MXsecurity User Manual

Version 1.0, September 2022

www.moxa.com/product

MXsecurity User Manual

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

Copyright Notice

Trademarks

Disclaimer

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

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. Introduction

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

Key Features

Centralized Management

Manage and monitor your firewall deployments 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, and 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.

System Requirements

The computer that MXsecurity is installed on must satisfy the following system requirements. The systems 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

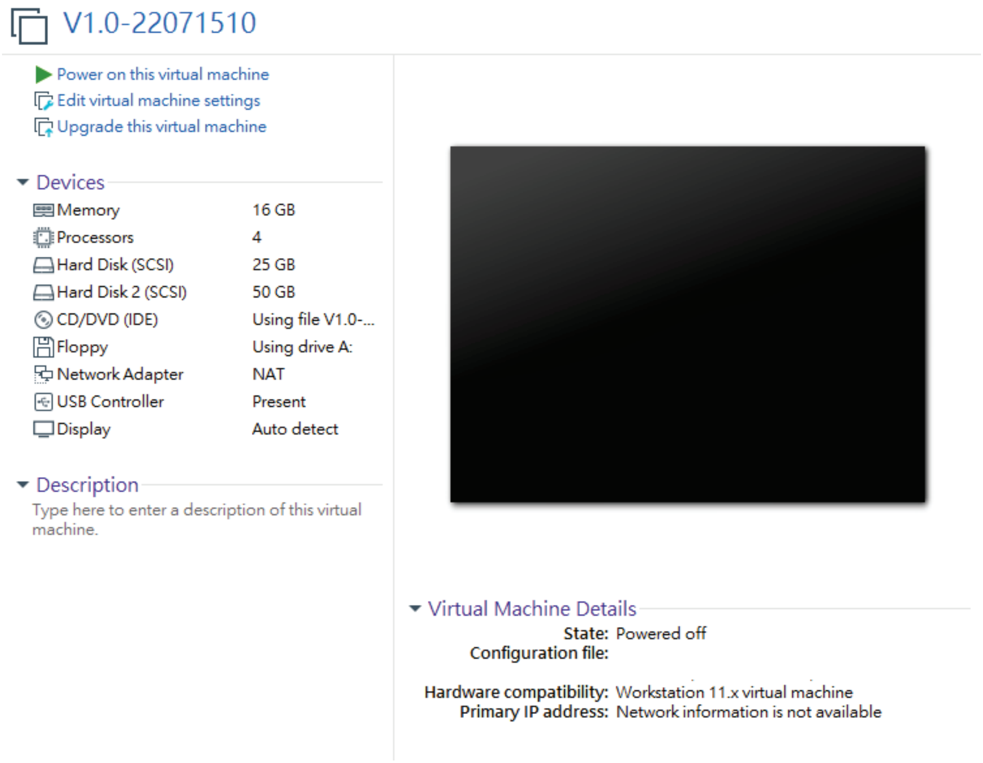
This section describes how to deploy MXsecurity to a VMware Workstation system.

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 and click **File** in the menu bar.
2. Select **Open** to import the MXsecurity VM image file (*.ova).
3. Select the MXsecurity VM image file 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.


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

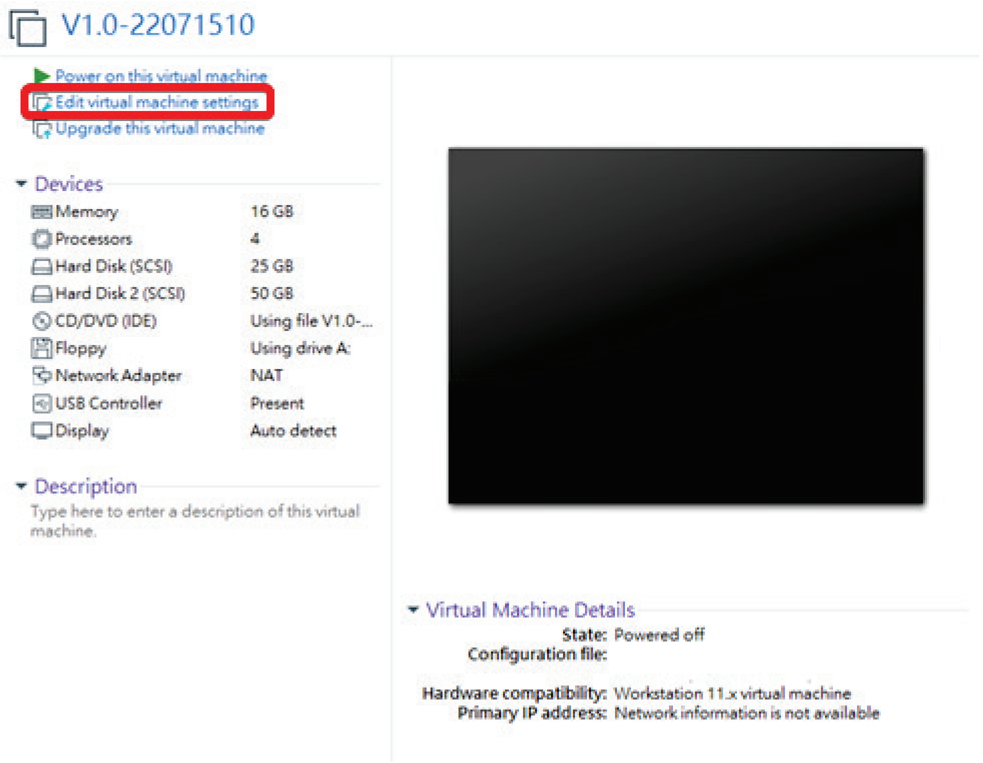
Type here to enter a description of this virtual machine.

Virtual Machine Details

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

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

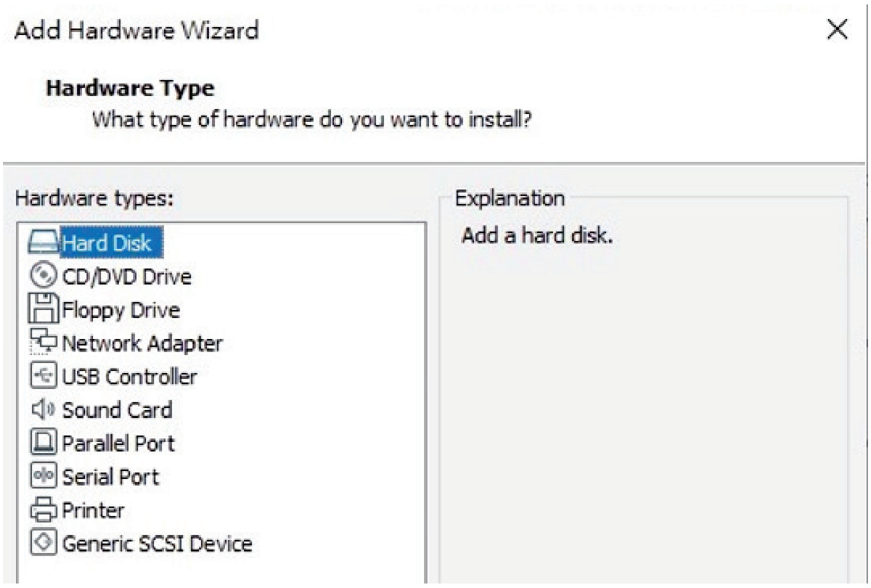
Description

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

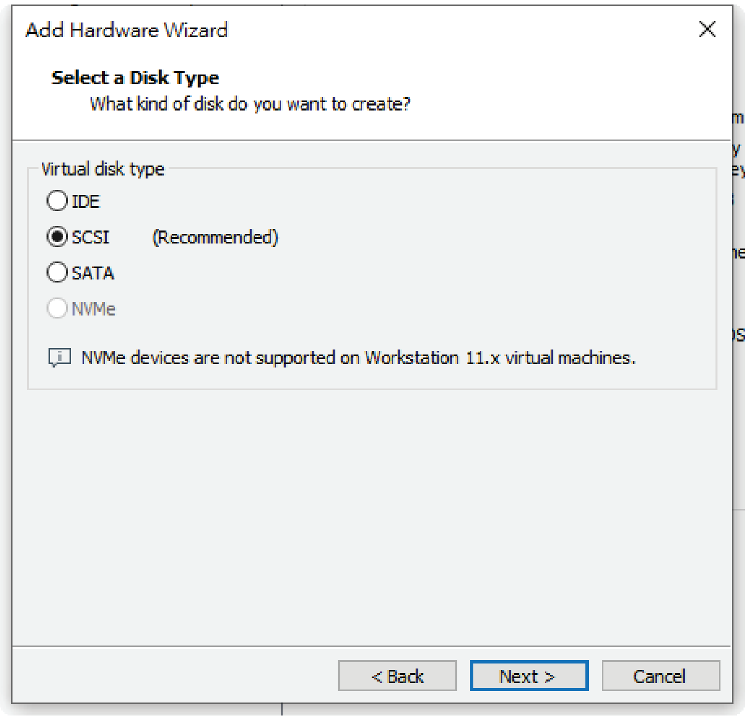
What type of hardware do you want to install?

Hardware types:

Explanation

Add a hard disk.

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



Add Hardware Wizard

Select a Disk Type

What kind of disk do you want to create?

Virtual disk type

○ IDE

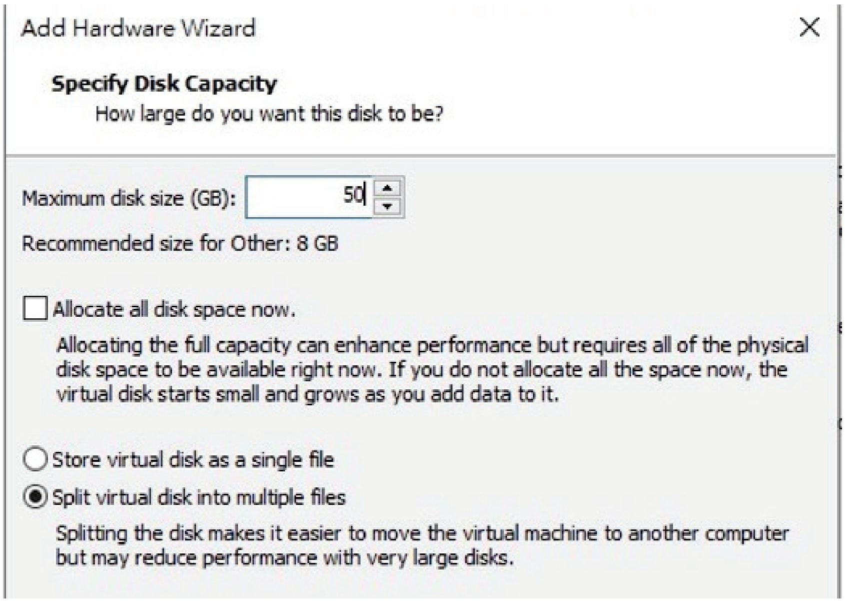
● SCSI (Recommended)

○ SATA

○ NVMe

NVMe devices are not supported on Workstation 11.x virtual machines.

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.



Add Hardware Wizard

Specify Disk Capacity

How large do you want this disk to be?

Maximum disk size (GB): 50

Recommended size for Other: 8 GB

□ Allocate all disk space now.

Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

e. Select the path to store the disk.

f. Click **Finish**.

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

i. Power off the MXsecurity instance.

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

iii. Power the MXsecurity instance back on.

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

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

b. Configure the amount of memory.

c. Configure the number of CPU cores.

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

Installing MXsecurity on a VMware ESXi System

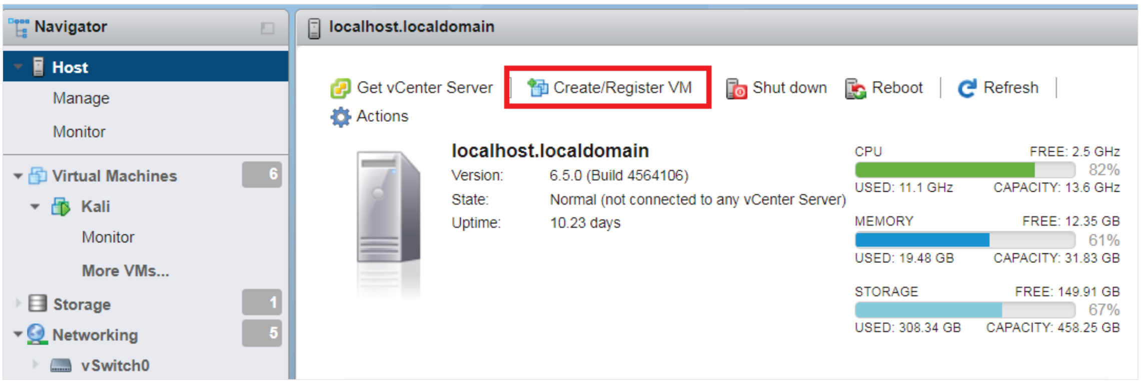
This section describes how to deploy MXsecurity to a VMware ESXi system.

