-G9010-VPN-2MGSFP-T	TBZKB1155160	00:90:E8:91:86:7D	V3.0.0	x(V3.1)		
<input checked="" type="checkbox"/> Firewall/VPN Router 7777	●	Device Location	EDR-G9010-VPN-2MGSFP	MOXA77777777	00:01:02:03:04:77	V3.0.0	x(V3.1)		

- Select a previously uploaded software package to upgrade to. Refer to [Software Package Management](#) for instructions on how to upload software packages.

Upgrade Package



1 item(s) selected

Version *

CANCEL UPGRADE


- Click **UPGRADE**.

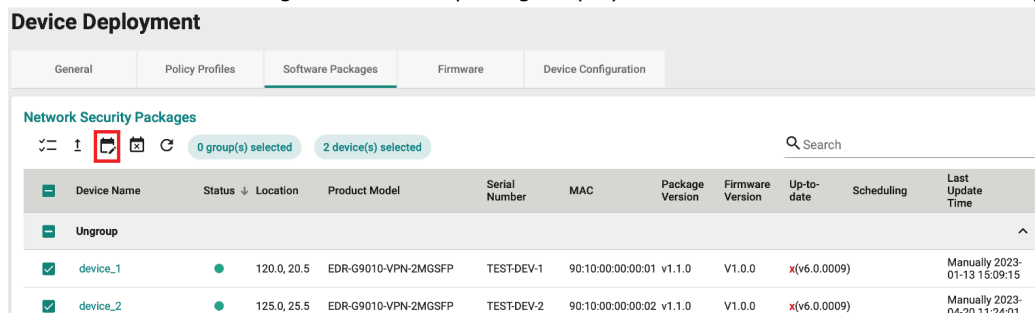
Scheduling a Software Package Deployment for Managed Devices

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:

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



Device Deployment

General Policy Profiles **Software Packages** Firmware Device Configuration

Network Security Packages

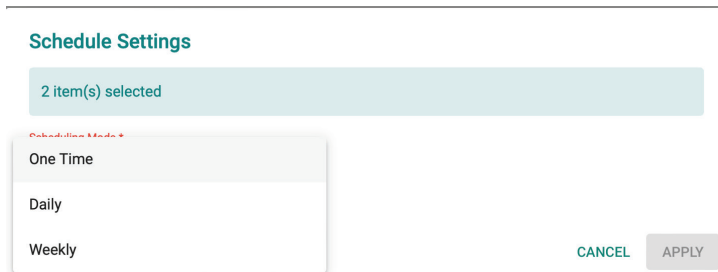
0 group(s) selected 2 device(s) selected

Device Name	Status ↓	Location	Product Model	Serial Number	MAC	Package Version	Firmware Version	Up-to-date	Scheduling	Last Update Time
Ungroup										
<input checked="" type="checkbox"/> device_1	●	120.0, 20.5	EDR-G9010-VPN-2MGSFP	TEST-DEV-1	90:10:00:00:00:01	v1.1.0	V1.0.0	x(v6.0.0009)		Manually 2023-01-13 15:09:15
<input checked="" type="checkbox"/> device_2	●	125.0, 25.5	EDR-G9010-VPN-2MGSFP	TEST-DEV-2	90:10:00:00:00:02	v1.1.0	V1.0.0	x(v6.0.0009)		Manually 2023-04-20 11:24:01

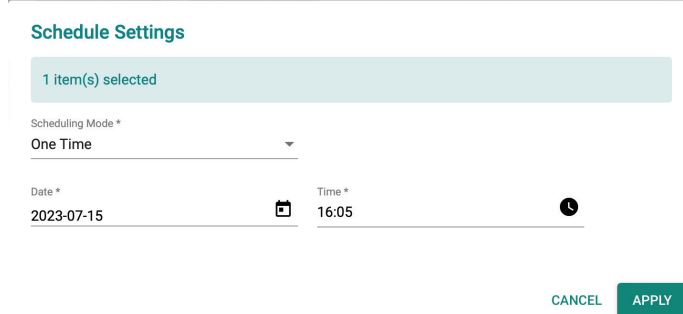
- Select the software package version to deploy. If you select **Up-to-date**, MXsecurity will deploy the latest version of the software package available in

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.

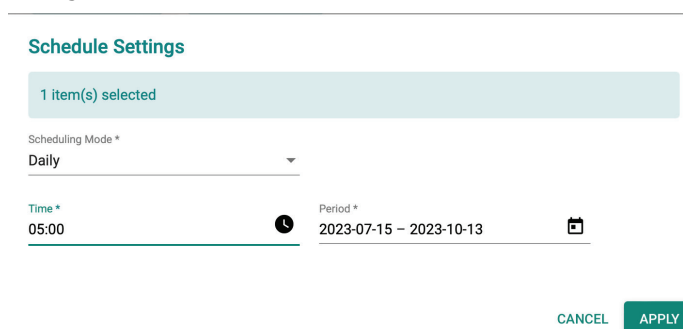
5. Select a scheduling mode:



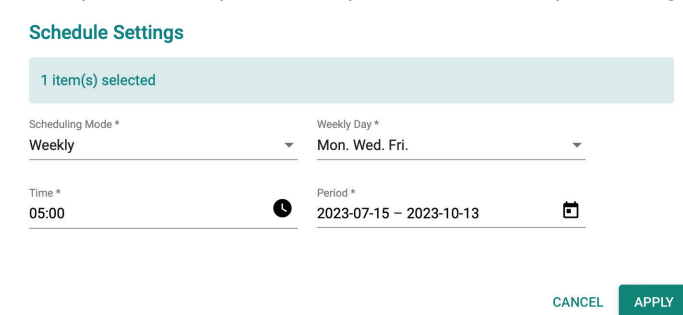
- a. **One Time:** Select the date and time the device(s) will reboot. One-time schedules can be configured for up to 30 days in the future. The reboot time should be set in 5-minute increments, for example 16:05.



- 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**.

Delete Scheduling

2 item(s) selected

Are you sure you want to delete the selected scheduling?

CANCEL

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).

Device Deployment										
General		Policy Profiles		Software Packages		Firmware		Device Configuration		
Device Name ↑	Status	Location	Product Model	Serial Number	MAC	Firmware Version	Up-to-date	Scheduling	Last Update Time	
Ungroup										
<input type="checkbox"/>	Firewall/VPN Router 55160	● Device Location	EDR-G9010-VPN-2MGSFP-T	TBZKB1155160	00:90:E8:91:86:7D	V3.0.0	x(V3.1)			
<input checked="" type="checkbox"/>	Firewall/VPN Router 77777	● Device Location	EDR-G9010-VPN-2MGSFP	MOXA77777777	00:01:02:03:04:77	V3.0.0	x(V3.1)			

- Select a previously uploaded firmware to upgrade to.
Refer to [Firmware Management](#) for instructions on how to upload firmware.

Upgrade Firmware

2 item(s) selected

Version
No version available ▾

Check the firmware files on the Management/Firmware page.

CANCEL UPGRADE

- 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:

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

Device Deployment

General Policy Profiles Software Packages **Firmware** Device Configuration

0 group(s) selected 1 device(s) selected

Device Name ↑	Status	Location	Product Model	Serial Number	MAC	Firmware Version	Up-to-date	Scheduling	Last Update Time
Ungroup									
<input type="checkbox"/> Firewall/VPN Router 55160	●	Device Location	EDR-G9010-VPN-2MGSPF-T	TBZKB1155160	00:90:E8:91:86:7D	V3.0.0	x(V3.1)		
<input checked="" type="checkbox"/> Firewall/VPN Router 77777	●	Device Location	EDR-G9010-VPN-2MGSPF	MOXA77777777	00:01:02:03:04:77	V3.0.0	x(V3.1)		

- 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.
- Select a scheduling mode:

Schedule Settings

2 item(s) selected

Scheduling Mode ▾

One Time

Daily

Weekly

CANCEL APPLY

- 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.

Schedule Settings

1 item(s) selected

Scheduling Mode *
One Time

Date * 2023-07-15 Time * 16:05

CANCEL APPLY

- 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.

Schedule Settings

1 item(s) selected

Scheduling Mode *
Daily

Time * 05:00 Period * 2023-07-15 – 2023-10-13

CANCEL APPLY

- 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.

Schedule Settings

1 item(s) selected

Scheduling Mode * Weekly Weekly Day * Mon. Wed. Fri.


Time * 05:00 Period * 2023-07-15 – 2023-10-13

CANCEL APPLY

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.

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

Delete Scheduling

2 item(s) selected

Are you sure you want to delete the selected scheduling?


CANCEL

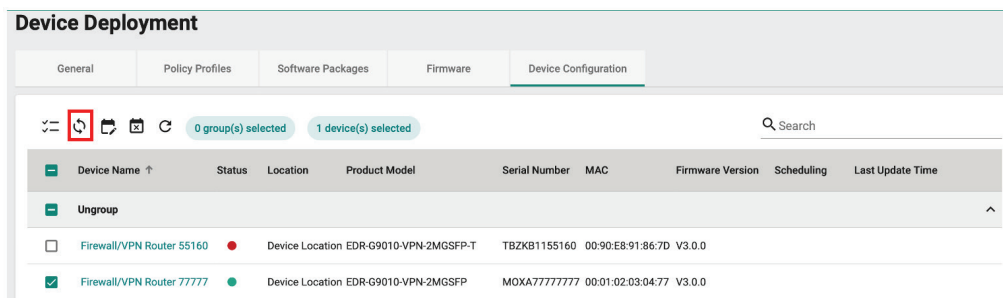
DELETE

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:

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



The screenshot shows the 'Device Deployment' interface with the 'Device Configuration' tab selected. A table lists devices with columns for Device Name, Status, Location, Product Model, Serial Number, MAC, Firmware Version, Scheduling, and Last Update Time. One device, 'Firewall/VPN Router 77777', is selected. The interface also shows '0 group(s) selected' and '1 device(s) selected'.

Device Name	Status	Location	Product Model	Serial Number	MAC	Firmware Version	Scheduling	Last Update Time
Ungroup								
<input type="checkbox"/> Firewall/VPN Router 55160	●	Device Location EDR-G9010-VPN-2MGSFP-T		TBZKB1155160	00:90:E8:91:86:7D	V3.0.0		
<input checked="" type="checkbox"/> Firewall/VPN Router 77777	●	Device Location EDR-G9010-VPN-2MGSFP		MOXA77777777	00:01:02:03:04:77	V3.0.0		

- Select a previously uploaded device configuration to deploy. Refer to [Device Configuration Management](#) for instructions on how to upload a configuration.