Prerequisites

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

Steps:

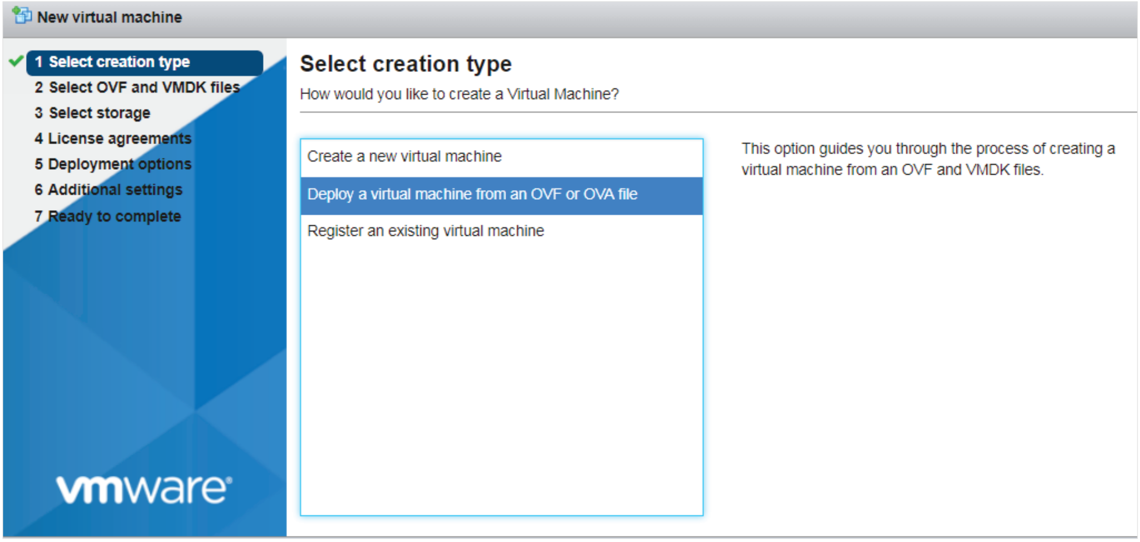
1. Log in to the VMware vSphere web client.
2. Under **Navigator**, click **Host** and then click **Create/Register VM**.



localhost.localdomain
Version: 6.5.0 (Build 4564106)
State: Normal (not connected to any vCenter Server)
Uptime: 10.23 days

CPU FREE: 2.5 GHz 82% USED: 11.1 GHz CAPACITY: 13.6 GHz
MEMORY FREE: 12.35 GB 61% USED: 19.48 GB CAPACITY: 31.83 GB
STORAGE FREE: 149.91 GB 67% USED: 308.34 GB CAPACITY: 458.25 GB

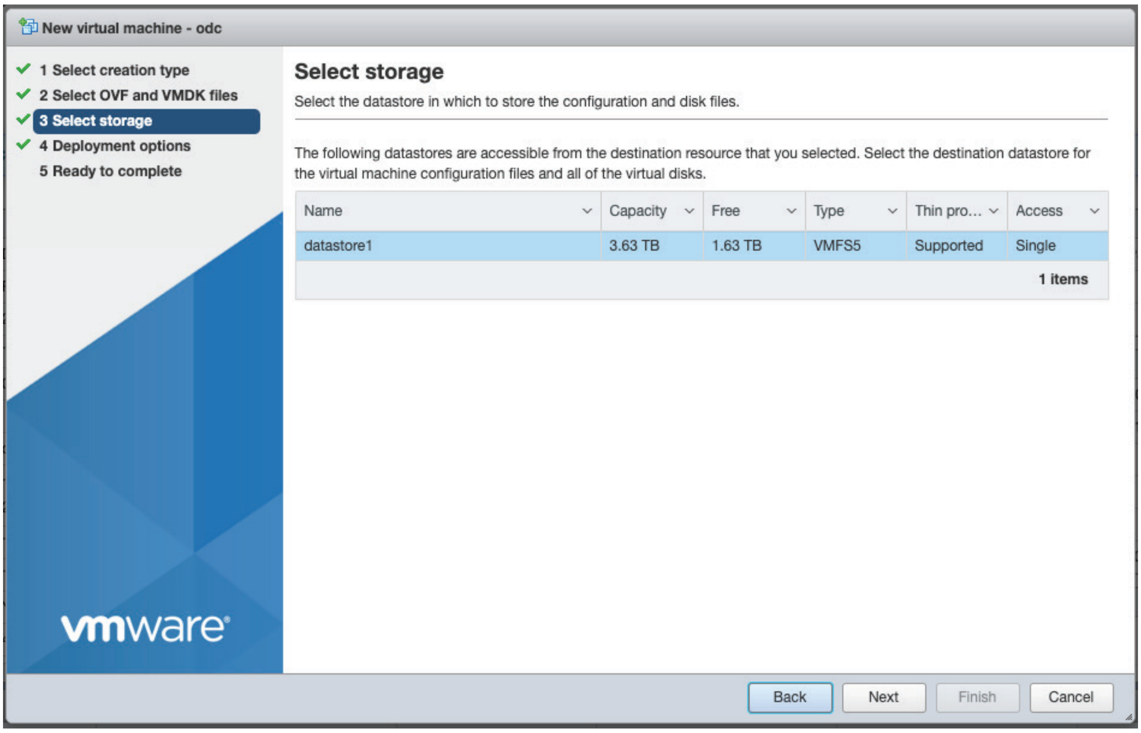
3. Select **Deploy a virtual machine from an OVF or OVA file**.



Select creation type
How would you like to create a Virtual Machine?

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

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.



Select storage

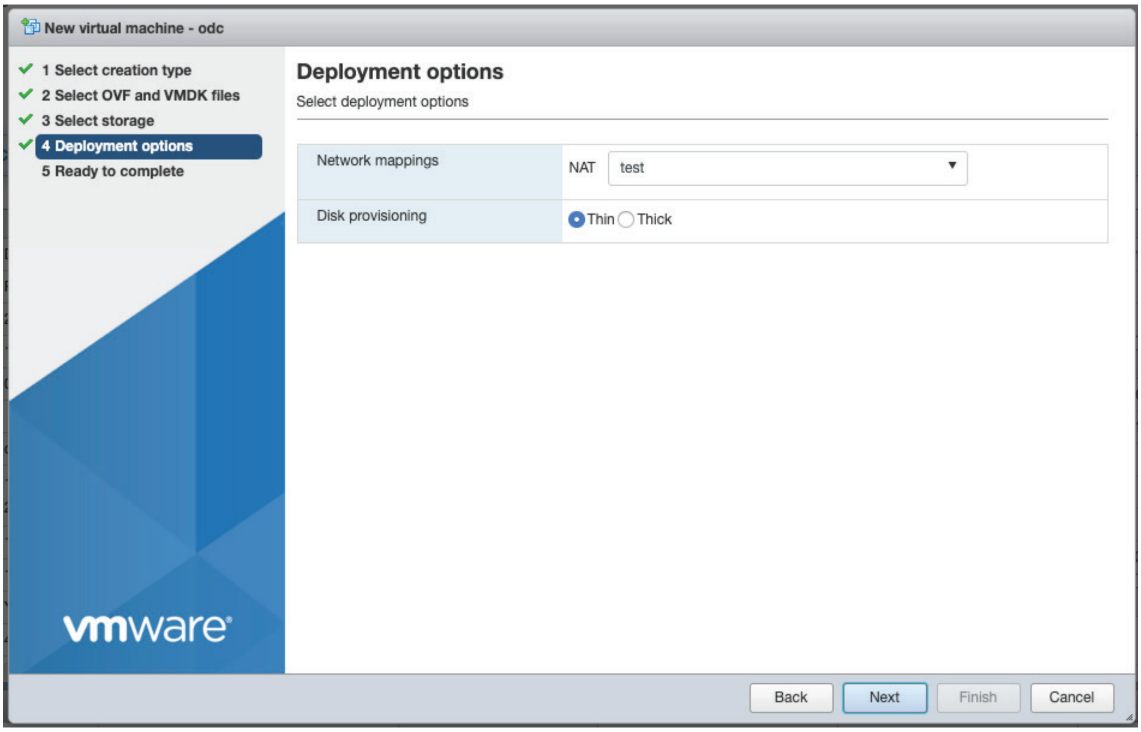
Select the datastore in which to store the configuration and disk files.

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	3.63 TB	1.63 TB	VMFS5	Supported	Single

1 items

6. Select the deployment options.

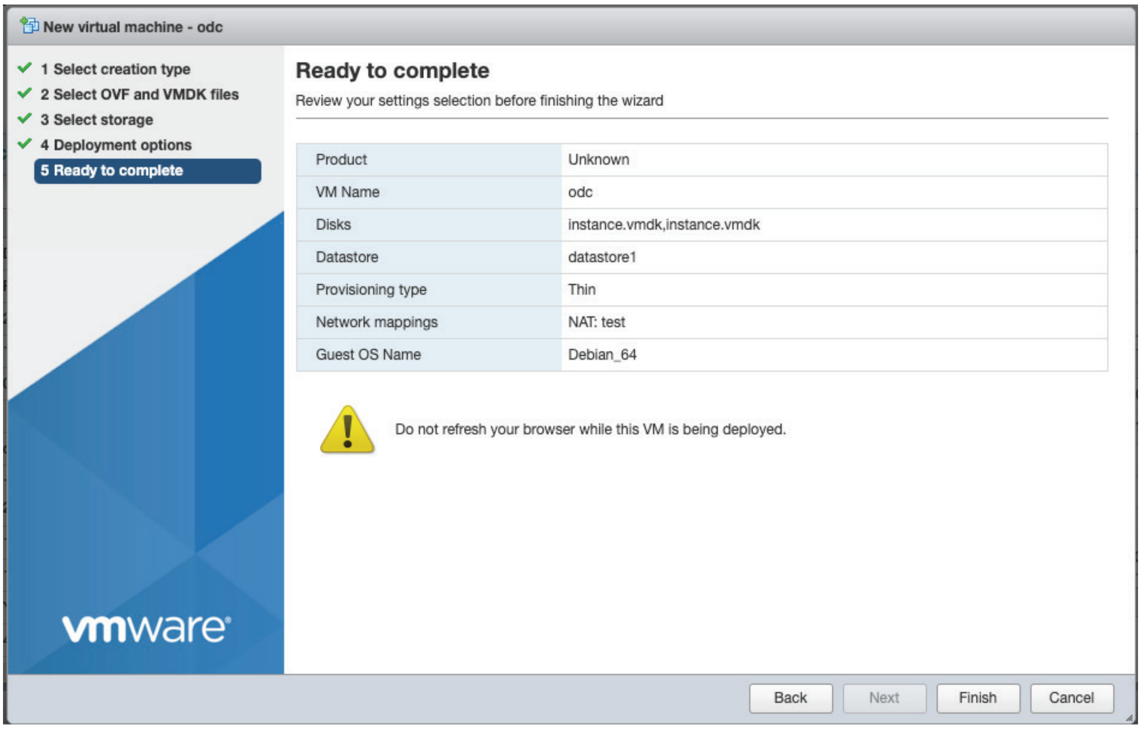


Deployment options

Select deployment options

Network mappings	NAT test ▾
Disk provisioning	● Thin ○ Thick

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



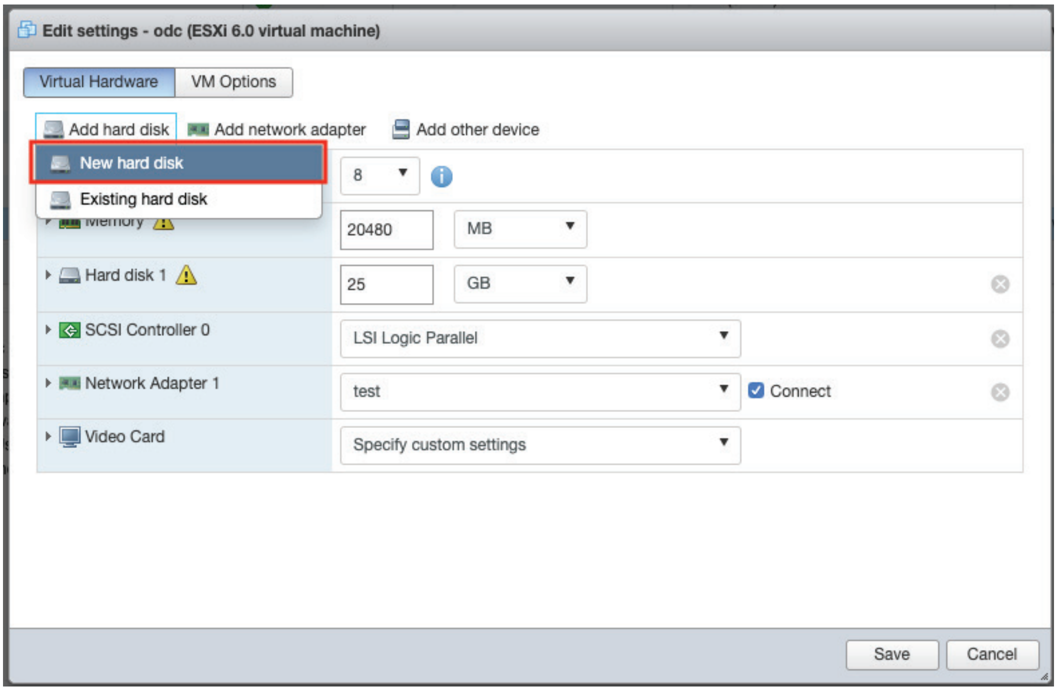
Ready to complete

Review your settings selection before finishing the wizard

Product	Unknown
VM Name	odc
Disks	instance.vmdk,instance.vmdk
Datastore	datastore1
Provisioning type	Thin
Network mappings	NAT: test
Guest OS Name	Debian_64

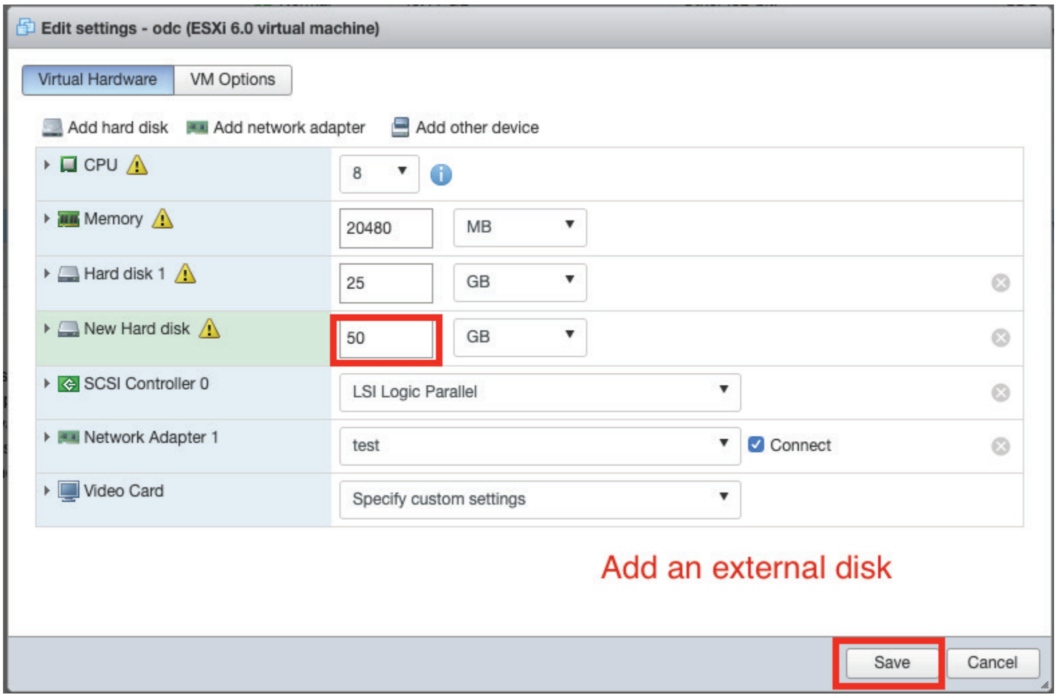
Do not refresh your browser while this VM is being deployed.

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**.



	8	
Memory	20480	MB
Hard disk 1	25	GB
SCSI Controller 0	LSI Logic Parallel	
Network Adapter 1	test	☑ Connect
Video Card	Specify custom settings	

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.