Sync Configuration To Device(s)

1 item(s) selected

Select Configuration File *

20230101_configure

CANCEL


APPLY

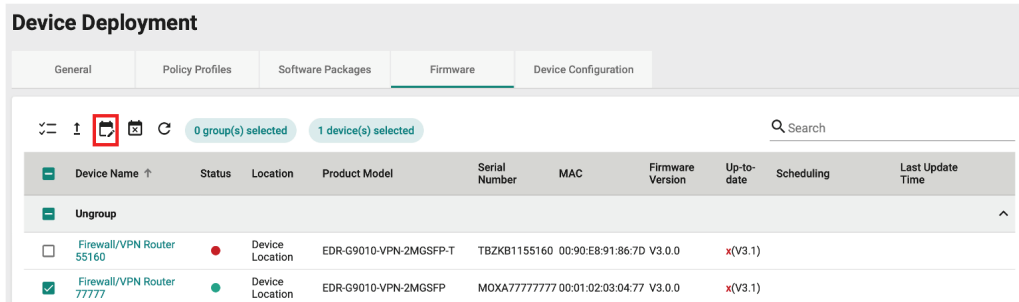
- Click **APPLY**.

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 execute 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).



Device Deployment

General | Policy Profiles | Software Packages | **Firmware** | Device Configuration

0 group(s) selected | 1 device(s) selected

Device Name ↑	Status	Location	Product Model	Serial Number	MAC	Firmware Version	Up-to-date	Scheduling	Last Update Time
Ungroup									
<input type="checkbox"/> Firewall/VPN Router 55160	●	Device Location	EDR-G9010-VPN-2MGSPF-T	TBZKB1155160	00:90:E8:91:86:7D	V3.0.0	x(V3.1)		
<input checked="" type="checkbox"/> Firewall/VPN Router 77777	●	Device Location	EDR-G9010-VPN-2MGSPF	MOXA77777777	00:01:02:03:04:77	V3.0.0	x(V3.1)		

4. Select a previously uploaded configuration file to deploy.



Schedule Settings

1 item(s) selected

Select File *
20230101_configuration

Scheduling Mode *

CANCEL APPLY

5. Select a scheduling mode:



Schedule Settings

2 item(s) selected

Scheduling Mode *

- One Time
- Daily
- Weekly

CANCEL APPLY

- 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.

Schedule Settings

1 item(s) selected

Scheduling Mode *
One Time

Date * 2023-07-15 Time * 16:05

CANCEL APPLY

- 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.

Schedule Settings

1 item(s) selected

Scheduling Mode *
Daily

Time * 05:00 Period * 2023-07-15 – 2023-10-13

CANCEL APPLY

- 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.

Schedule Settings

1 item(s) selected

Scheduling Mode * Weekly Weekly Day * Mon. Wed. Fri.


Time * 05:00 Period * 2023-07-15 – 2023-10-13

CANCEL APPLY

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.

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

Delete Scheduling

2 item(s) selected

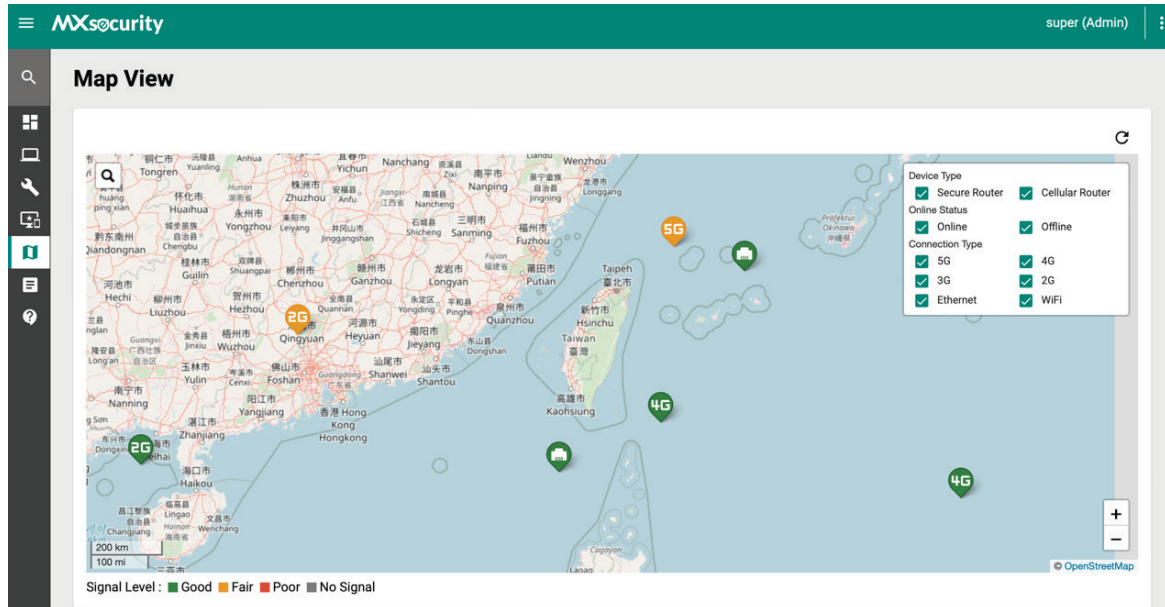
Are you sure you want to delete the selected scheduling?

CANCEL

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
	The cellular signal RSSI is higher than -73 dBm or the Ethernet WAN link is up.
	The cellular signal RSSI is between -73 to -89 dBm.
	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.

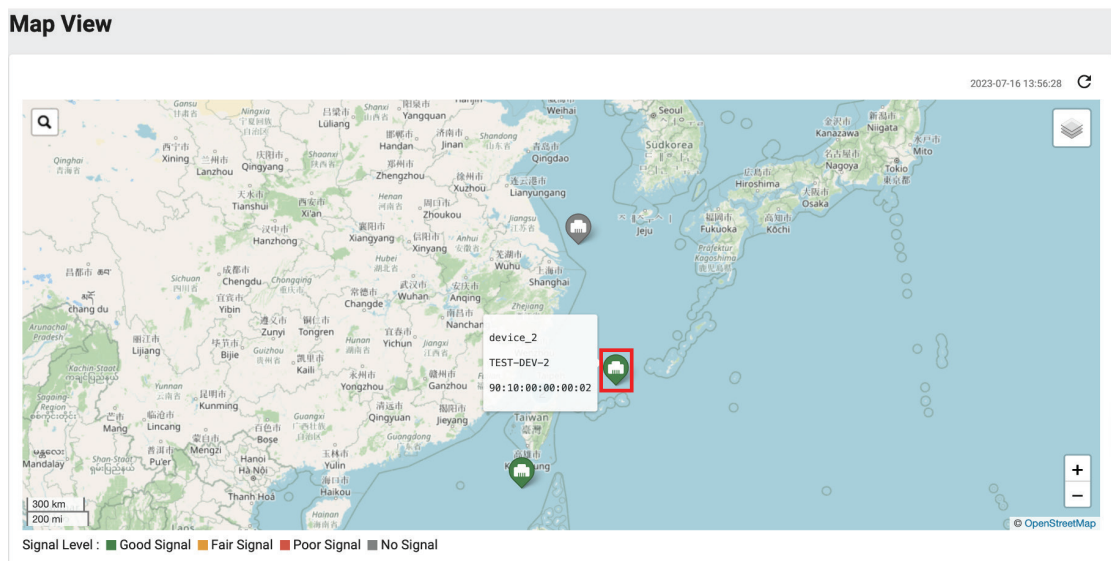
Icon	Description
	The device is using Ethernet WAN to connect to the internet.
	The device is using cellular 5G to connect to the internet.
	The device is using cellular 4G to connect to the internet.
	The device is using cellular 3G to connect to the internet.
	The device is using cellular 2G to connect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

Device device_2 Information



● Online
System Uptime
1d23h21m55s

Basic Information

Device Name device_2	Serial Number TEST-DEV-2	Product Model EDR-G9010-VPN-2MGSPF
MAC Address 90:10:00:00:00:02	LAN IP Address 202.212.5.254	Firmware Version V1.0.0
Location 125.0, 25.5	WAN IP Address 130.254.165.196	

CLOSE

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

Device device_4 Information



● Online
System Uptime
1d23h20m17s

Cellular Information

Cellular Module Enabled	Cellular Signal ---	Phone Number +886920629279
Cellular SIM SIM1	Cellular Mode ---	IMSI 933653273918636
Cellular Carrier CHUNGHWA TELECOM	Cellular Band WCDMA	IMEI 353251085809483


CLOSE

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.

Device Firewall/VPN Router 77777 Information

 **Online**
System Uptime
2d21h1m5s



Basic Information

Device Name Firewall/VPN Router 77777	Serial Number MOXA77777777	Product Model EDR-G9010-VPN-2MGSP
MAC Address 00:01:02:03:04:77	LAN IP Address 192.168.127.254	Firmware Version V3.0.0
Location ⓘ Device Location 	WAN IP Address 0.0.0.0	

CLOSE


4. Enter the longitude and latitude coordinates.

Location ⓘ

122.51, 31.2  

12 / 80

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.

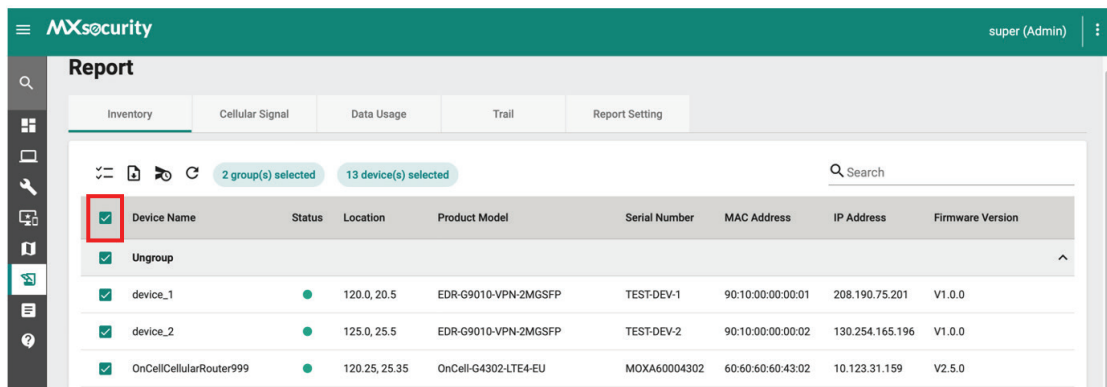
Inventory Reports

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.



The screenshot shows the MXsecurity web interface. The top navigation bar includes the MXsecurity logo and the user 'super (Admin)'. The main content area is titled 'Report' and has tabs for 'Inventory', 'Cellular Signal', 'Data Usage', 'Trail', and 'Report Setting'. The 'Inventory' tab is active. Below the tabs, there are icons for filtering, a search bar, and selection status indicators: '2 group(s) selected' and '13 device(s) selected'. A table with the following columns is displayed: Device Name, Status, Location, Product Model, Serial Number, MAC Address, IP Address, and Firmware Version. The table contains four rows: an 'Ungroup' header row, and three device entries: 'device_1', 'device_2', and 'OnCellCellularRouter999'. A red box highlights the 'Device Name' column header.

Device Name	Status	Location	Product Model	Serial Number	MAC Address	IP Address	Firmware Version
Ungroup							
device_1	●	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	●	125.0, 25.5	EDR-G9010-VPN-2MGSFP	TEST-DEV-2	90:10:00:00:00:02	130.254.165.196	V1.0.0
OnCellCellularRouter999	●	120.25, 25.35	OnCell-G4302-LTE4-EU	MOXA60004302	60:60:60:60:43:02	10.123.31.159	V2.5.0

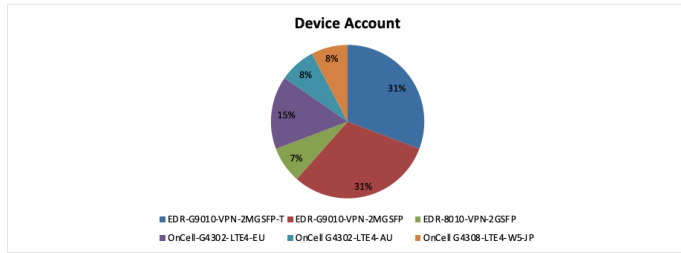
3. Click the  icon to generate a report in CSV format.

The inventory report includes the following information:

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

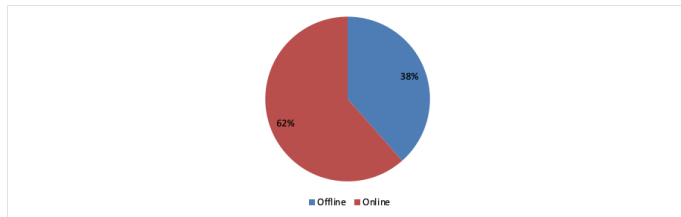
Product Model Statistics

Product Model	Device Account
EDR-G9010-VPN-2MGSPF-T	4
EDR-G9010-VPN-2MGSPF	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-2MGSPF-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-2MGSPF	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-2MGSPF-T	MOXA95275487	00:01:02:03:04:05	10.123.31.176	V3.0.0
OOOwen 9010	Offline	122, 25	EDR-G9010-VPN-2MGSPF-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	1071:98:43:02:01	0.0.0.0	V3.0.0
device 1	Online	120.0, 20.5	EDR-G9010-VPN-2MGSPF	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-2MGSPF	TEST-DEV-2	90:10:00:00:00:02	130.254.165.196	V1.0.0
device 3	Online	location 3	EDR-G9010-VPN-2MGSPF-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-2MGSPF	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.

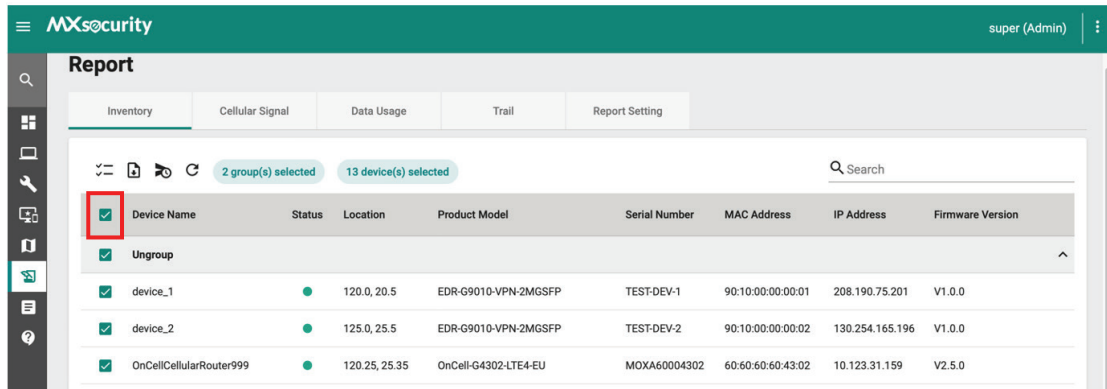
Scheduling an Inventory Report


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.

Schedule an Email to Send Inventory Report

13 item(s) selected


Receiver Email *

test1@moxa.com × Test2@moxa.com × 

Test3@moxa.com ×


3 / 5

Subject *

Inventory report of Tapei Site 

30 / 50

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.

Scheduling 


Scheduling Mode *


One Time Monthly

Report sending date

The report will be sent at 0:30 on the selected date and will include the **data** for the **selected date**.

Date *

2023-07-17 

 Current time zone at UTC+8, user can modify in the report setting.

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


Schedule Settings

1 item(s) selected


Scheduling Mode *

Daily

Time *

05:00 

Period *

2023-07-15 – 2023-10-13 

CANCEL APPLY


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 it to specified recipients by 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.

Schedule an Email to Send Cellular Signal Report

4 item(s) selected


Receiver Email *

test1@moxa.com × test2@moxa.com × 

test3@moxa.com ×


3 / 5

Subject *

Cellular Signal Report of Tapei Site 

36 / 50

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.

Scheduling 


Scheduling Mode *


One Time Daily

Report sending date


The report will be sent at 0:30 on the selected date and will include the **data** for the **previous date**.

Date *

2023-07-17 

 Current time zone at UTC+8, user can modify in the report setting.

- 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.

Scheduling 


Scheduling Mode *


One Time Daily

Report sending date

The report will be sent at 0:30 on the selected date and will include the **data** for the **previous date**.

Period *

2023-07-17 ~ 2024-07-15 

 Current time zone at UTC+8, user can modify in the report setting.


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

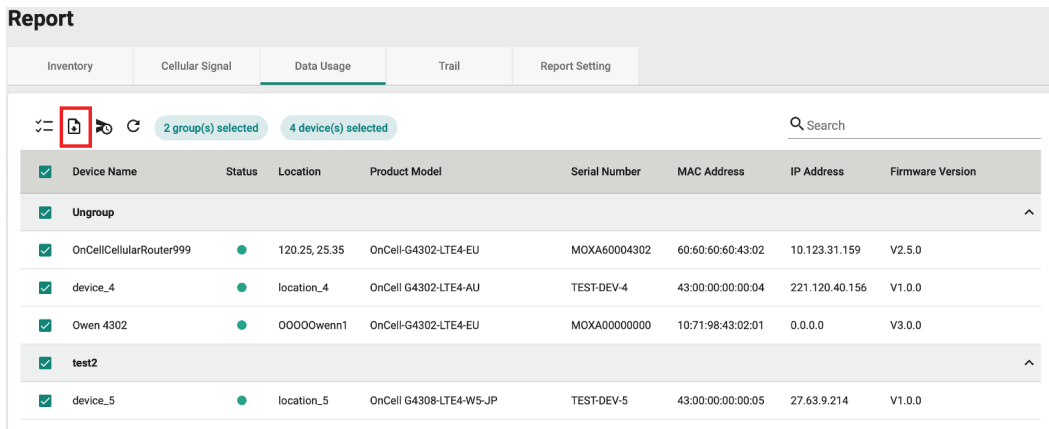
Data Usage Reports

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.



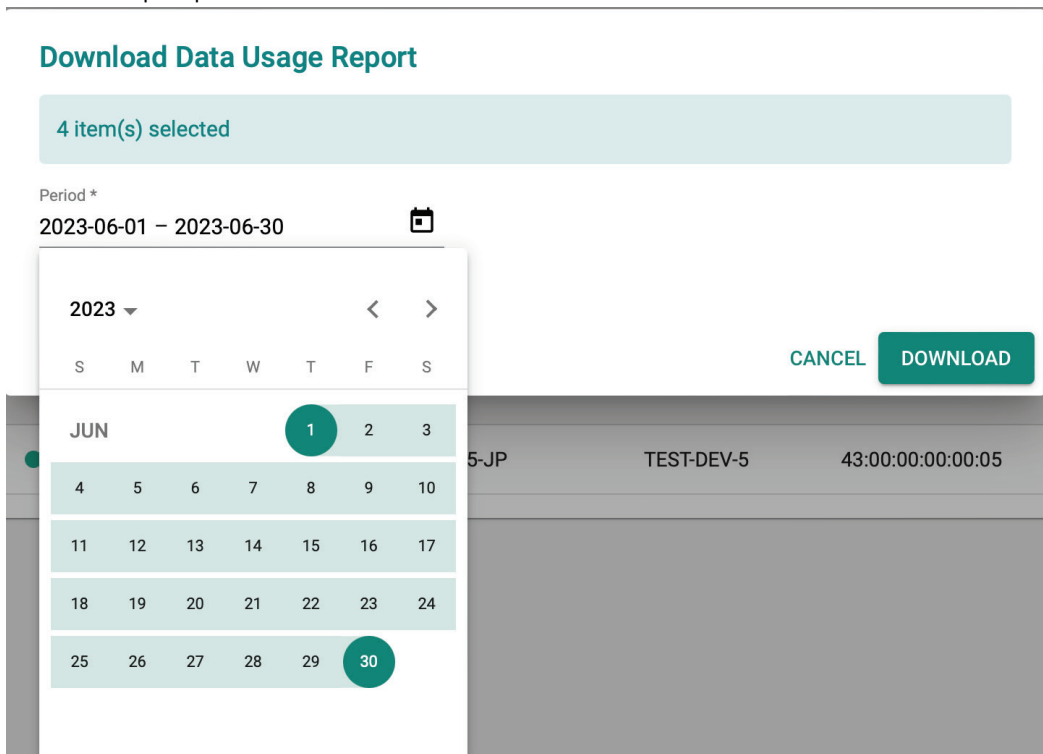
Report

Inventory Cellular Signal **Data Usage** Trail Report Setting

2 group(s) selected 4 device(s) selected

Device Name	Status	Location	Product Model	Serial Number	MAC Address	IP Address	Firmware Version
OnCellCellularRouter999	●	120.25, 25.35	OnCell-G4302-LTE4-EU	MOXA60004302	60:60:60:60:43:02	10.123.31.159	V2.5.0
device_4	●	location_4	OnCell-G4302-LTE4-AU	TEST-DEV-4	43:00:00:00:00:04	221.120.40.156	V1.0.0
Owen 4302	●	0000Owenn1	OnCell-G4302-LTE4-EU	MOXA00000000	10:71:98:43:02:01	0.0.0.0	V3.0.0
device_5	●	location_5	OnCell-G4308-LTE4-W5-JP	TEST-DEV-5	43:00:00:00:00:05	27.63.9.214	V1.0.0

4. Select the report period.



Download Data Usage Report

4 item(s) selected

Period *
2023-06-01 – 2023-06-30

2023

S M T W T F S

JUN

1 2 3

4 5 6 7 8 9 10

11 12 13 14 15 16 17

18 19 20 21 22 23 24

25 26 27 28 29 30

CANCEL DOWNLOAD



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**.