Edit settings - odc (ESXi 6.0 virtual machine)

Virtual Hardware | VM Options

Add hard disk | Add network adapter | Add other device

- CPU: 8
- Memory: 20480 MB
- Hard disk 1: 25 GB
- New Hard disk: 50 GB
- SCSI Controller 0: LSI Logic Parallel
- Network Adapter 1: test ☑ Connect
- Video Card: Specify custom settings

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

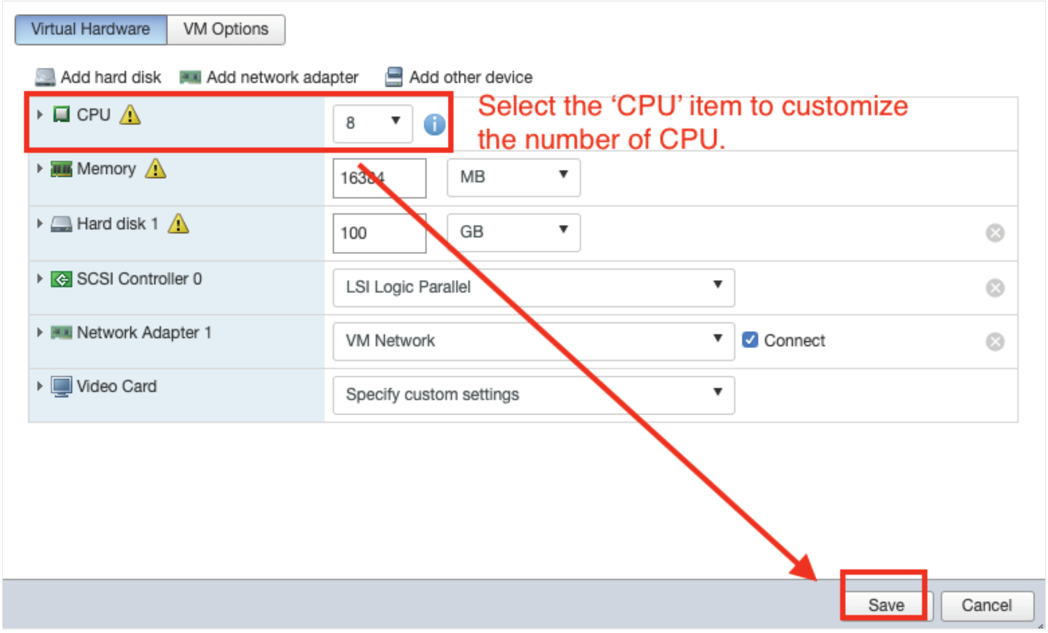
If you want to migrate the existing MXsecurity settings to the newly launched VM, please refer to Migrating to a Newer Version of MXsecurity.

NOTE

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

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

       The **Edit settings** window appears.
    b. Configure the number of CPU cores.



CPU: 8

Memory: 16384 MB

Hard disk 1: 100 GB

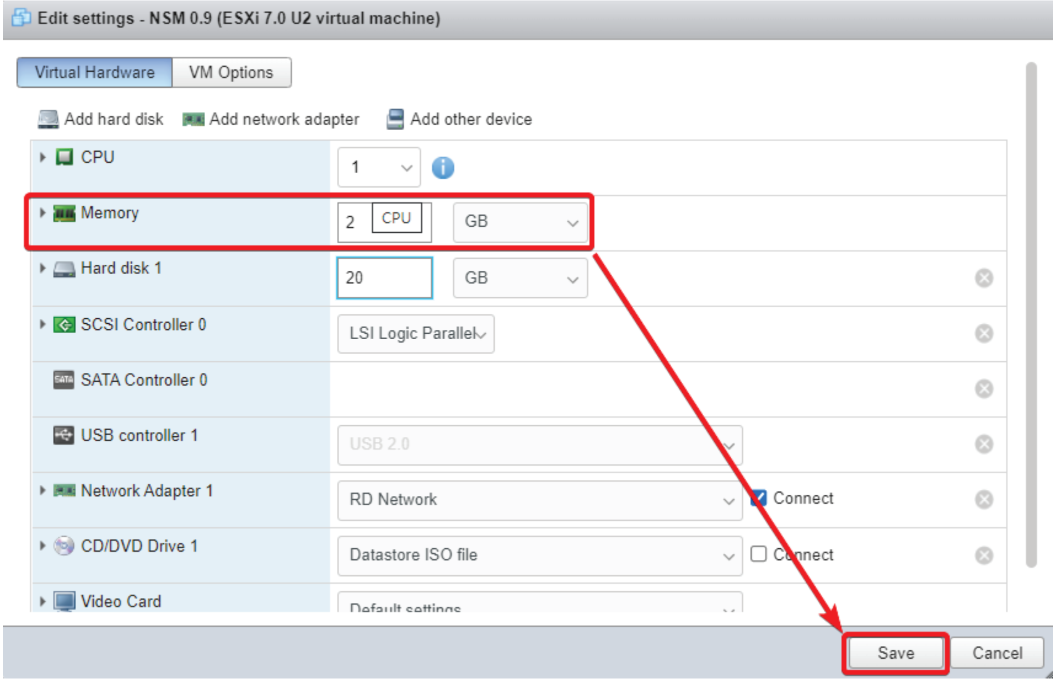
SCSI Controller 0: LSI Logic Parallel

Network Adapter 1: VM Network ☑ Connect

Video Card: Specify custom settings

Select the ‘CPU’ item to customize the number of CPU.

c. Configure the amount of memory.



Edit settings - NSM 0.9 (ESXi 7.0 U2 virtual machine)

CPU: 1

Memory: 2 CPU GB

Hard disk 1: 20 GB

SCSI Controller 0: LSI Logic Parallel

SATA Controller 0

USB controller 1: USB 2.0

Network Adapter 1: RD Network ☑ Connect

CD/DVD Drive 1: Datastore ISO file □ Connect

Video Card: Default settings

d. Click **Save**.

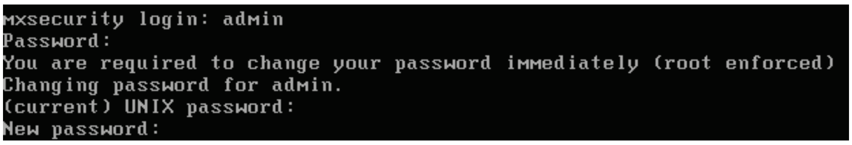
e. Boot the MXsecurity instance.

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

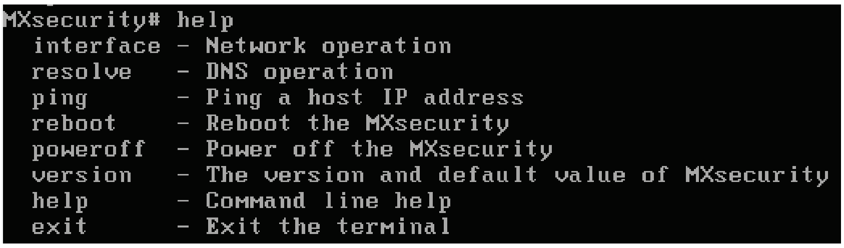
➢ The new password cannot be the same as the old password

➢ 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.