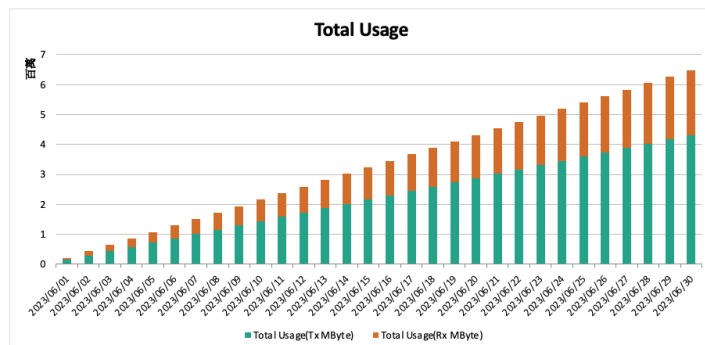
The cellular data usage report includes the following information:

Data Usage Report

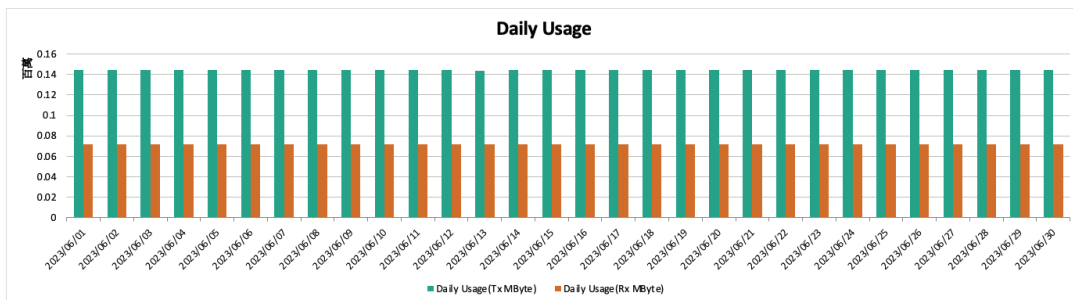
Create Account	super
Report Generated Date	2023/07/16
Report Generated Time	06:01 PM
Data Period	2023/06/01 - 2023/06/30
Device Name	device_4
Device MAC Address	43:00:00:00:00:04
Device Serial Number	TEST-DEV-4

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 it to specified recipients by 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.

Schedule an Email to Send Data Usage Report

4 item(s) selected


Receiver Email *

test1@moxa.com × Test2@moxa.com × 

Test3@moxa.com ×

3 / 5

Subject *

Data Usage report of Tapei Site 

31 / 50

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.

Scheduling 

Scheduling Mode *


One Time Monthly

Report sending date

The report will be sent at 0:30 on the selected date and will include the **data** for the **previous month**.

Date *

2023-07-17 

 Current time zone at UTC+8, user can modify in the report setting.

- 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.

Scheduling 


Scheduling Mode *

One Time Monthly


Report sending date

The report will be sent at 0:30 on the selected date and will include the **data** for the **previous month**.

Generate Report Date * Period *

17 2023-07-17 - 2024-07-15 

1 ~ 31

 Current time zone at UTC+8, user can modify in the report setting.


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

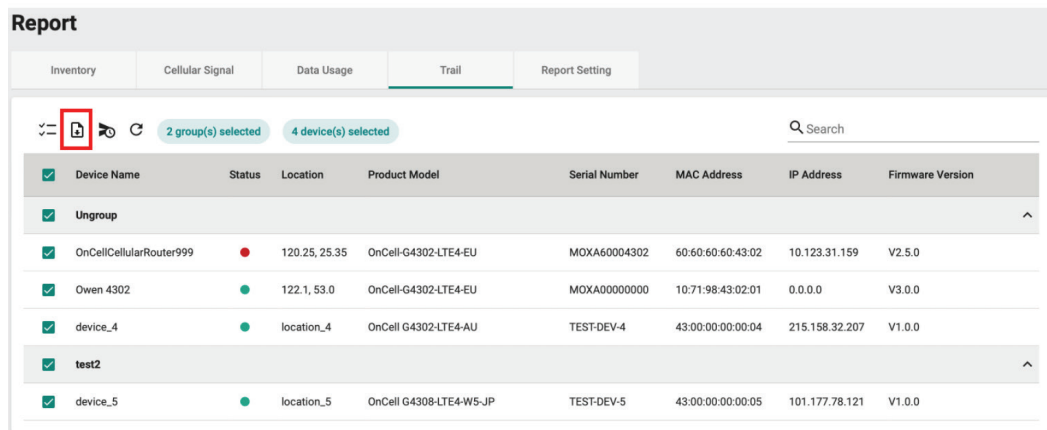
Trail Reports

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:

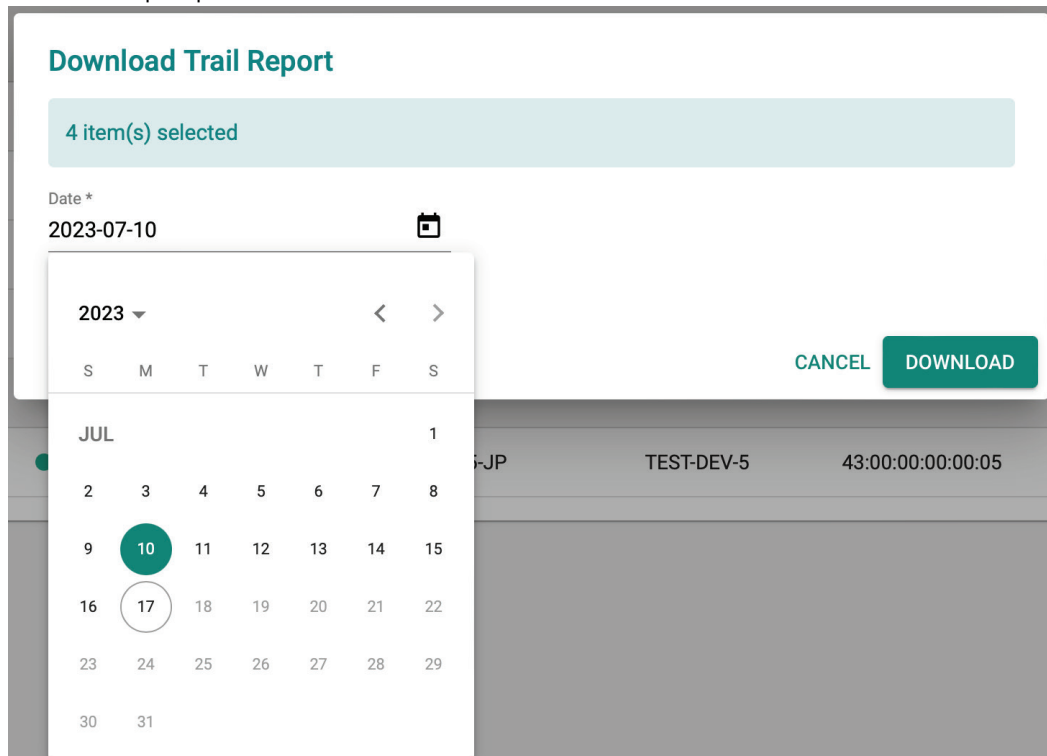
1. Navigate to **Report > Trail**.
2. Select the device(s) you want to generate a report for.
3. Click the  icon to generate a report in CSV format.



The screenshot shows the 'Report' interface with the 'Trail' tab selected. A table lists several devices with columns for Device Name, Status, Location, Product Model, Serial Number, MAC Address, IP Address, and Firmware Version. A red box highlights the download icon in the top left corner of the table area. Above the table, it indicates '2 group(s) selected' and '4 device(s) selected'.

Device Name	Status	Location	Product Model	Serial Number	MAC Address	IP Address	Firmware Version
OnCellCellularRouter999	●	120.25, 25.35	OnCell-G4302-LTE4-EU	MOXA60004302	60:60:60:60:43:02	10.123.31.159	V2.5.0
Owen 4302	●	122.1, 53.0	OnCell-G4302-LTE4-EU	MOXA00000000	10:71:98:43:02:01	0.0.0.0	V3.0.0
device_4	●	location_4	OnCell G4302-LTE4-AU	TEST-DEV-4	43:00:00:00:00:04	215.158.32.207	V1.0.0
test2	●						
device_5	●	location_5	OnCell G4308-LTE4-W5-JP	TEST-DEV-5	43:00:00:00:00:05	101.177.78.121	V1.0.0

4. Select the report period.



The screenshot shows the 'Download Trail Report' dialog box. It displays '4 item(s) selected' and a date selection interface. The date '2023-07-10' is selected. A calendar is open, showing the month of July 2023, with the 10th and 17th highlighted. The dialog includes 'CANCEL' and 'DOWNLOAD' buttons.



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 it to specified recipients by 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.

Schedule an Email to Send Trail Report

4 item(s) selected

Receiver Email *

test1@moxa.com × test2@moxa.com × i

test3@moxa.com ×

3 / 5

Subject *

Trail Report of OnCell Devices i

30 / 50

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.

Scheduling i

Scheduling Mode *

- One Time Daily

Report sending date

The report will be sent at 0:30 on the selected date and will include the **data** for the **previous date**.

Date *

2023-07-18 i

- 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.

Scheduling i

Scheduling Mode *

- One Time Daily

Report sending date

The report will be sent at 0:30 on the selected date and will include the **data** for the **previous date**.

Period *

2023-07-18 – 2024-07-16 i

i Current time zone at UTC+8, user can modify in the report setting.

7. Click **APPLY**.

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

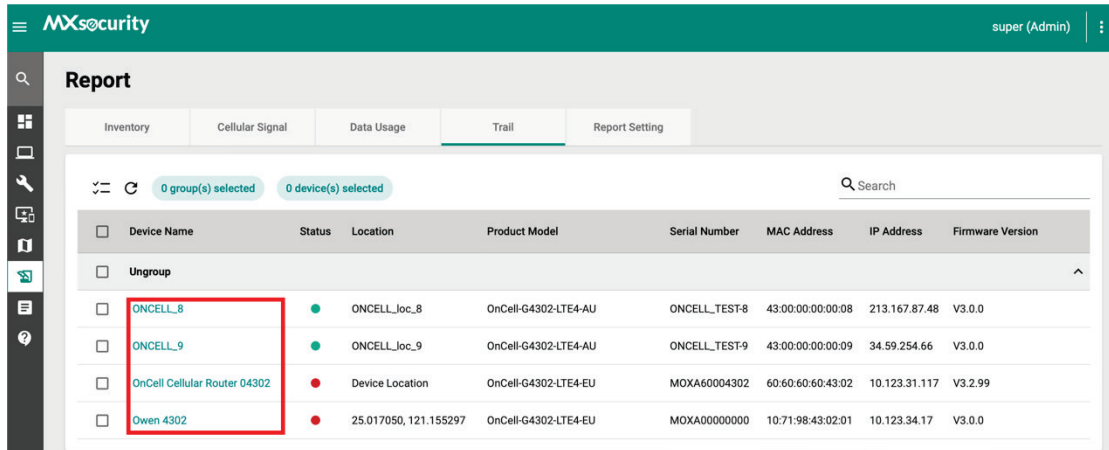
Viewing GPS Trajectories

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.

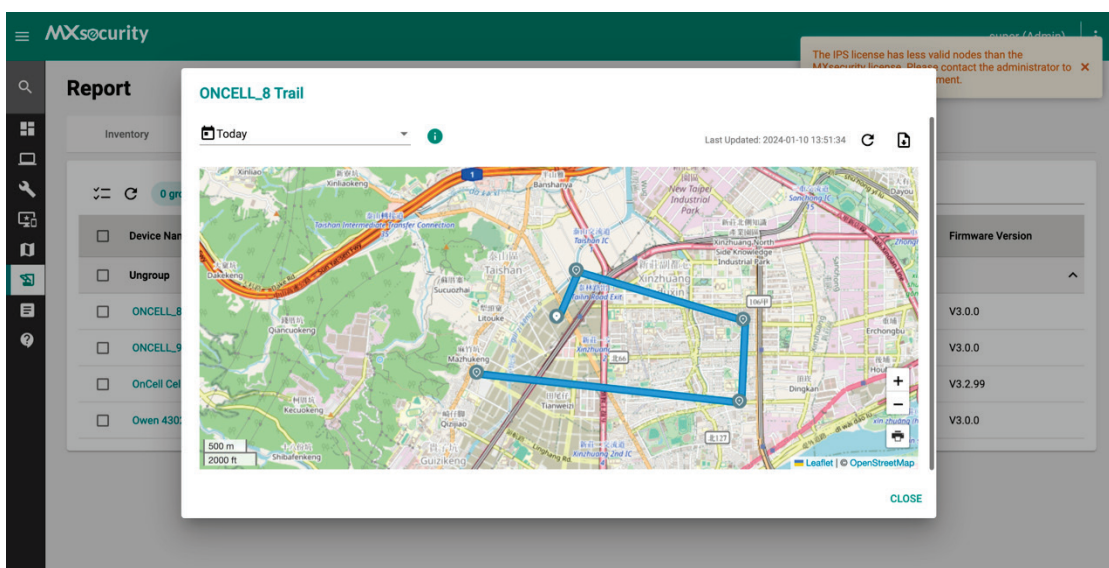
Steps:

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

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



- 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:

- Navigate to **Report > Report Setting > Time Zone Setting**.
- Select the time zone from the drop-down menu.
- 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

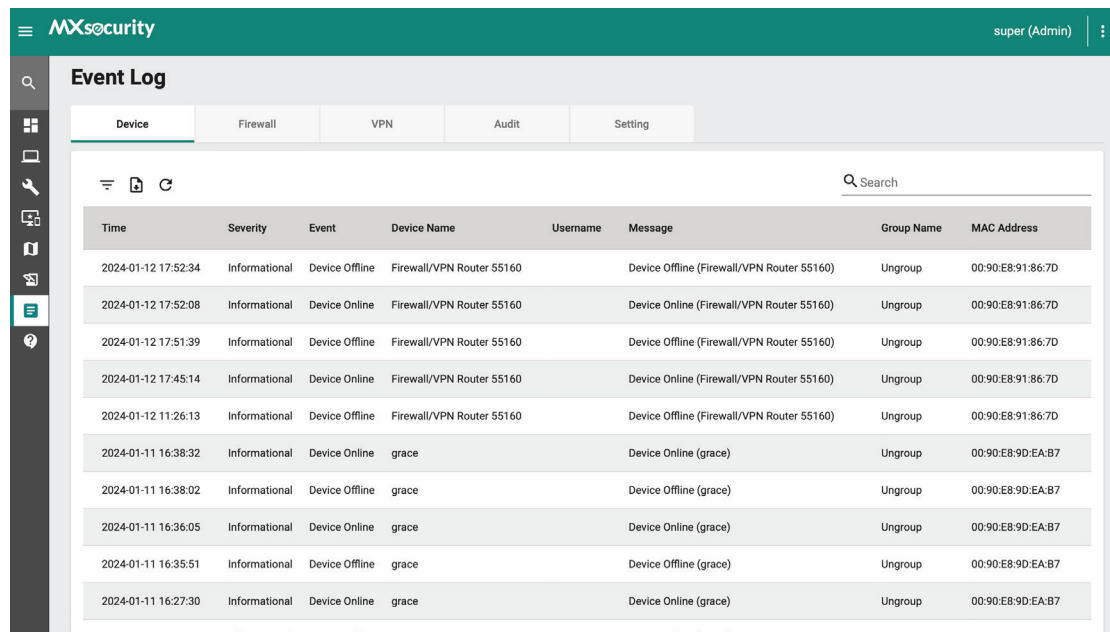
This chapter covers the event log and notification functions. Users can view logs related to the device, firewall, VPN, and audits. The notification function enables users to receive notifications for particular event logs. Users can send these notifications to designated email recipients or a syslog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




The screenshot shows the MXsecurity Event Log interface. The top navigation bar includes the MXsecurity logo and the user 'super (Admin)'. The main content area is titled 'Event Log' and features a sidebar with navigation icons. Below the title, there are tabs for 'Device', 'Firewall', 'VPN', 'Audit', and 'Setting', with 'Device' selected. A search bar is located on the right. The main table displays a list of events with the following columns: Time, Severity, Event, Device Name, Username, Message, Group Name, and MAC Address. The table contains several rows of device online and offline events for a 'Firewall/VPN Router 55160' and a device named 'grace'.

Time	Severity	Event	Device Name	Username	Message	Group Name	MAC Address
2024-01-12 17:52:34	Informational	Device Offline	Firewall/VPN Router 55160		Device Offline (Firewall/VPN Router 55160)	Ungroup	00:90:E8:91:86:7D
2024-01-12 17:52:08	Informational	Device Online	Firewall/VPN Router 55160		Device Online (Firewall/VPN Router 55160)	Ungroup	00:90:E8:91:86:7D
2024-01-12 17:51:39	Informational	Device Offline	Firewall/VPN Router 55160		Device Offline (Firewall/VPN Router 55160)	Ungroup	00:90:E8:91:86:7D
2024-01-12 17:45:14	Informational	Device Online	Firewall/VPN Router 55160		Device Online (Firewall/VPN Router 55160)	Ungroup	00:90:E8:91:86:7D
2024-01-12 11:26:13	Informational	Device Offline	Firewall/VPN Router 55160		Device Offline (Firewall/VPN Router 55160)	Ungroup	00:90:E8:91:86:7D
2024-01-11 16:38:32	Informational	Device Online	grace		Device Online (grace)	Ungroup	00:90:E8:9D:EA:B7
2024-01-11 16:38:02	Informational	Device Offline	grace		Device Offline (grace)	Ungroup	00:90:E8:9D:EA:B7
2024-01-11 16:36:05	Informational	Device Online	grace		Device Online (grace)	Ungroup	00:90:E8:9D:EA:B7
2024-01-11 16:35:51	Informational	Device Offline	grace		Device Offline (grace)	Ungroup	00:90:E8:9D:EA:B7
2024-01-11 16:27:30	Informational	Device Online	grace		Device Online (grace)	Ungroup	00:90:E8:9D:EA:B7
2024-01-11 16:26:52	Informational	Device Offline	grace		Device Offline (grace)	Ungroup	00:90:E8:9D:EA:B7


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 and click **APPLY**. The logs will renew immediately to reflect the selected


criteria.


Filters ×


Start Date 

Start Time 


End Date 

End Time 


Event 

Severity 

CLEAR APPLY

- 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.

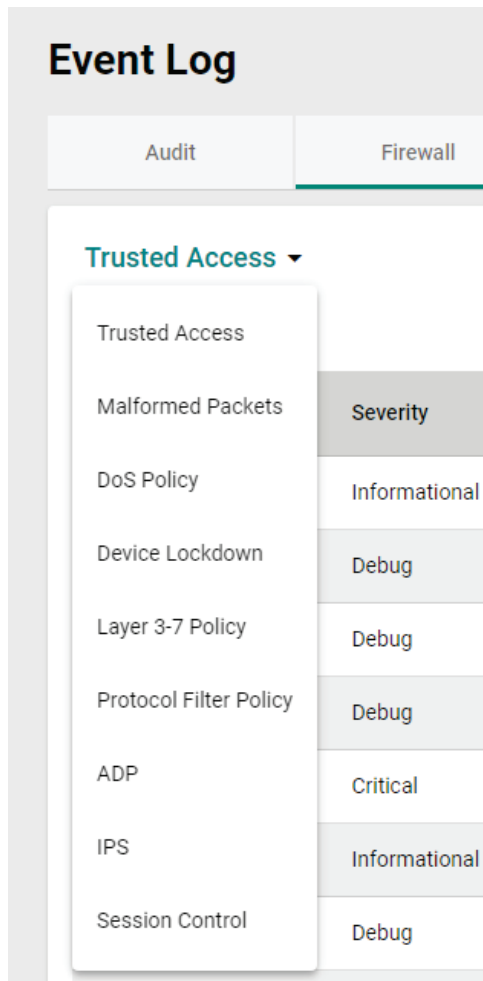
Index	Time	Severity	Device Name	Group Name	EtherType	IP Protocol	Incoming Interface	Source MAC	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	TCP Flags	ICMP Type	ICMP Code	Action	Addition Message
8747347	2024-01-14 23:22:11	Emergency	ROUTER_7	Ungroup 2048		TCP	WAN	00:26:0A:25:B2:00	192.168.1.7	0	--	10.124.34.7	0	--	--	--	Allow	
8747346	2024-01-14 23:22:11	Error	ROUTER_5	Ungroup 2048		TCP	WAN	00:26:0A:25:B2:00	192.168.1.3	0	--	10.124.34.3	0	--	--	--	Allow	
8747345	2024-01-14 23:22:11	Emergency	ROUTER_6	Ungroup 2048		TCP	WAN	00:26:0A:25:B2:00	192.168.1.7	0	--	10.124.34.7	0	--	--	--	Allow	
8747344	2024-01-14 23:22:10	Error	ROUTER_1	Ungroup 2048		TCP	WAN	00:26:0A:25:B2:00	192.168.1.8	0	--	10.124.34.8	0	--	--	--	Allow	
8747343	2024-01-14 23:21:11	Emergency	ROUTER_7	Ungroup 2048		TCP	WAN	00:26:0A:25:B2:00	192.168.1.4	0	--	10.124.34.4	0	--	--	--	Allow	
8747342	2024-01-14 23:21:11	Error	ROUTER_7	Ungroup 2048		TCP	WAN	00:26:0A:25:B2:00	192.168.1.9	0	--	10.124.34.9	0	--	--	--	Allow	
8747341	2024-01-14 23:21:11	Error	ROUTER_6	Ungroup 2048		TCP	WAN	00:26:0A:25:B2:00	192.168.1.8	0	--	10.124.34.8	0	--	--	--	Allow	
8747340	2024-01-14 23:21:11	Critical	ROUTER_3	Ungroup 2048		TCP	WAN	00:26:0A:25:B2:00	192.168.1.5	0	--	10.124.34.5	0	--	--	--	Allow	
8747339	2024-01-14 23:21:11	Warning	ROUTER_3	Ungroup 2048		TCP	WAN	00:26:0A:25:B2:00	192.168.1.1	0	--	10.124.34.1	0	--	--	--	Allow	

Viewing Firewall Logs


Steps:

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

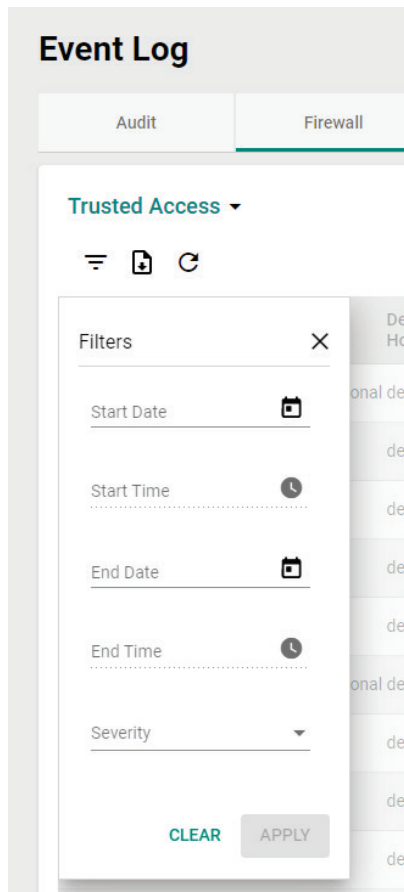
2. Select the firewall function event log type from the drop-down menu.