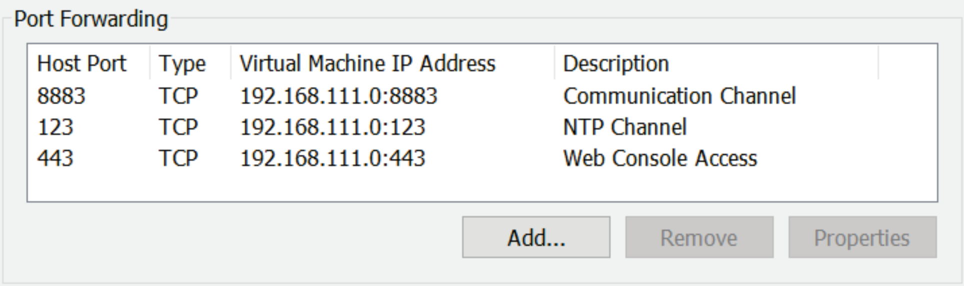


```
MXsecurity# help
  interface - Network operation
  resolve   - DNS operation
  ping      - Ping a host IP address
  reboot    - Reboot the MXsecurity
  poweroff  - Power off the MXsecurity
  version   - The version and default value of MXsecurity
  help      - Command line help
  exit      - Exit 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 TCP port 123 to the MXsecurity server IP TCP port 123.
      iii. To access the web management console, forward packets from host TCP port 443 to the MXsecurity server IP TCP port 443.



Port Forwarding

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

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. 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.

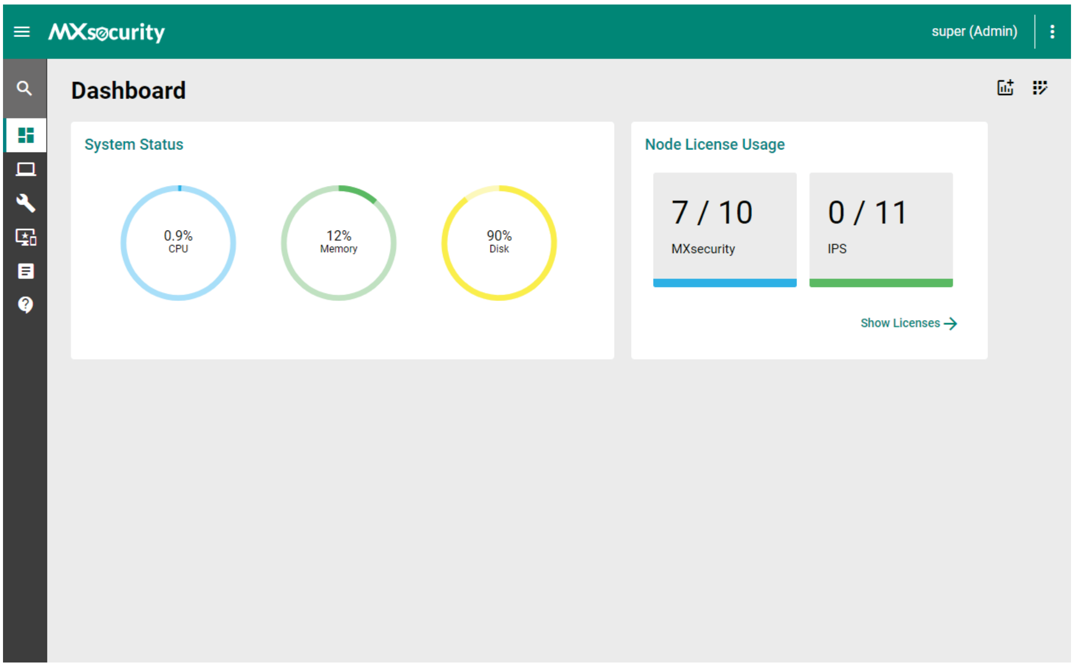
NOTE

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.

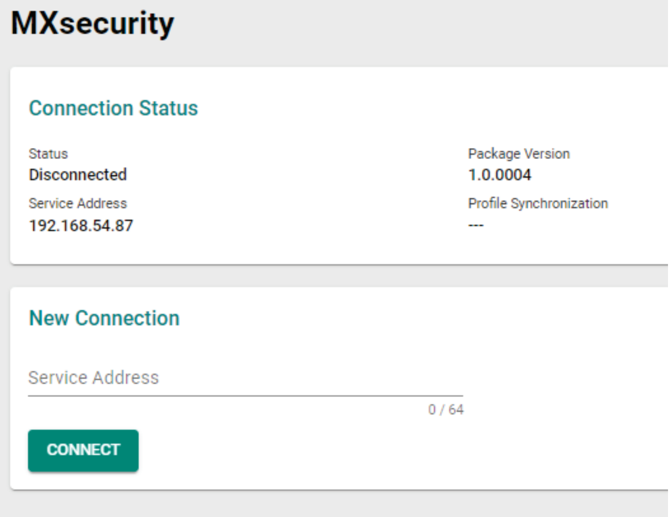


Connecting EDR-G9010 Series Devices to MXsecurity

To manage EDR-G9010 Series devices through MXsecurity, the device needs to be synced to MXsecurity.

Steps:

1. Open a web browser and navigate to the EDR-G9010 device'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.



MXsecurity

Connection Status

Status
Disconnected

Package Version
1.0.0004

Service Address
192.168.54.87

Profile Synchronization

New Connection

Service Address

0 / 64

4. Click **CONNECT**.

4. 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

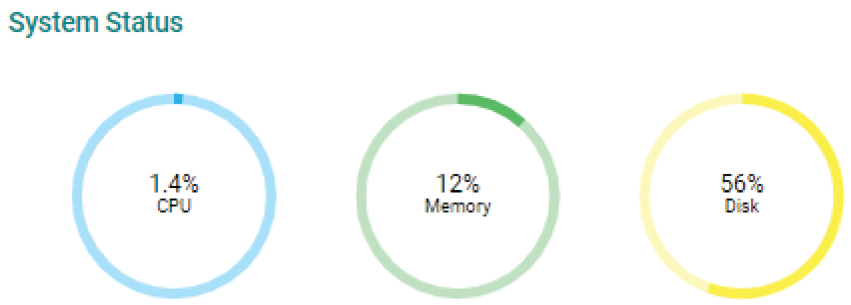
The amount of statistical information shown depends on your user account role and whether permission to manage each device group has been shared with you.

Dashboard Widgets Overview

This section describes available widgets on the dashboard.

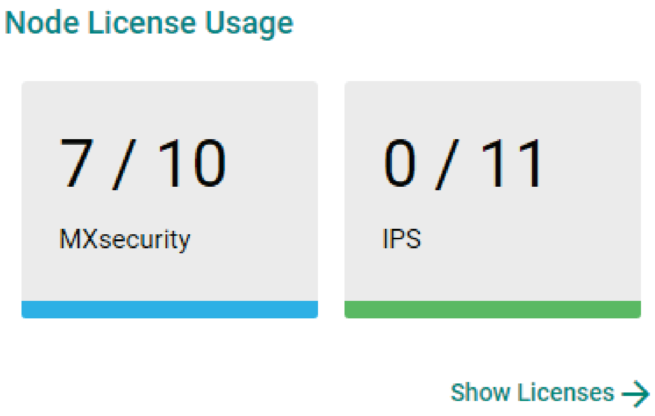
System Status

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



Node License Usage

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



Node License Usage

7 / 10

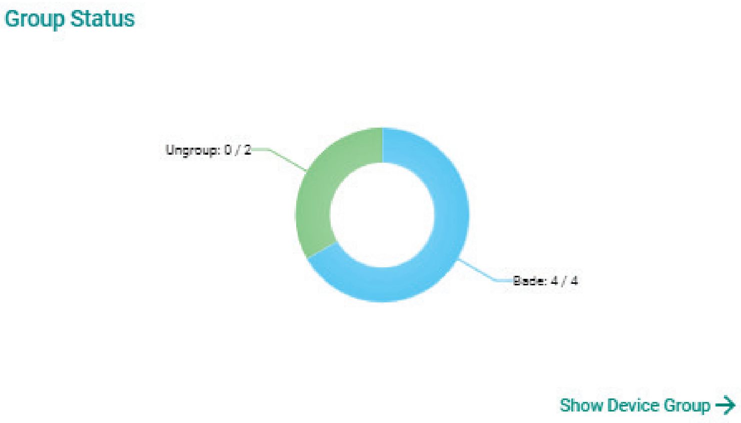
MXsecurity

0 / 11

IPS

Group Status

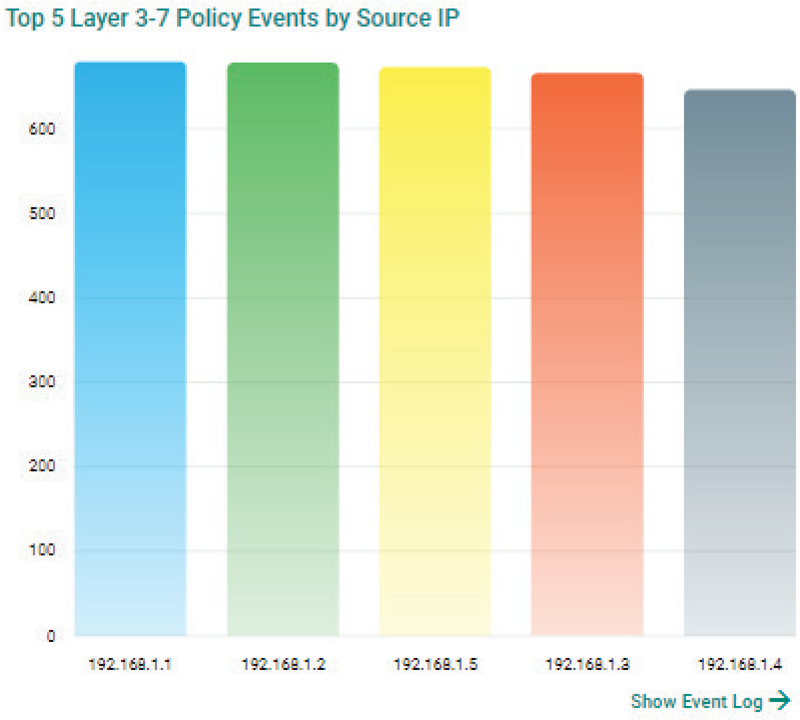
This widget lists the information of device groups and device status.



Group Status

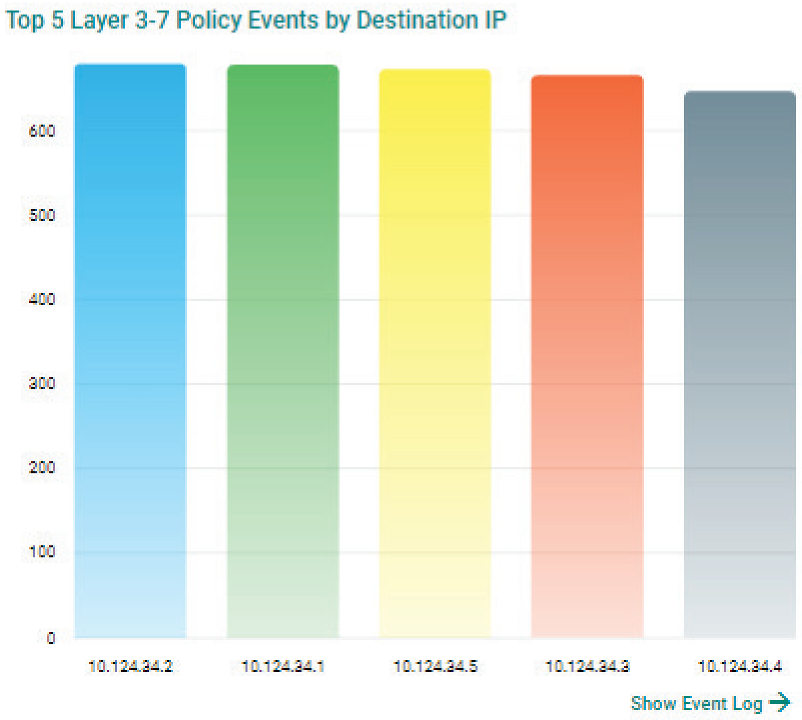
Top 5 Layer 3-7 Policy Events by Source IP

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



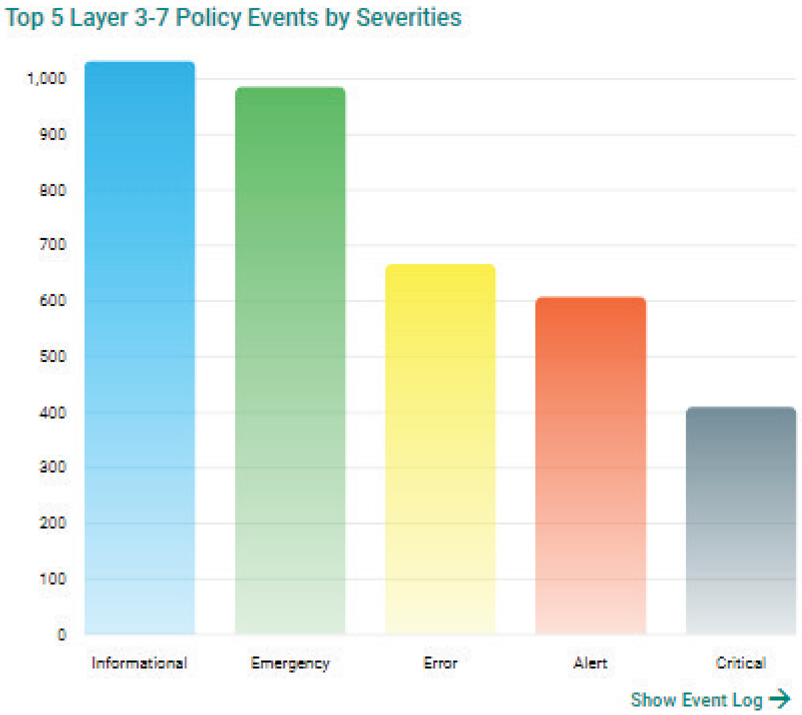
Top 5 Layer 3-7 Policy Events by Destination IP

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



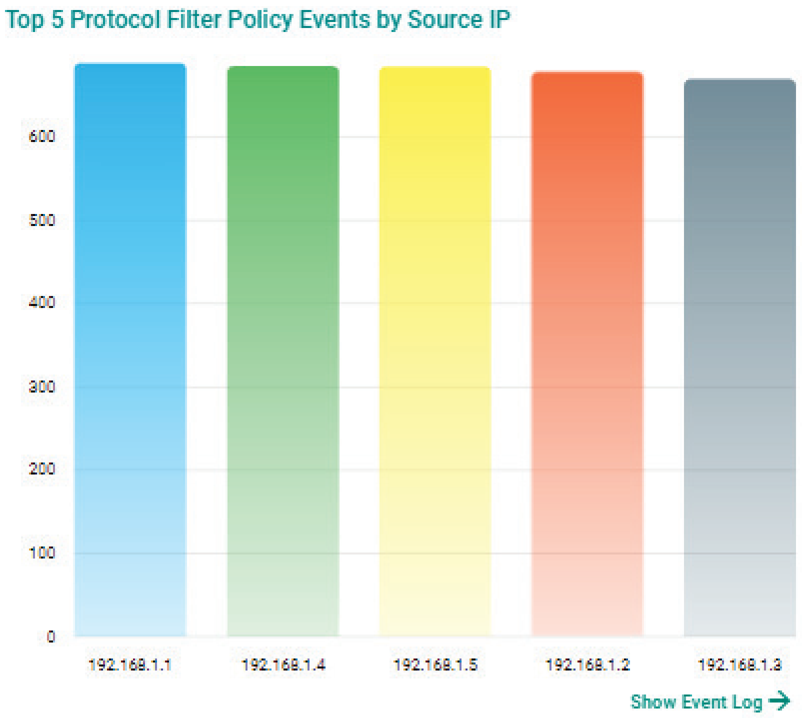
Top 5 Layer 3-7 Policy Events by Severity

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



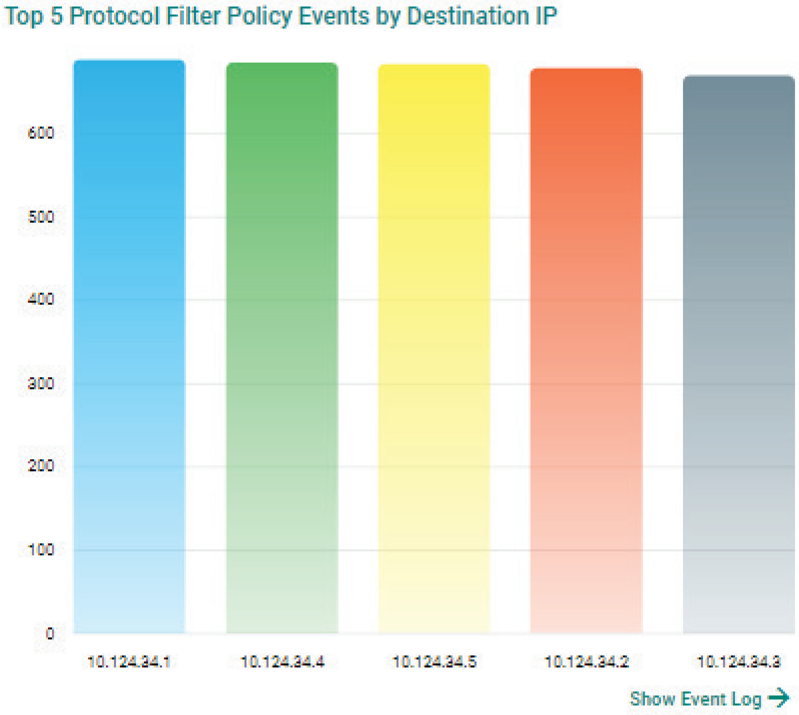
Top 5 Protocol Filter Policy Events by Source IP

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



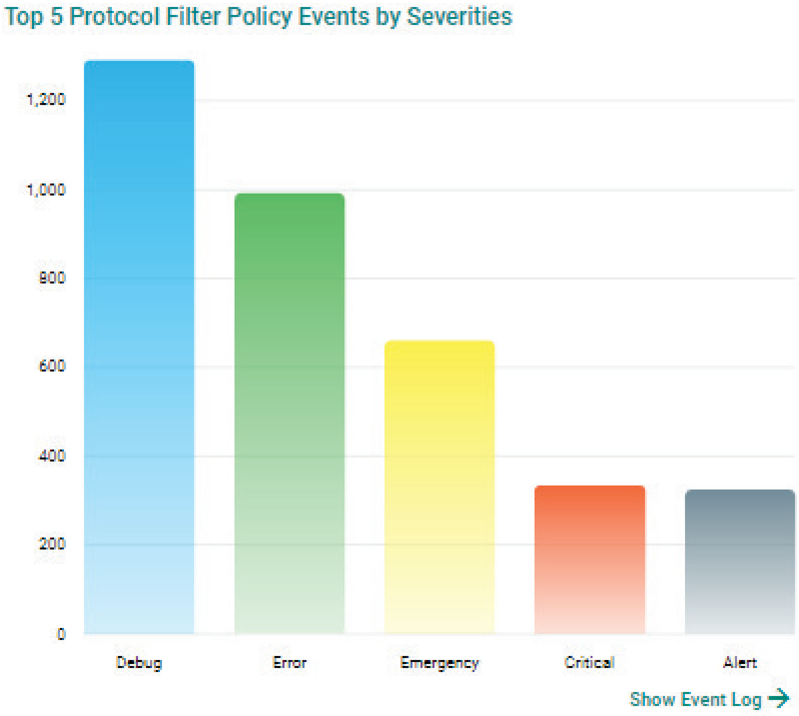
Top 5 Protocol Filter Policy Events by Destination IP

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



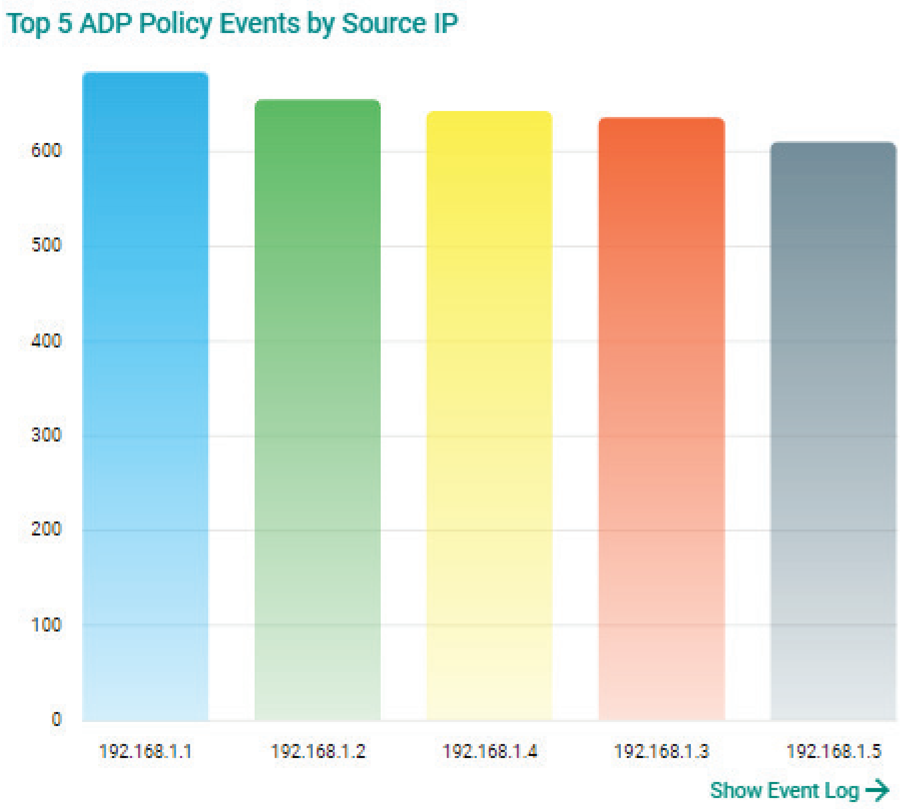
Top 5 Protocol Filter Policy Events by Severity

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



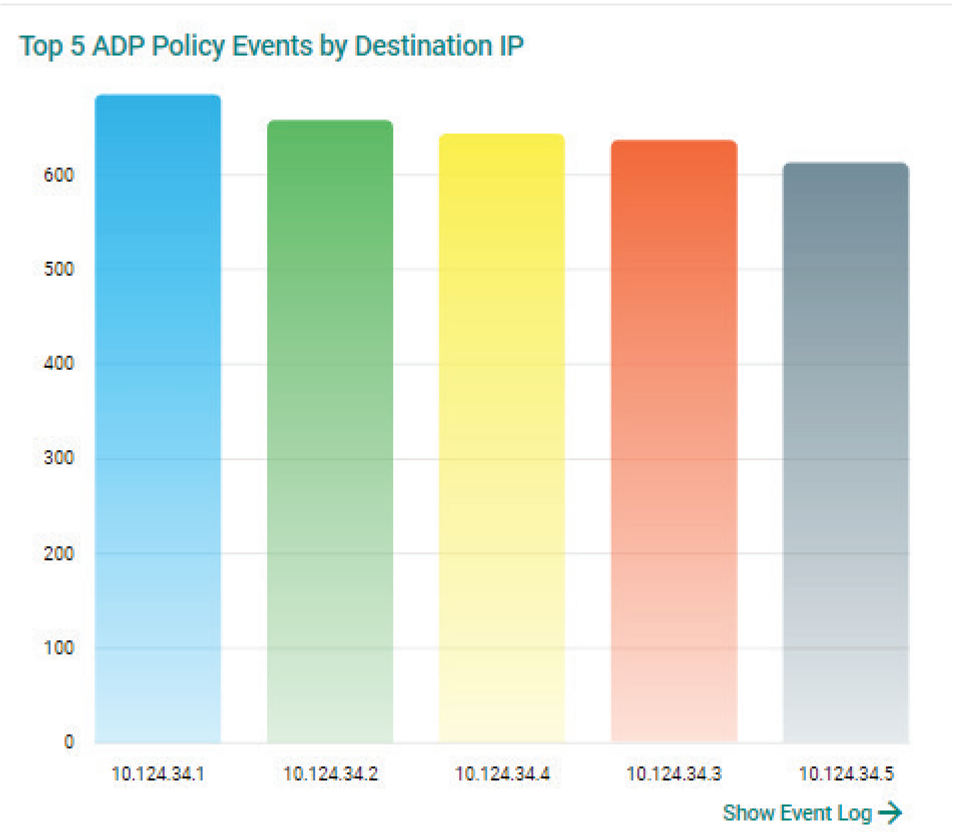
Top 5 ADP Events by Source IP

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



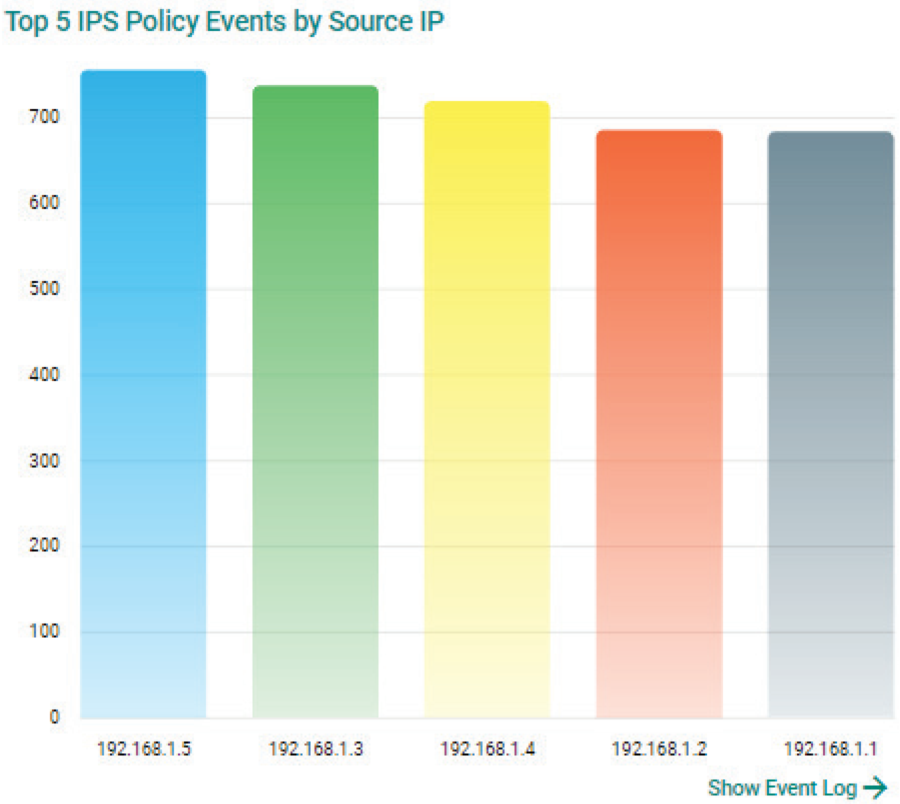
Top 5 ADP Events by Destination IP

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



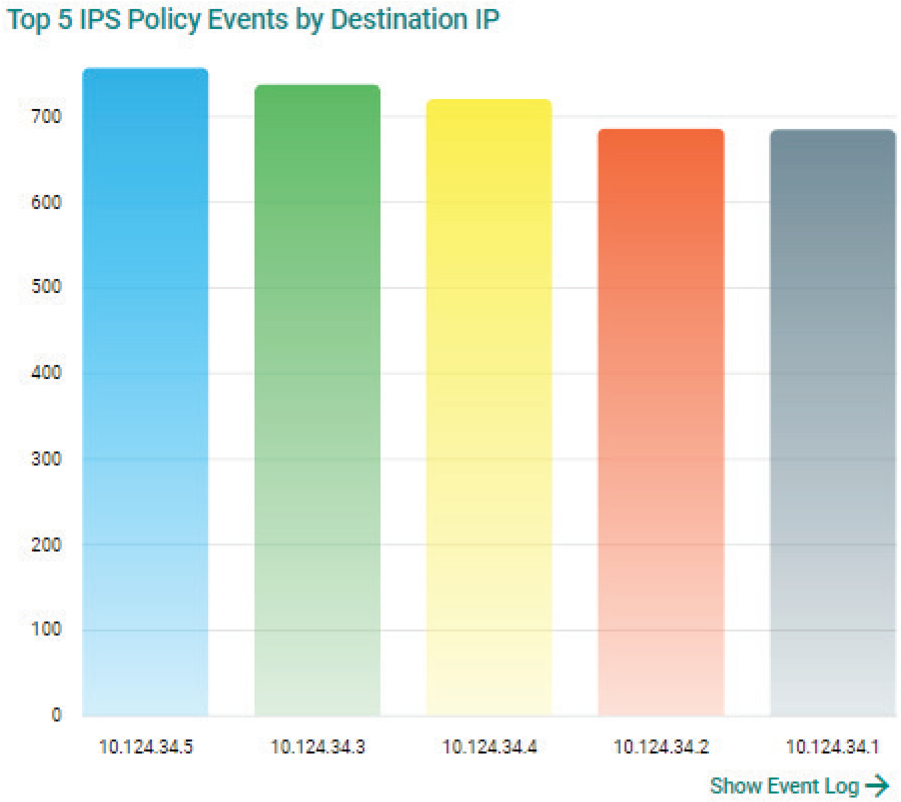
Top 5 IPS Events by Source IP

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



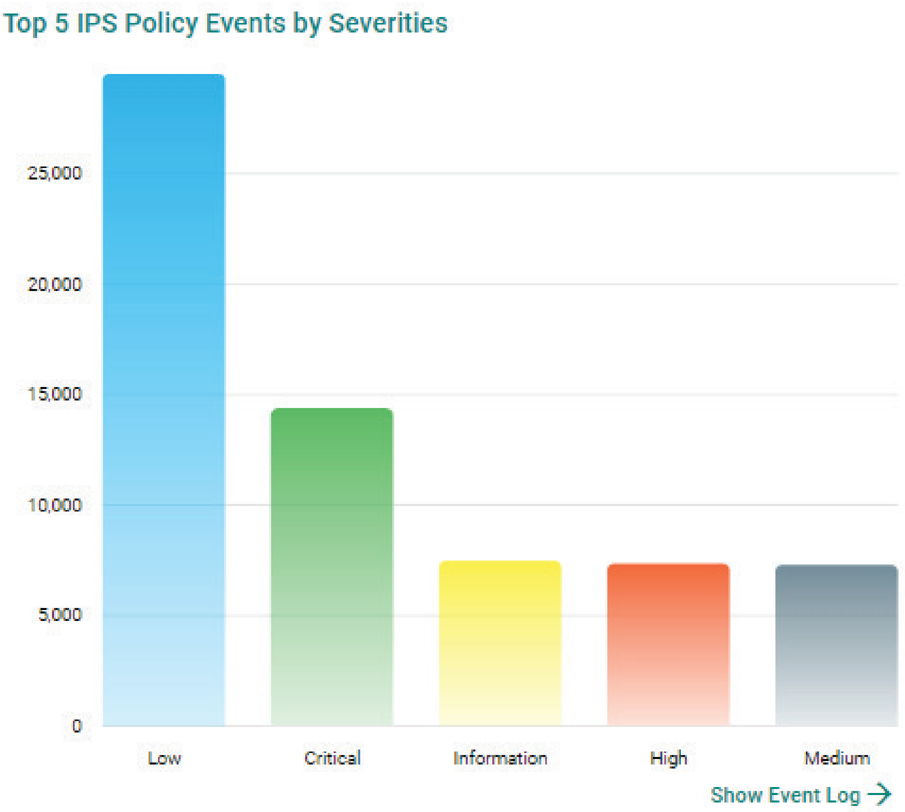
Top 5 IPS Events by Destination IP

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


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

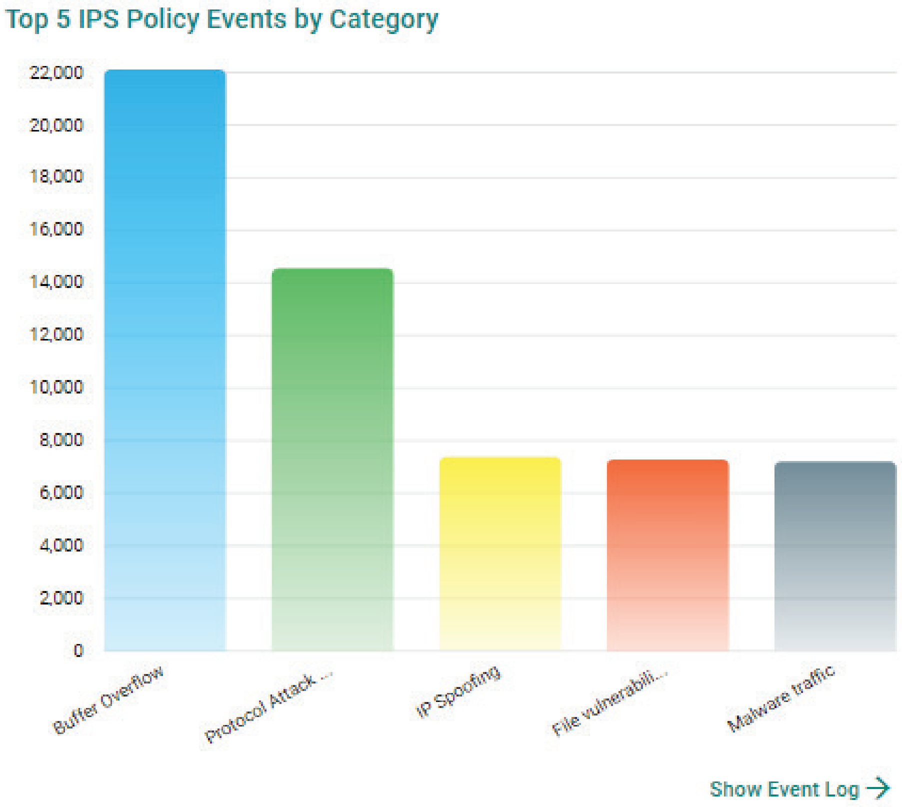
Top 5 IPS Events by Severity

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



Top 5 IPS Events by Category

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


Top 5 IPS Policy Events by Category
22,000
20,000
18,000
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
Buffer Overflow
Protocol Attack ...
IP Spoofing
File vulnerabili...
Malware traffic
Show Event Log

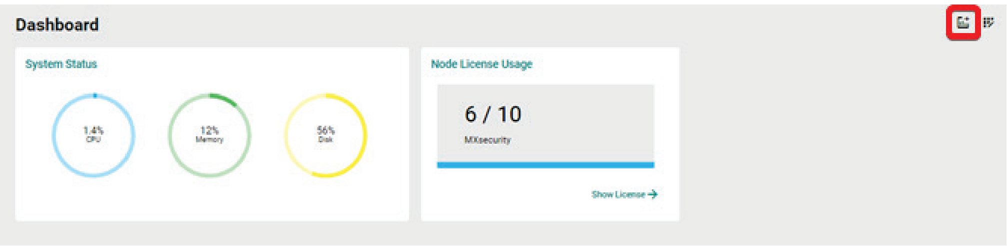
Widget Management

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

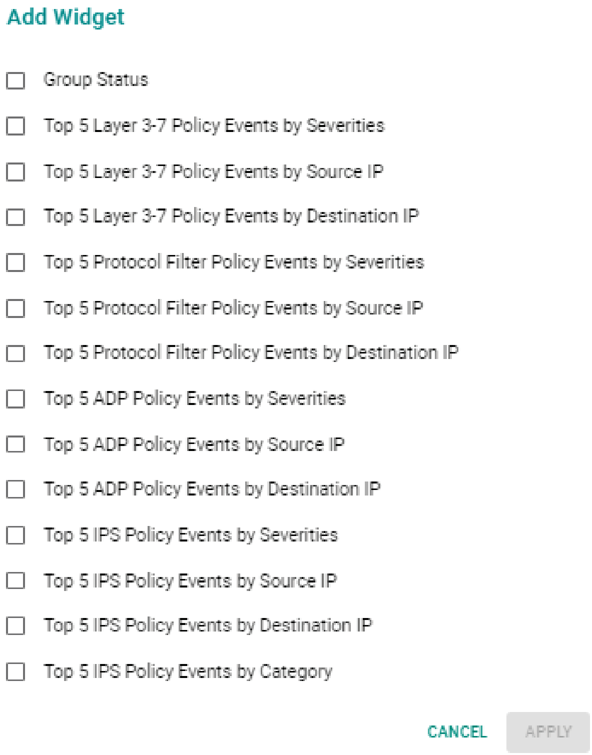
Adding a Widget to the Dashboard

Steps:

1. Click the icon to add widgets.



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



Add Widget

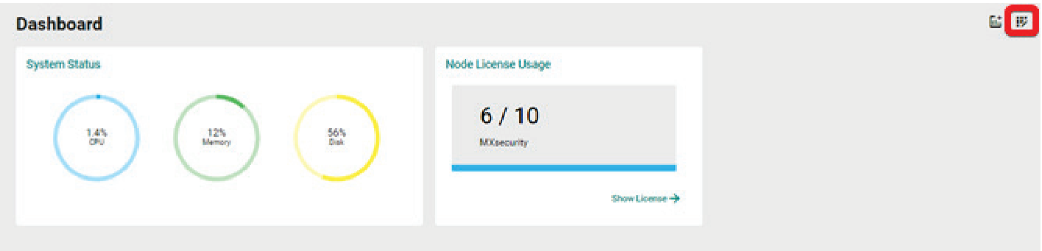
□ Group Status
□ Top 5 Layer 3-7 Policy Events by Severities
□ Top 5 Layer 3-7 Policy Events by Source IP
□ Top 5 Layer 3-7 Policy Events by Destination IP
□ Top 5 Protocol Filter Policy Events by Severities
□ Top 5 Protocol Filter Policy Events by Source IP
□ Top 5 Protocol Filter Policy Events by Destination IP
□ Top 5 ADP Policy Events by Severities
□ Top 5 ADP Policy Events by Source IP
□ Top 5 ADP Policy Events by Destination IP
□ Top 5 IPS Policy Events by Severities
□ Top 5 IPS Policy Events by Source IP
□ Top 5 IPS Policy Events by Destination IP
□ Top 5 IPS Policy Events by Category

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

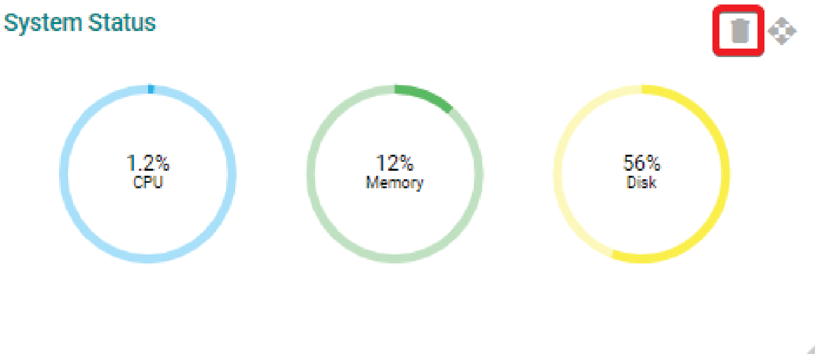
Removing a Widget from the Dashboard

Steps:

1. Click the icon to edit the dashboard.



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

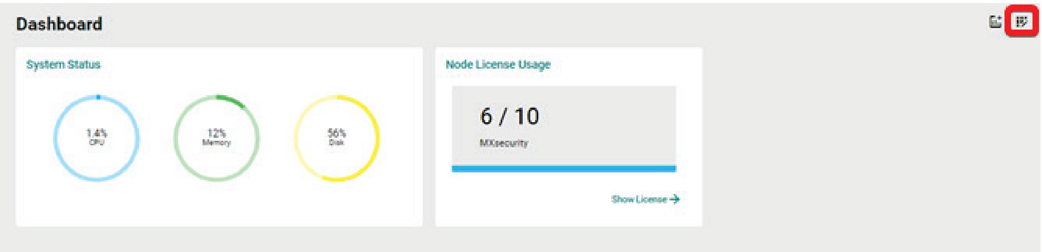


3. Click the icon again to save your changes and leave edit mode.

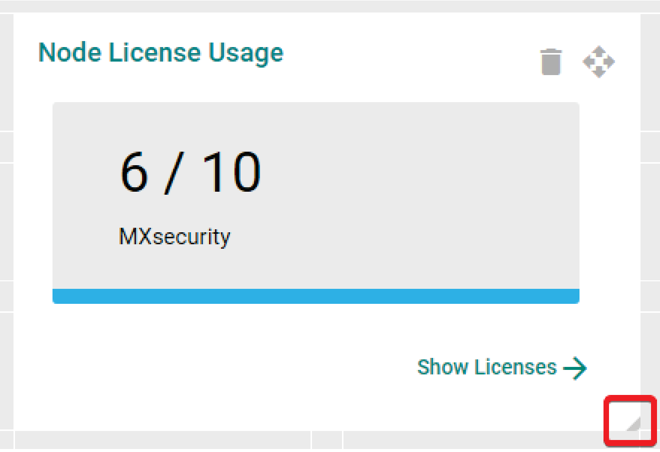
Resizing a Widget

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.



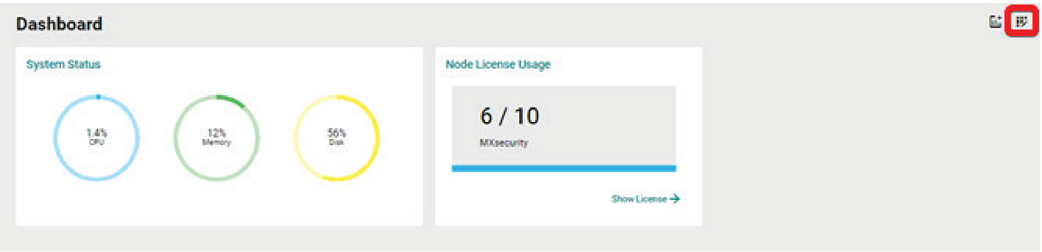
3. Click and drag the corner of the widget to the desired size, then release the mouse. The dark grey area in the Dashboard background indicates the final size of the widget.

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

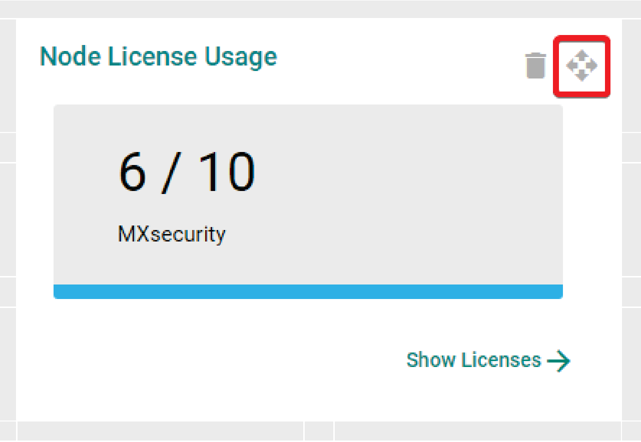
Moving the Widget Position

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.

5. Management

The Management page lets you manage device groups, and system databases for firmware software, packages, objects, and policy profiles. 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.

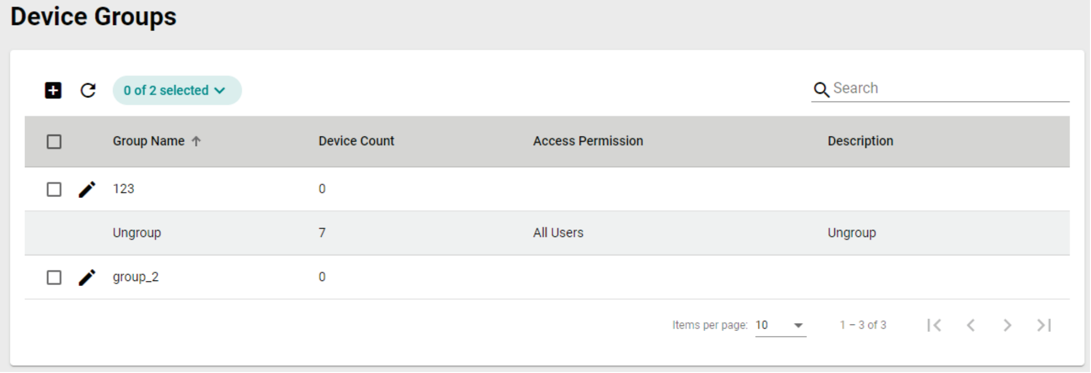
The configurations and policies that can be shared are:

- Firmware
- Software packages
- Objects
- Policy profiles

Creating a New Device Group