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 and 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.



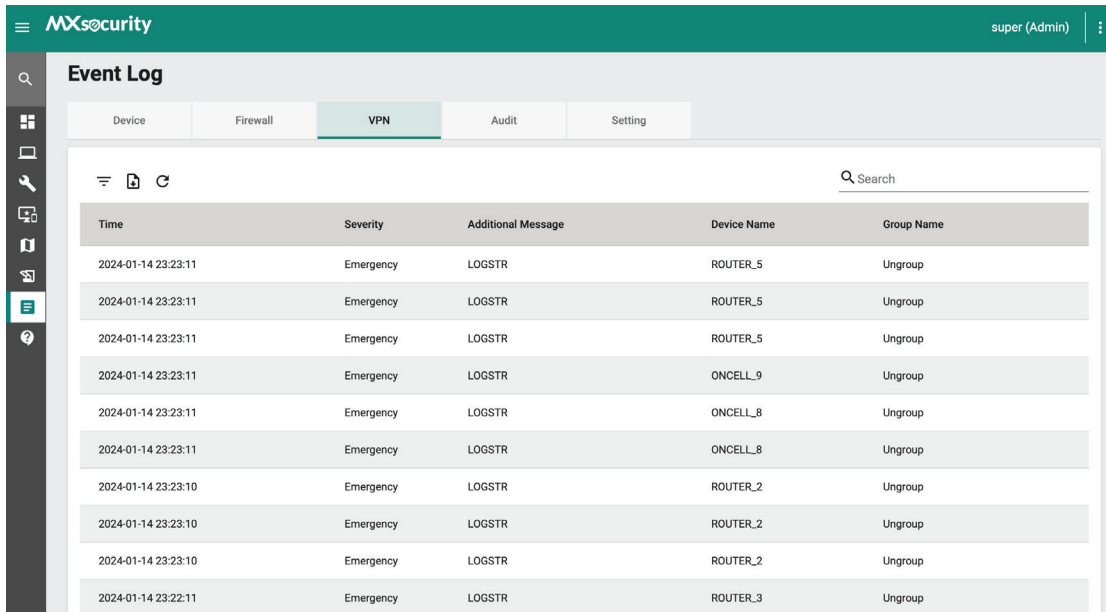
The following table describes the log's fields.

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.

Field	Description
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.
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.




The screenshot shows the MXsecurity web interface. At the top, there is a green header with the MXsecurity logo on the left and the user 'super (Admin)' on the right. Below the header is a navigation bar with tabs for 'Device', 'Firewall', 'VPN', 'Audit', and 'Setting'. The 'VPN' tab is currently selected. The main content area is titled 'Event Log' and contains a table of log entries. The table has columns for 'Time', 'Severity', 'Additional Message', 'Device Name', and 'Group Name'. There are 11 log entries, all with a severity of 'Emergency' and a message of 'LOGSTR'. The device names include ROUTER_5, ONCELL_9, ONCELL_8, ROUTER_2, and ROUTER_3. The group name for all entries is 'Ungroup'. A search bar is located at the top right of the table area.

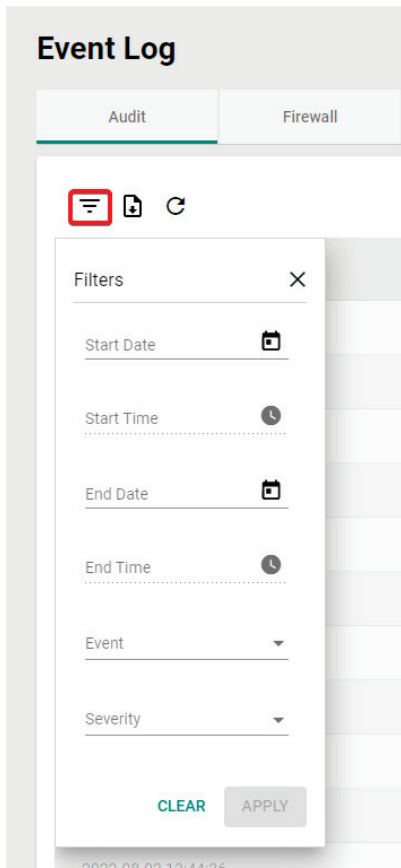
Time	Severity	Additional Message	Device Name	Group Name
2024-01-14 23:23:11	Emergency	LOGSTR	ROUTER_5	Ungroup
2024-01-14 23:23:11	Emergency	LOGSTR	ROUTER_5	Ungroup
2024-01-14 23:23:11	Emergency	LOGSTR	ROUTER_5	Ungroup
2024-01-14 23:23:11	Emergency	LOGSTR	ONCELL_9	Ungroup
2024-01-14 23:23:11	Emergency	LOGSTR	ONCELL_8	Ungroup
2024-01-14 23:23:11	Emergency	LOGSTR	ONCELL_8	Ungroup
2024-01-14 23:23:10	Emergency	LOGSTR	ROUTER_2	Ungroup
2024-01-14 23:23:10	Emergency	LOGSTR	ROUTER_2	Ungroup
2024-01-14 23:23:10	Emergency	LOGSTR	ROUTER_2	Ungroup
2024-01-14 23:22:11	Emergency	LOGSTR	ROUTER_3	Ungroup


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, event category, or log severity from the respective drop-menu and 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.

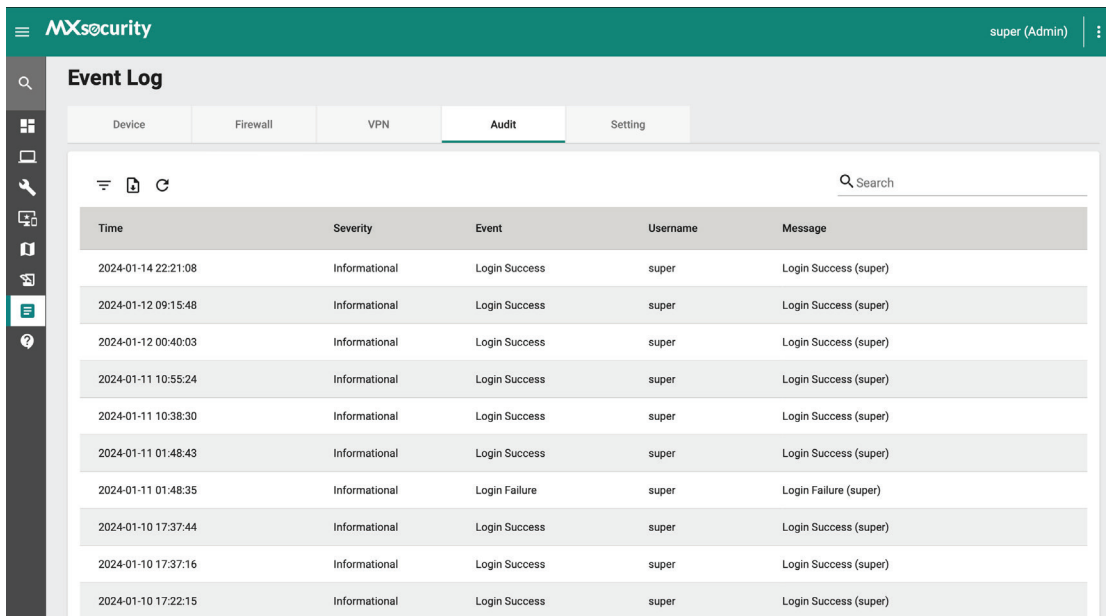


The following table describes the log's fields.

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.




The screenshot shows the MXsecurity web interface. At the top, there is a green header with the MXsecurity logo on the left and the user 'super (Admin)' on the right. Below the header is a navigation bar with tabs for 'Device', 'Firewall', 'VPN', 'Audit', and 'Setting'. The 'Audit' tab is selected. The main content area is titled 'Event Log' and contains a search bar and a table of events. The table has columns for Time, Severity, Event, Username, and Message. The events listed are:

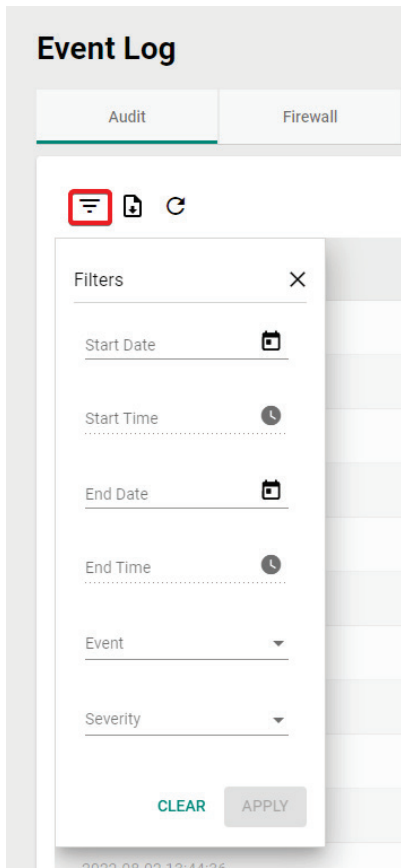
Time	Severity	Event	Username	Message
2024-01-14 22:21:08	Informational	Login Success	super	Login Success (super)
2024-01-12 09:15:48	Informational	Login Success	super	Login Success (super)
2024-01-12 00:40:03	Informational	Login Success	super	Login Success (super)
2024-01-11 10:55:24	Informational	Login Success	super	Login Success (super)
2024-01-11 10:38:30	Informational	Login Success	super	Login Success (super)
2024-01-11 01:48:43	Informational	Login Success	super	Login Success (super)
2024-01-11 01:48:35	Informational	Login Failure	super	Login Failure (super)
2024-01-10 17:37:44	Informational	Login Success	super	Login Success (super)
2024-01-10 17:37:16	Informational	Login Success	super	Login Success (super)
2024-01-10 17:22:15	Informational	Login Success	super	Login Success (super)


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, event category, or log severity from the respective drop-menu and 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.