Steps:

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



Device Groups

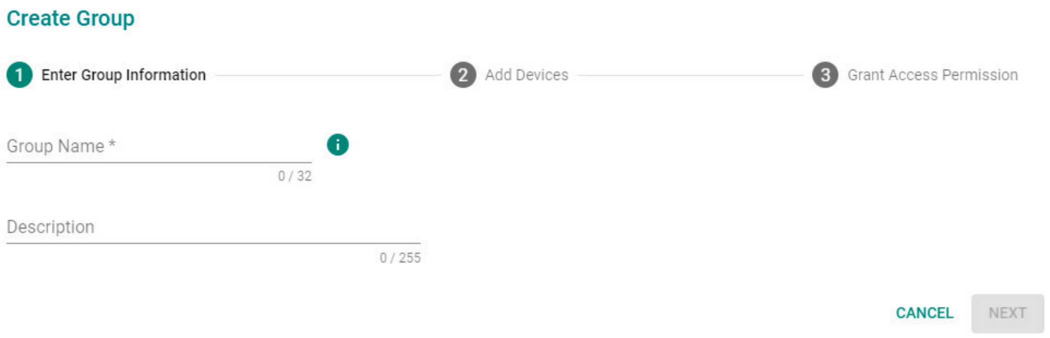
0 of 2 selected

□	Group Name	Device Count	Access Permission	Description
□	123	0		
	Ungroup	7	All Users	Ungroup
□	group_2	0		

Items per page: 10 1 – 3 of 3

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 (_).



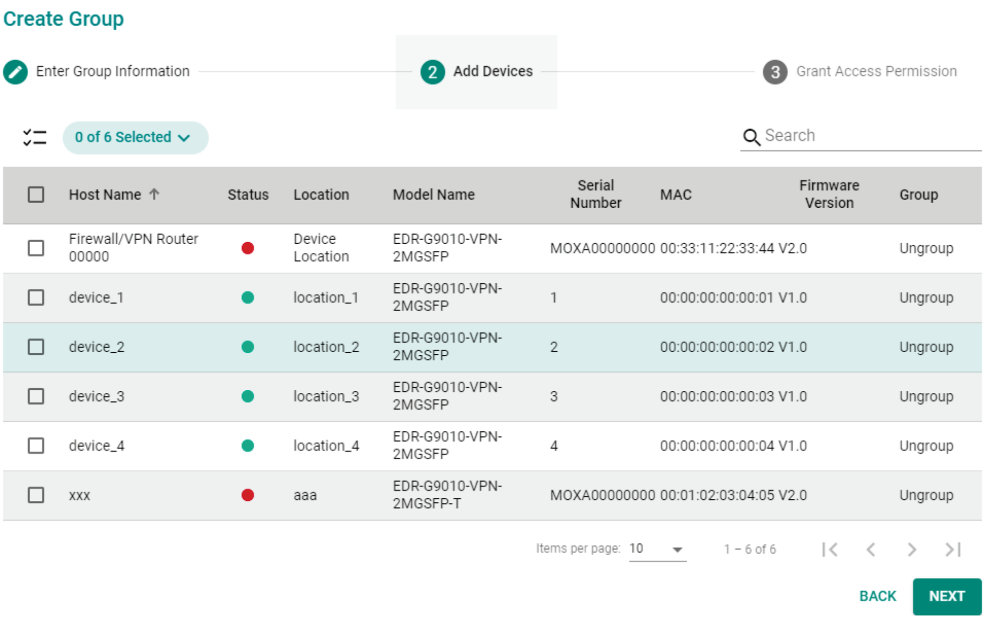
Create Group

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

Group Name * 0 / 32

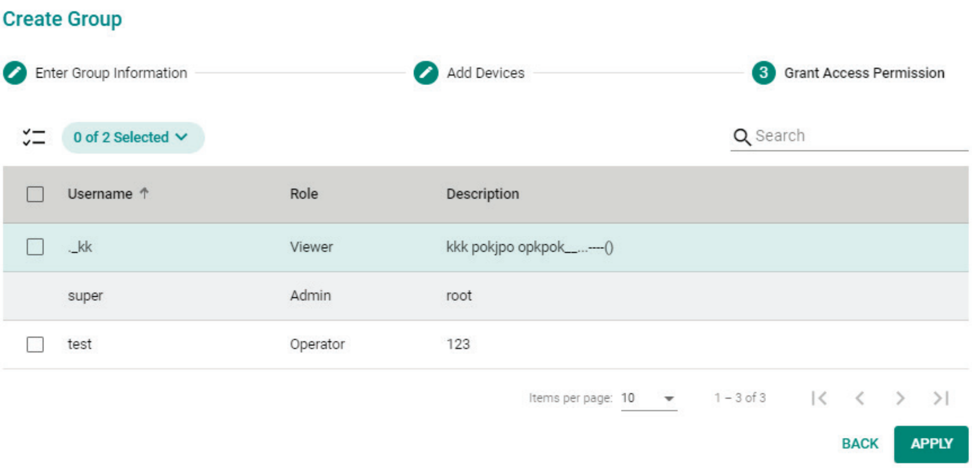
Description 0 / 255

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



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

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



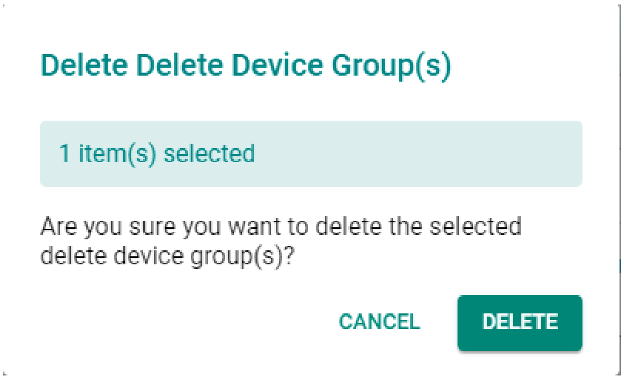
☐	Username ↑	Role	Description
☐	_kk	Viewer	kkk pokjpo opkpok__...---()
	super	Admin	root
☐	test	Operator	123

Deleting a Device Group

Steps:

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

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



Delete Delete Device Group(s)

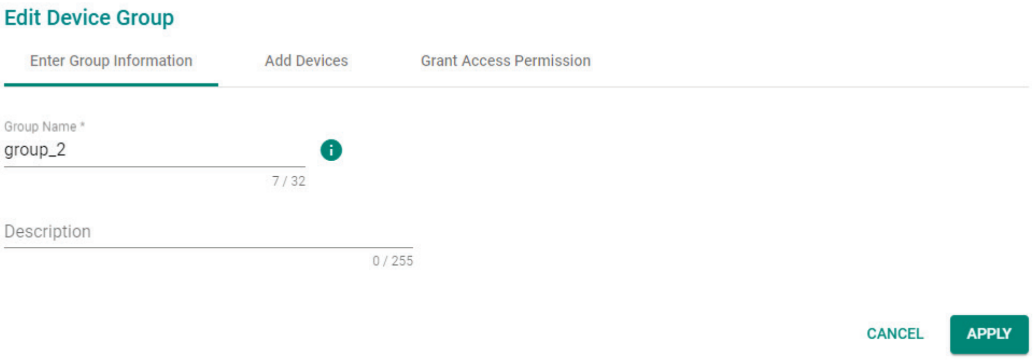
1 item(s) selected

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

Editing a Device Group

Steps:

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



Edit Device Group

Group Name *: group_2

7 / 32

Description

0 / 255

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

Firmware Management

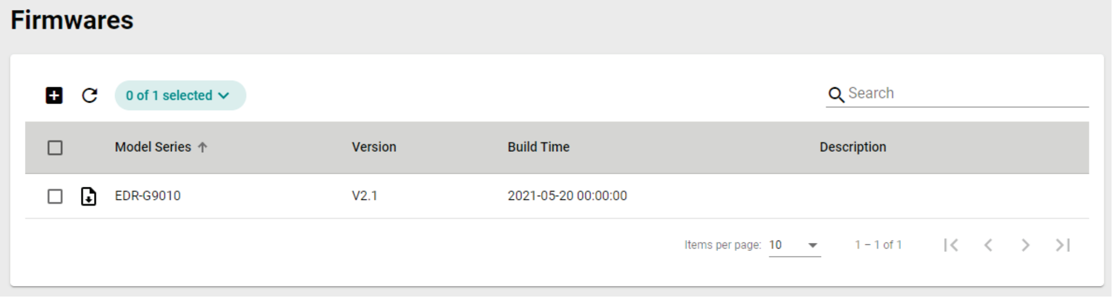
This section describes how to manage the local firmware database from MXsecurity.

Uploading a New Firmware

Steps:

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

2. Click the ➕ icon to add a new firmware.



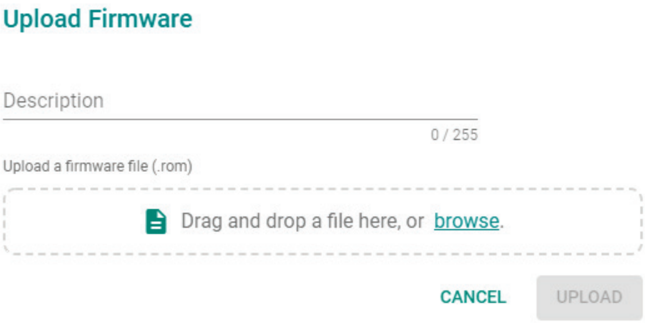
Firmwares

0 of 1 selected

☐	Model Series	Version	Build Time	Description
☐	EDR-G9010	V2.1	2021-05-20 00:00:00	

Items per page: 10 1 – 1 of 1

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)

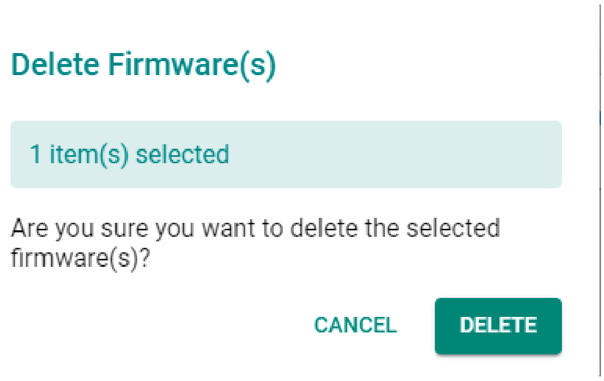
Drag and drop a file here, or browse.

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)?

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.

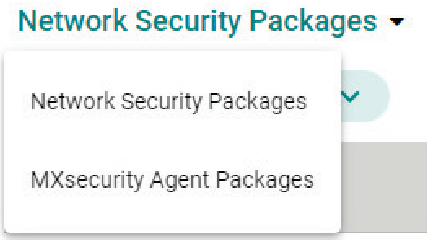
The following packages can be managed in MXsecurity:

- Network Security Package
- MXsecurity Agent packages

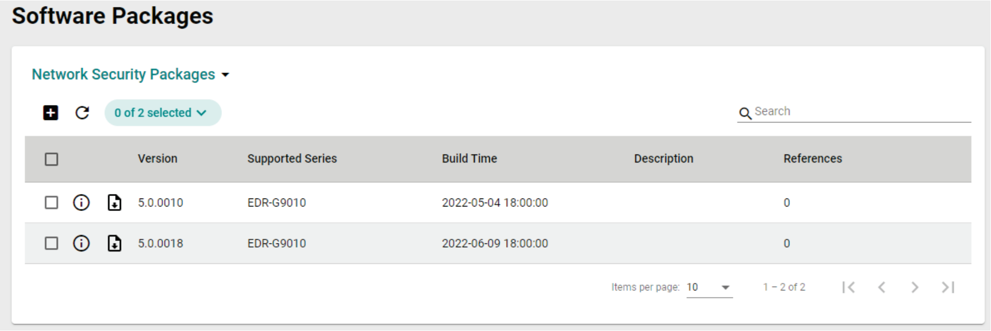
Uploading a New Software Package

Steps:

1. Navigate to **Management > Software Packages**.
2. Select the software package type from the drop-down menu.


Network Security Packages ▾
Network Security Packages
MXsecurity Agent Packages

3. Click the ⊞ icon to upload a new software package.



Software Packages

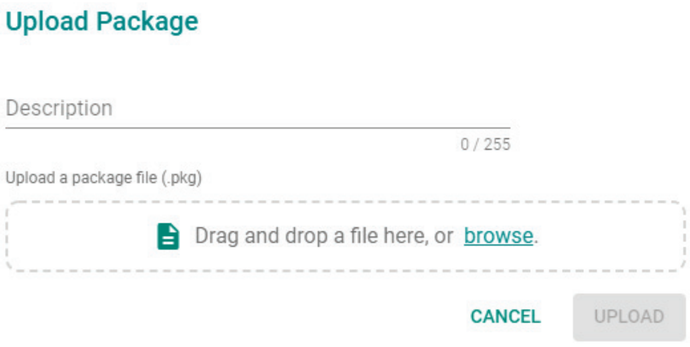
Network Security Packages ▾

⊞ ⟳ 0 of 2 selected ⌄ Search

□		Version	Supported Series	Build Time	Description	References
□	ⓘ ⤓	5.0.0010	EDR-G9010	2022-05-04 18:00:00		0
□	ⓘ ⤓	5.0.0018	EDR-G9010	2022-06-09 18:00:00		0

Items per page: 10 ▾ 1 – 2 of 2 |< < > >|

4. 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.

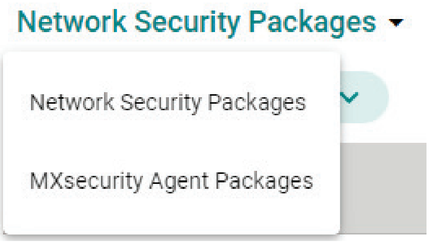
CANCEL UPLOAD

5. Click **UPLOAD**.

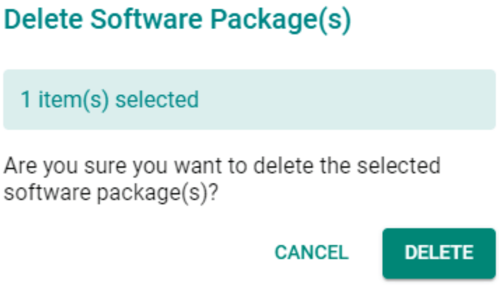
Deleting a Software Package

Steps:

1. Navigate to **Management > Software Packages**.
2. Select the software package type from the drop-down menu.


Network Security Packages
Network Security Packages
MXsecurity Agent Packages

3. Check the box of the package(s) you want to delete.
4. Click the 🗑 icon to delete the selected software package(s).
5. When prompted to confirm, click **DELETE**.



Delete Software Package(s)

1 item(s) selected

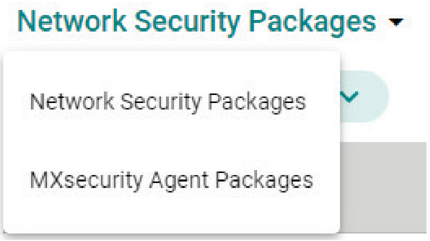
Are you sure you want to delete the selected software package(s)?

Exporting Software Packages

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

Steps:

1. Navigate to **Management > Software Packages**.
2. Select the software package type from the drop-down menu.


Network Security Packages
Network Security Packages
MXsecurity Agent Packages

3. Click the ⤓ icon to download the software packages.

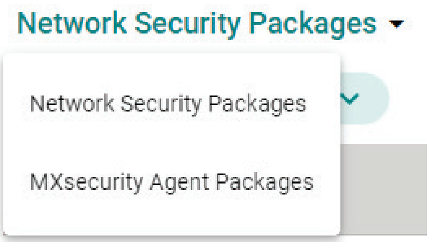
Viewing Detailed Information of a Software Package

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

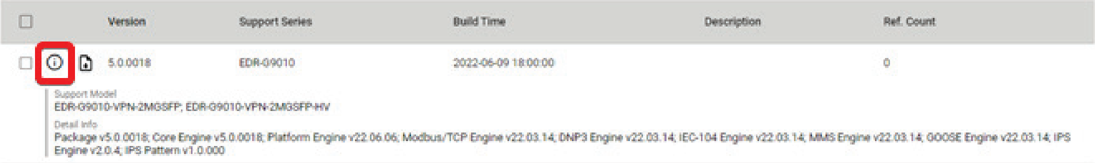
Steps:

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

2. Select the software package type from the drop-down menu.


Network Security Packages
Network Security Packages
MXsecurity Agent Packages

3. Click the ⓘ icon to show detailed information for the software package.



□	Version	Support Series	Build Time	Description	Ref. Count
□ ⓘ	5.0.0018	EDR-G9010	2022-06-09 18:00:00		0

Support Model
EDR-G9010-VPN-2MGSFP; EDR-G9010-VPN-2MGSFP-HV

Detail Info
Package v5.0.0018; Core Engine v5.0.0018; Platform Engine v22.06.06; Modbus/TCP Engine v22.03.14; DNP3 Engine v22.03.14; IEC-104 Engine v22.03.14; MMS Engine v22.03.14; GOOSE Engine v22.03.14; IPS Engine v2.0.4; IPS Pattern v1.0.000

Object Management

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

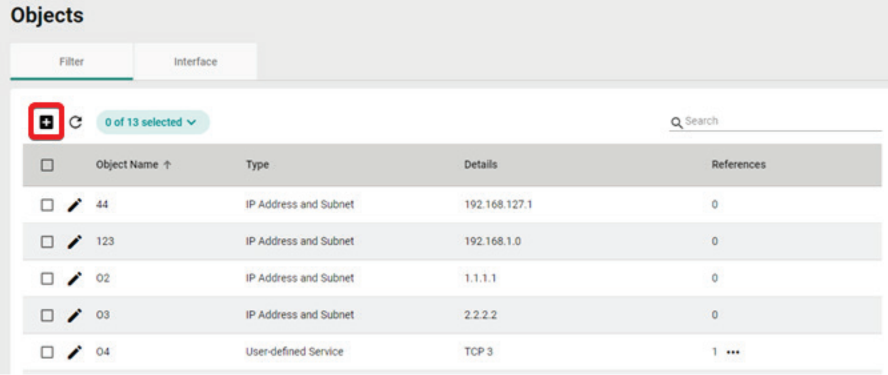
You can configure the following types of objects in MXsecurity:

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

Creating a New Filter Object

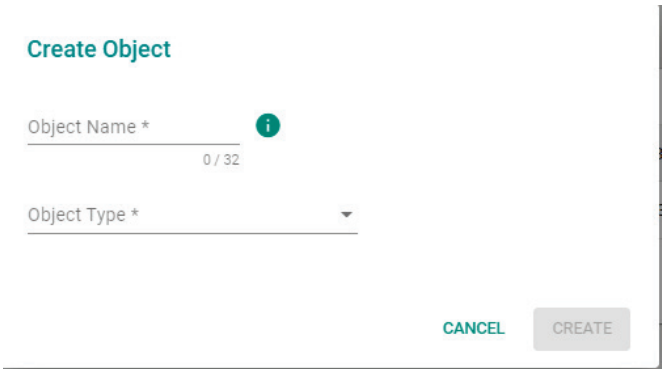
Steps:

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

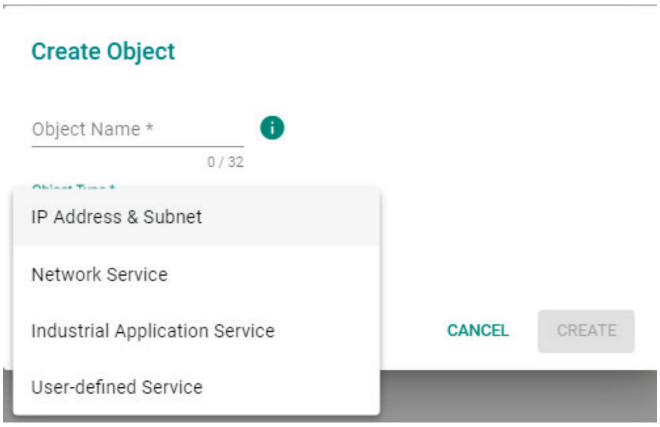


□	Object Name ↑	Type	Details	References
□	44	IP Address and Subnet	192.168.127.1	0
□	123	IP Address and Subnet	192.168.1.0	0
□	02	IP Address and Subnet	1.1.1.1	0
□	03	IP Address and Subnet	2.2.2.2	0
□	04	User-defined Service	TCP 3	1 •••

4. Enter a name for the object.



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



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

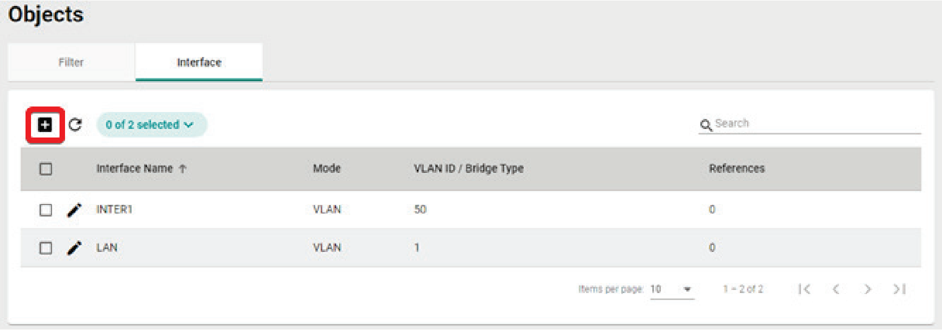
6. Click **CREATE**.

Creating a New Interface Object

Steps:

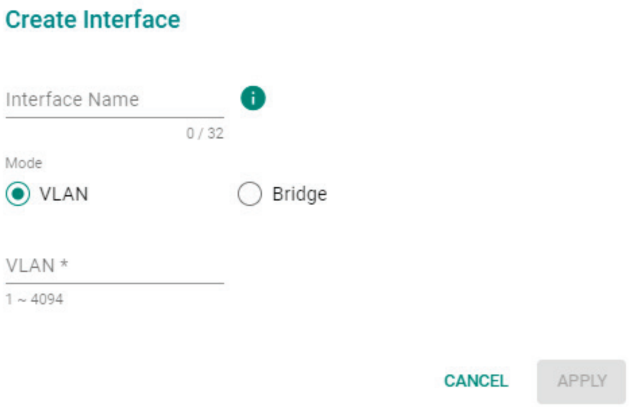
1. Navigate to **Management > Objects**.
2. Click the **Interface** tab.

3. Click the ⊞ icon to create a new object.



☐	Interface Name ↑	Mode	VLAN ID / Bridge Type	References
☐ ✏	INTER1	VLAN	50	0
☐ ✏	LAN	VLAN	1	0

4. Enter a name for the object.



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

Editing an Object

Steps:

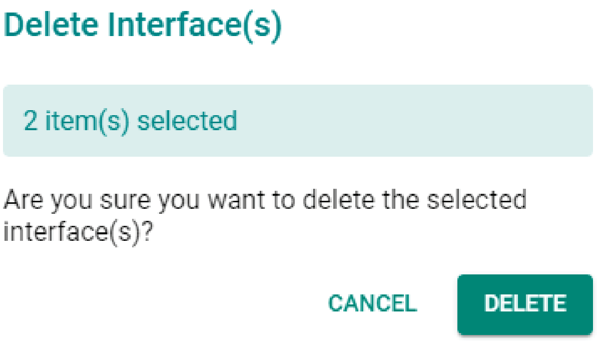
1. Navigate to **Management > Objects**.
2. Depending on the object you want to edit, click the **Filter** or **Interface** tab.