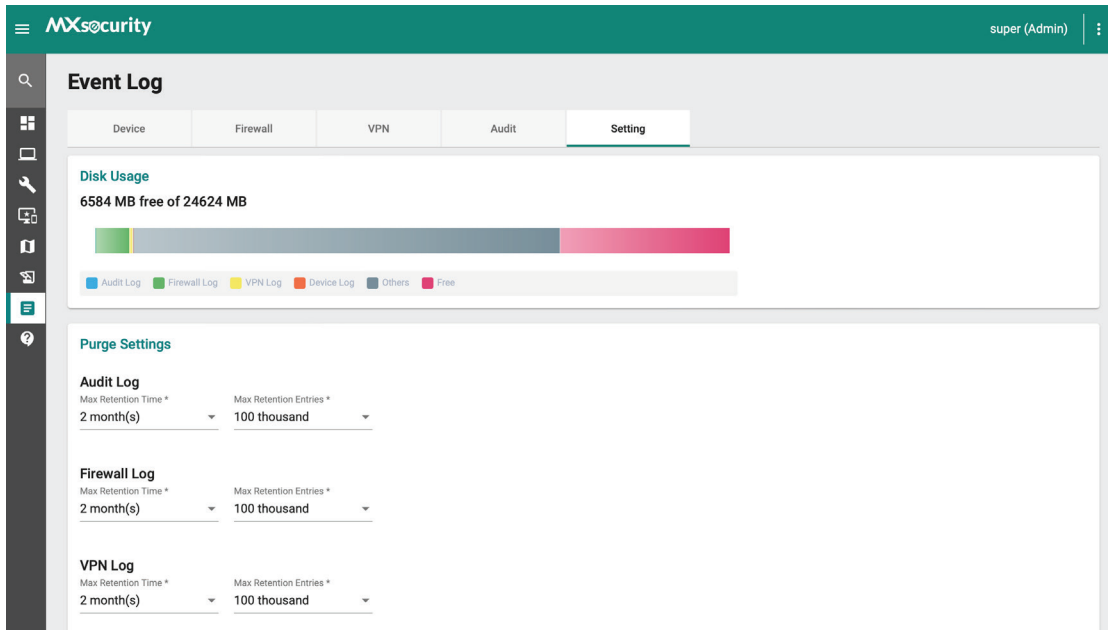


The following table describes the log's fields.

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 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.

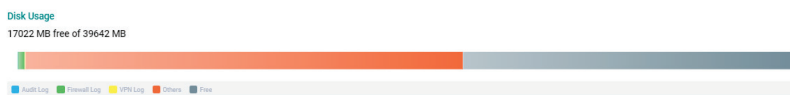


Purging Event Logs

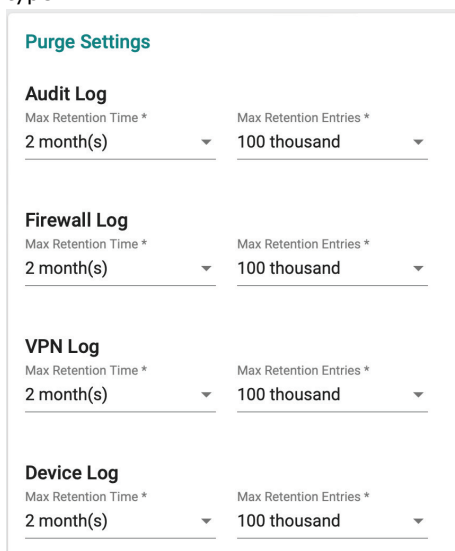
The log purging function allows users to configure automatic log purging based on the specified retention time and log amount. Purging logs may be useful when the system generates a lot of event logs, which may affect network performance.

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.

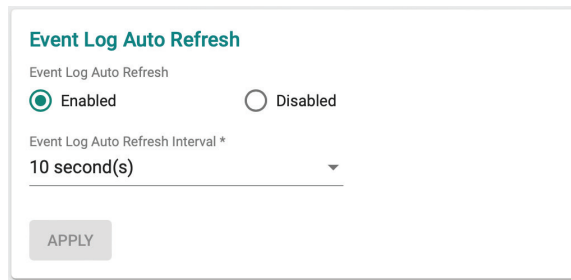
1. Navigate to **Logging > Event Log > Setting**.
2. In the Disk Usage section, check the current used and available disk space.



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.



The screenshot shows a configuration panel titled "Event Log Auto Refresh". It contains two radio buttons: "Enabled" (which is selected) and "Disabled". Below this is a dropdown menu labeled "Event Log Auto Refresh Interval *" with "10 second(s)" selected. At the bottom of the panel is an "APPLY" button.


5. Click **APPLY**.

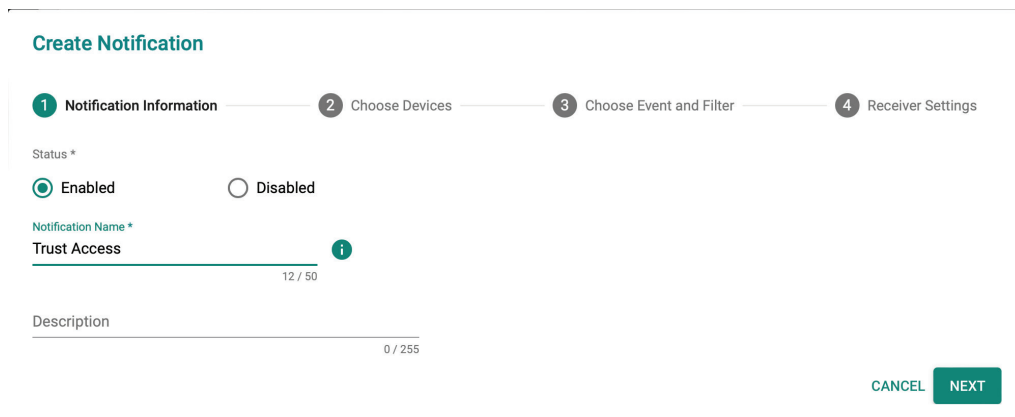
Notifications

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.



The screenshot shows the "Create Notification" wizard. It has a progress bar with four steps: 1. Notification Information (active), 2. Choose Devices, 3. Choose Event and Filter, and 4. Receiver Settings. Below the progress bar, there are two radio buttons: "Enabled" (selected) and "Disabled". The "Notification Name *" field contains "Trust Access" with a character count of "12 / 50" and an information icon. The "Description" field is empty with a character count of "0 / 255". At the bottom right, there are "CANCEL" and "NEXT" buttons.

4. Click **NEXT**.

- Select the device(s) that will send notifications for the specified events.

Create Notification

1 Notification Information — 2 Choose Devices — 3 Choose Event and Filter — 4 Receiver Settings

10 of 13 selected Search

<input checked="" type="checkbox"/>	Device Name ↑	Status	Location	Product Model	Serial Number	MAC Address	Firmware Version	Group
<input checked="" type="checkbox"/>	Firewall/VPN Router 55160	●	Device Location	EDR-G9010-VPN-2MGSFP-T	TBZKB1155160	00:90:E8:91:86:7D	V3.0.0	Ungroup
<input checked="" type="checkbox"/>	Firewall/VPN Router 77777	●	Device Location	EDR-G9010-VPN-2MGSFP	MOXA77777777	00:01:02:03:04:77	V3.0.0	Ungroup
<input checked="" type="checkbox"/>	Firewall/VPN Router Hades	●	Device Location	EDR-G9010-VPN-2MGSFP-T	MOXA95275487	00:01:02:03:04:05	V3.0.0	Ungroup
<input checked="" type="checkbox"/>	Firewall/VPN Router Hades	●	Device Location	EDR-8010-VPN-2GSFP	MOXA00000000	00:90:E8:A7:72:C0	V3.0.0	Ungroup
<input checked="" type="checkbox"/>	OOOwen 9010	●	122, 25	EDR-G9010-VPN-2MGSFP-T	MOXA00112233	00:90:E8:90:10:06	V3.0.0	Ungroup
<input checked="" type="checkbox"/>	OnCellCellularRouter999	●	120.25, 25.35	OnCell-G4302-LTE4-EU	MOXA60004302	60:60:60:60:43:02	V2.5.0	Ungroup
<input checked="" type="checkbox"/>	Owen 4302	●	OOOOwenn1	OnCell-G4302-LTE4-EU	MOXA00000000	10:71:98:43:02:01	V3.0.0	Ungroup

- Select the event types and configure filter rules:

- Select the event type.

Create Notification

1 Notification Information — 2 Choose Devices — 3 Choose Event and Filter — 4 Receiver Settings

Firewall

- Trusted Access
- Malformed Packets
- DoS Policy
- Layer 3-7 Policy
- Protocol Filter Policy

Severity Mode

Source IP Destination IP

Source IP Destination IP

BACK NEXT

- 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.

Create Notification

1 Notification Information — 2 Choose Devices — 3 Choose Event and Filter — 4 Receiver Settings

Notification Event *
Trusted Access

Event Filter Rule

Severity
Severity Rule
Lower than or Equal to Severity Mode

Source IP Destination IP

Source IP Destination IP

BACK NEXT

7. Configure the notification content and recipient settings.

Create Notification

Dear Sir/ Madam,

This notification was automatically sent from MXsecurity.

Email Content *

The event \${event} triggered at device \${productModel}, \${deviceName}, happened at \${eventTime}.

96 / 256 [Reset to default](#)

Please check the detailed information on MXsecurity.

Best regards,
MXsecurity

Receiver Email Address *

0 / 5

- + Device Name
- + Product Model
- + Mac Address
- + Location
- + Serial Number
- + Event Time
- + Notification Name
- + Event

- 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.

Advanced Settings *

Notification Limit *

Enabled Disabled

MAX. Notification * Period of Time *

1 ~ 5 1 ~ 60 minute(s)

i Once the maximum number of notifications has been reach in period of time, no more notifications are sent until next period.

- 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.

Username	Role	Last Login	Description
o1	Operator	2022-07-28 11:24:50	
super	Admin	2022-08-02 08:00:27	root

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

Task	Description
Add a user account	Click the icon 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

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

System Tab

Configuration Screen	Action	User Roles		
		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

Configuration Screen	Action	User Roles		
		Admin	Operator	Viewer
Device Group	View	Yes	VG	No
	All operations	Yes	No	No
Firmwares	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

Configuration Screen	Action	User Roles		
		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

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

Report

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

Logging

Configuration Screen	Action	User Roles		
		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.


Create User

Username * 


 0 / 32

Password *  

 0 / 32

Confirm Password * 

 0 / 32

Role * 

Description

 0 / 255

CANCEL

APPLY

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.

User Accounts

Account List Password Policy

  0 of 1 selected

<input type="checkbox"/>	Username ↑	Role
<input type="checkbox"/> 	o1	Operator
	super	Admin

The **Create User** screen will appear.

Create User

Username * 0 / 32

Password * 0 / 32

Confirm Password * 0 / 32

Role *


Description 0 / 255

CANCEL APPLY

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.

User Accounts

Account List Password Policy


+ ↻ 0 of 1 selected

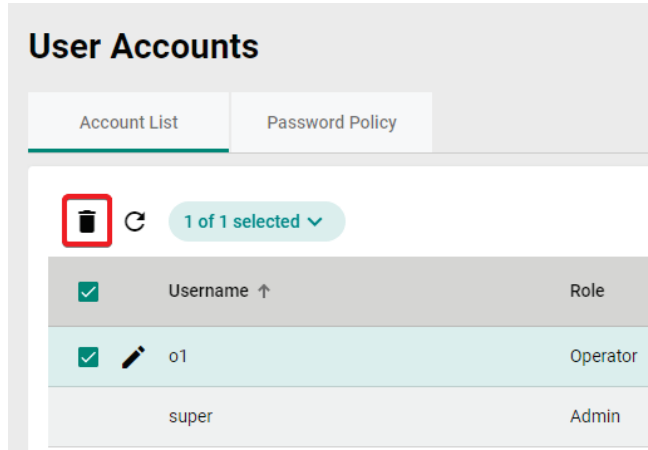
<input type="checkbox"/>	Username ↑	Role
<input type="checkbox"/>	o1	Operator
<input type="checkbox"/>	super	Admin

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**.

Delete User(s)

1 item(s) selected

Are you sure you want to delete the selected user(s)?

CANCEL

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.

The screenshot shows the 'User Accounts' management console with the 'Password Policy' tab selected. The 'Minimum Length' is set to 8, with a range of 8 to 32. The following options are checked: 'Cannot include the username' and 'The new password cannot be the same as the last password'. Other options for uppercase, lowercase, and digit requirements are unchecked. A list of special characters is provided. An 'APPLY' button is at the bottom.

3. Click **APPLY**.

Changing Your Account Password

Steps:

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

The screenshot shows the user management console banner for 'super (Admin)'. A dropdown menu is open, showing three options: 'Change Password' (with a lock icon), 'Troubleshooting' (with a magnifying glass icon), and 'Log Out' (with a door icon).

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

The 'Change Password' screen has three input fields: 'Current Password *', 'New Password *', and 'Confirm New Password *'. Each field has a password strength indicator (0/32) and a toggle icon. The 'New Password' field also has an information icon. At the bottom, there are 'CANCEL' and 'APPLY' buttons.

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:** The number of seats allowed in the license should be equal to or greater than the nodes managed by MXsecurity, so that IPS functionality is enabled and can be managed via MXsecurity.



NOTE

Only one IPS license can be used at any given time. When more than one IPS license is applied to MXsecurity, only the latest one will be kept.

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 table describes the license information.

Field	Description
Name	The name of the license.
Valid for	The remaining duration the license is valid for.
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.
MXsecurity ID	The unique ID of this MXsecurity instance.

The following table describes the license history.

Message	Description
Update Date	The date of this license was entered.
Activation Code	The activation code of the license.
License Type	The type of license.
License Duration	The duration of the license.
License Nodes	The number of nodes 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) represents 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.

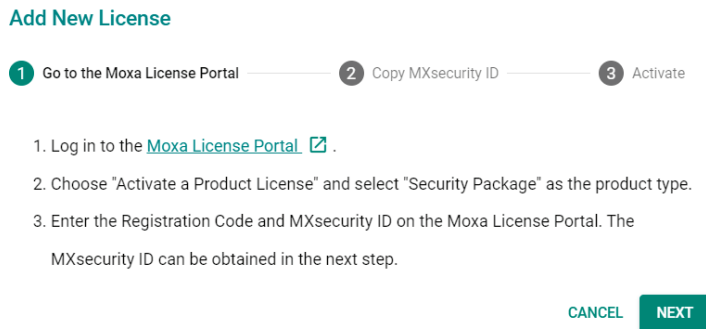
Adding a New License

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

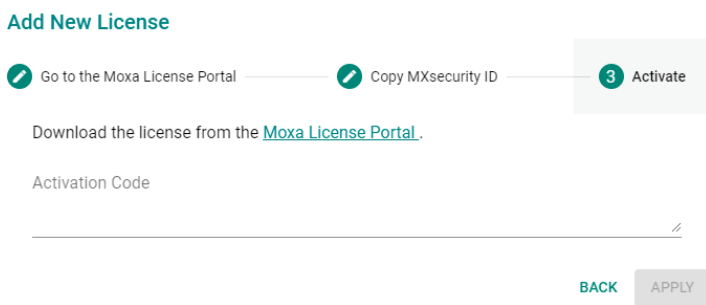
Steps:

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

2. Click the  button.
The **Add New License** screen will appear.



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




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

Binding a License to a Device

To enable specific functions on devices, you need to bind the appropriate license to the managed device first.

Steps:

1. Navigate to **System > Licenses**.
2. Click the **IPS** tab.
3. In the **Device License Binding** section, check the box of the device(s) you want to bind the license to.
4. Click the  icon to bind the license to the selected device(s).

- When prompted to confirm, click **APPLY**.

Apply a Device License

1 item(s) selected

Are you sure you want to apply the license to the selected device(s)?


CANCEL

APPLY

Unbinding a License From a Device

You can unbind a license from a managed device in order to assign it to another device. Note that unbinding a license will cause the relevant function to become unavailable on that device.

Steps:

- Navigate to **System > Licenses**.
- Click the **IPS** tab.
- Check the box of the device(s) you want to unbind the license from.
- Click the  icon to unbind the license from the selected device(s).
- When prompted to confirm, click **REMOVE**.

Remove a Device License

1 item(s) selected

Are you sure you want to remove the license from the selected device(s)?

CANCEL

REMOVE

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.


The screenshot shows the 'Settings' page with the 'Preferences' tab active. The 'User Auto Logout After *' dropdown is set to '15 minute(s)' and the 'Dashboard Auto Refresh Interva...' dropdown is set to '15 second(s)'. An 'APPLY' button is located at the bottom of the form.

3. Click **APPLY**.

Configuring the System Time

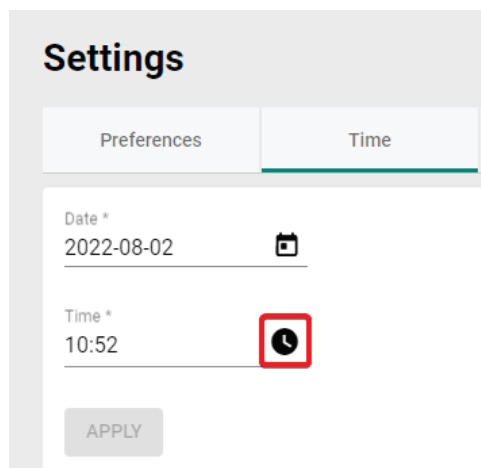
From the Time tab, you can manually set the system time. MXsecurity will automatically synchronize the system time with all managed nodes.

Steps:

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

The screenshot shows the 'Settings' page with the 'Time' tab active. The 'Date *' field is set to '2022-08-02' and has a calendar icon to its right, which is highlighted with a red square. The 'Time *' field is set to '10:52' and has a clock icon to its right. An 'APPLY' button is located at the bottom of the form.

- Click the  icon to select the time.

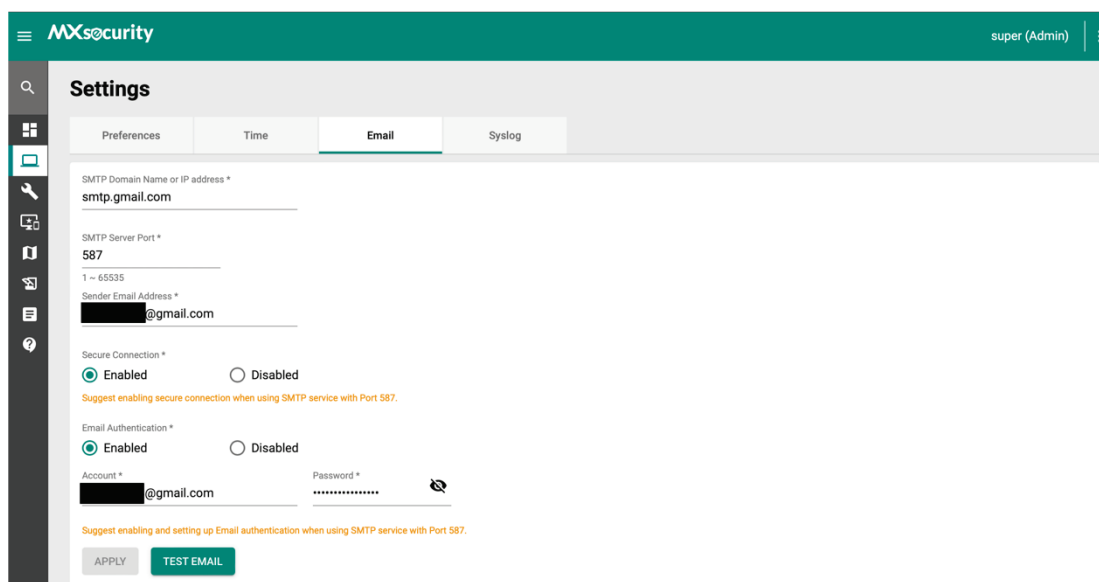


The screenshot shows the 'Settings' page with the 'Time' tab selected. The 'Date' field is set to '2022-08-02' and the 'Time' field is set to '10:52'. A red box highlights the 'Time' field, and a clock icon is visible next to it. An 'APPLY' button is at the bottom.

- 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.



The screenshot shows the 'MXsecurity' interface with the 'Settings' page and the 'Email' tab selected. The settings include:

- SMTP Domain Name or IP address: smtp.gmail.com
- SMTP Server Port: 587 (range 1 ~ 65535)
- Sender Email Address: [redacted]@gmail.com
- Secure Connection: Enabled, Disabled. Suggest enabling secure connection when using SMTP service with Port 587.
- Email Authentication: Enabled, Disabled. Suggest enabling and setting up Email authentication when using SMTP service with Port 587.
- Account: [redacted]@gmail.com
- Password: [redacted]

Buttons for 'APPLY' and 'TEST EMAIL' are at the bottom.

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.

The screenshot shows the MXsecurity web interface. At the top, there's a green header with the MXsecurity logo and a user profile 'super (Admin)'. Below the header is a navigation menu with icons for home, settings, and help. The main content area is titled 'Settings' and has four tabs: 'Preferences', 'Time', 'Email', and 'Syslog'. The 'Syslog' tab is active. It contains a form with the following fields: 'Send logs to Syslog Server*' with radio buttons for 'Enabled' (selected) and 'Disabled'; 'Server Address/ Domain Name*' with the value '18.118.160.233'; 'Port*' with the value '514'; and 'Format*' with a dropdown menu showing 'LEEF'. At the bottom of the form are two buttons: 'APPLY' and 'SEND TEST SYSLOG'.

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**.