3. Click the ✏ icon to edit the object.
4. Modify the object settings.
   For Filter Objects, refer to Creating a New Filter Object.
   For Interface Objects, refer to Creating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

Deleting an Object

Steps:

1. Navigate to **Management > Objects**.
2. Depending on the object you want to delete, click the **Filter** or **Interface** tab.
3. Check the box of the object(s) that you want to delete.

4. Click the 🗑 icon to delete the selected object(s).
5. When prompted to confirm, click **DELETE**.



Delete Interface(s)

2 item(s) selected

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

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.

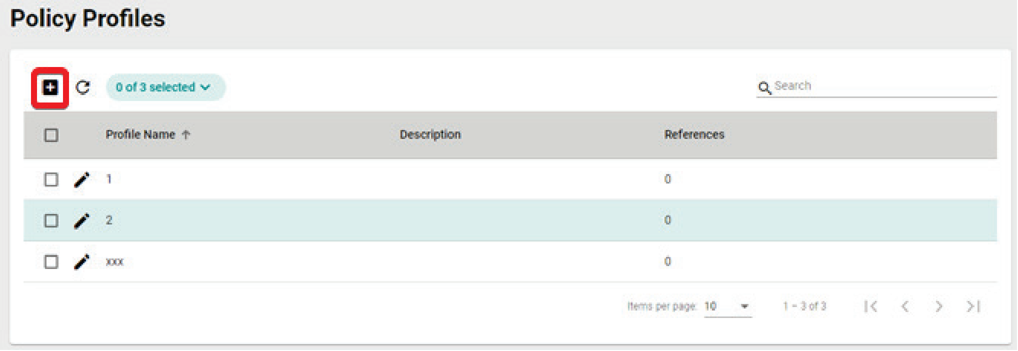
You can configure the following types of policies in MXsecurity:

- **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 network from security threats.

Creating a New Layer 3-7 Policy Profile

Steps:

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

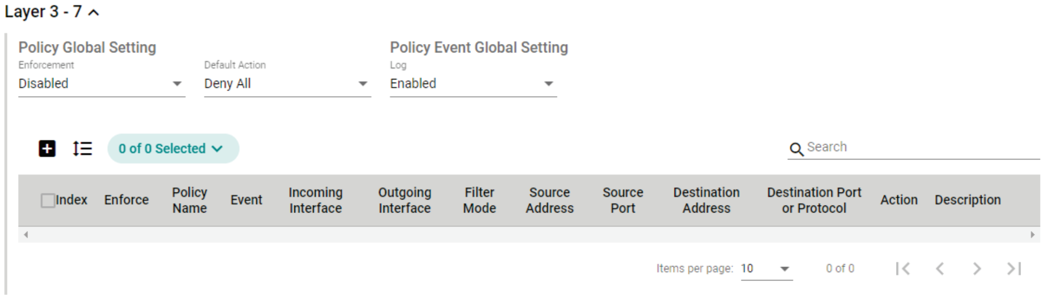


Policy Profiles

□	Profile Name ↑	Description	References
□ ✎	1		0
□ ✎	2		0
□ ✎	xxx		0

3. Enter a name and description for the policy profile.

4. Expand the **Layer 3-7** profile options.



Layer 3 - 7 ^

Policy Global Setting

Enforcement: Disabled

Default Action: Deny All

Policy Event Global Setting

Log: Enabled

0 of 0 Selected

Search

□ Index	Enforce	Policy Name	Event	Incoming Interface	Outgoing Interface	Filter Mode	Source Address	Source Port	Destination Address	Destination Port or Protocol	Action	Description

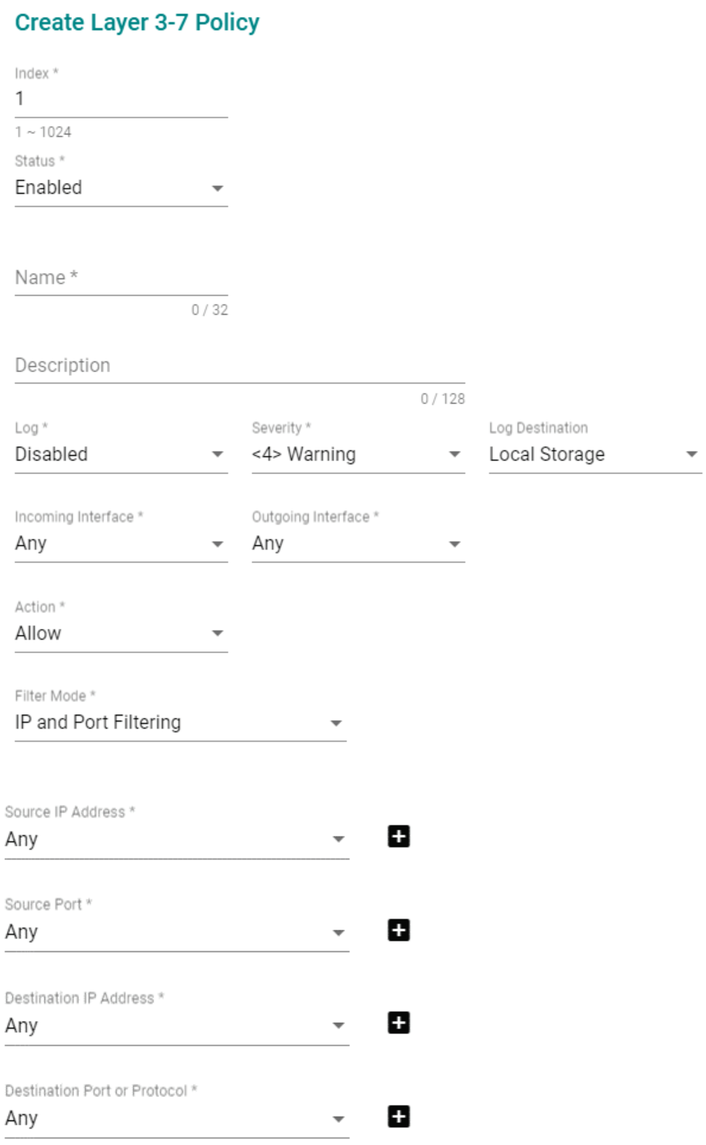
Items per page: 10

0 of 0

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

6. Click the ⊞ icon to create a Layer 3-7 policy profile.

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



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:

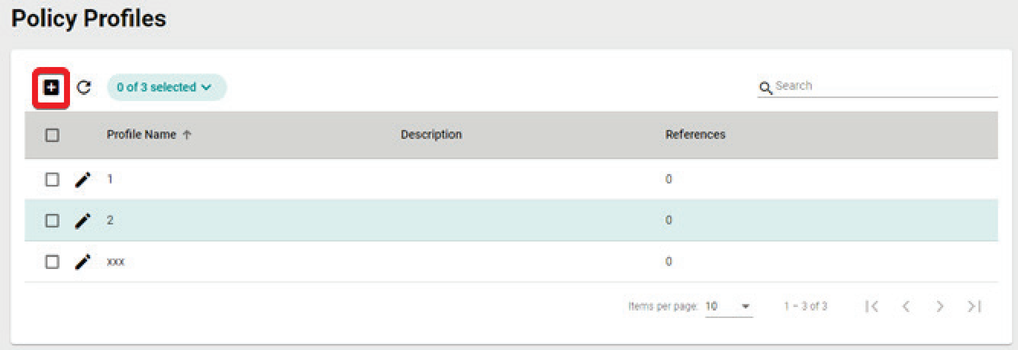
   i. Source MAC Address: Specify the source MAC address.

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

Creating a New Session Control Policy Profile

Steps:

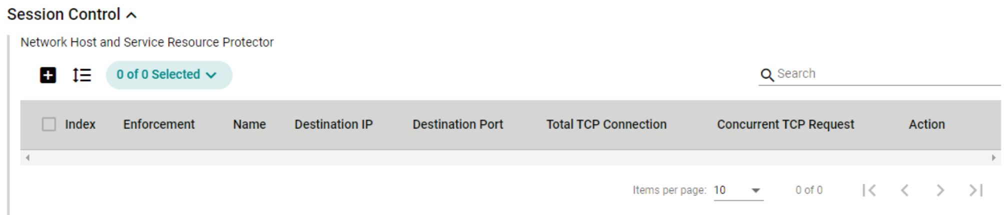
1. Navigate to **Management > Policy Profiles**.
2. Click the ⊞ icon to create a policy profile.



Policy Profiles

☐	Profile Name	Description	References
☐	1		0
☐	2		0
☐	xxx		0

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

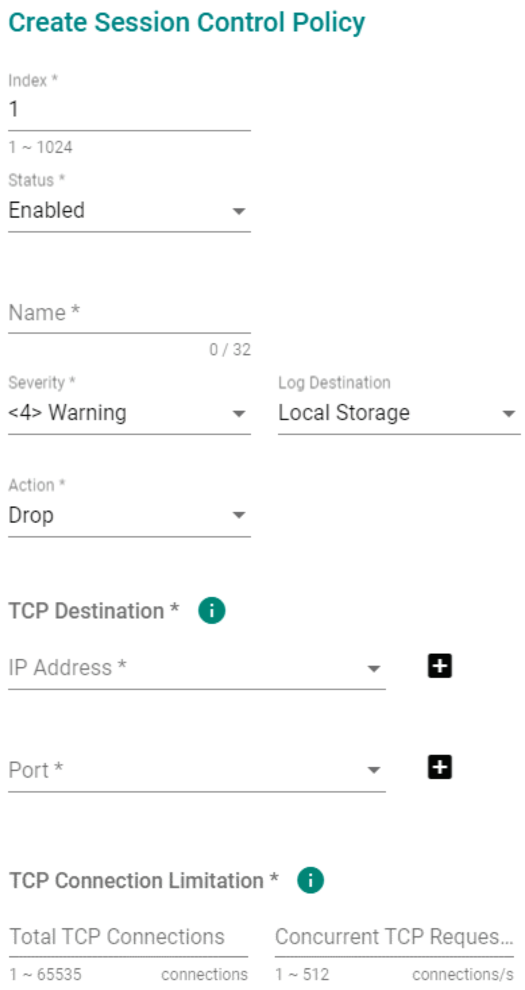


Session Control

Network Host and Service Resource Protector

☐ Index	Enforcement	Name	Destination IP	Destination Port	Total TCP Connection	Concurrent TCP Request	Action

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

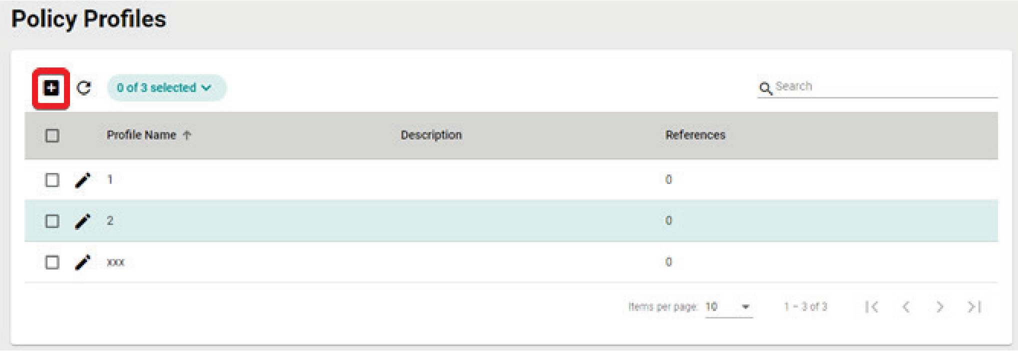
   a. **Index**: Specify the index for the policy profile.
   b. **Status**: Enable or disable the policy profile.
   c. **Name**: Enter a description for the policy profile.
   d. **Severity**: Select the log severity level.
   e. **Log Destination**: If logging is enabled, choose where the logs will be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

2. Click the ⊞ icon to create a policy profile.



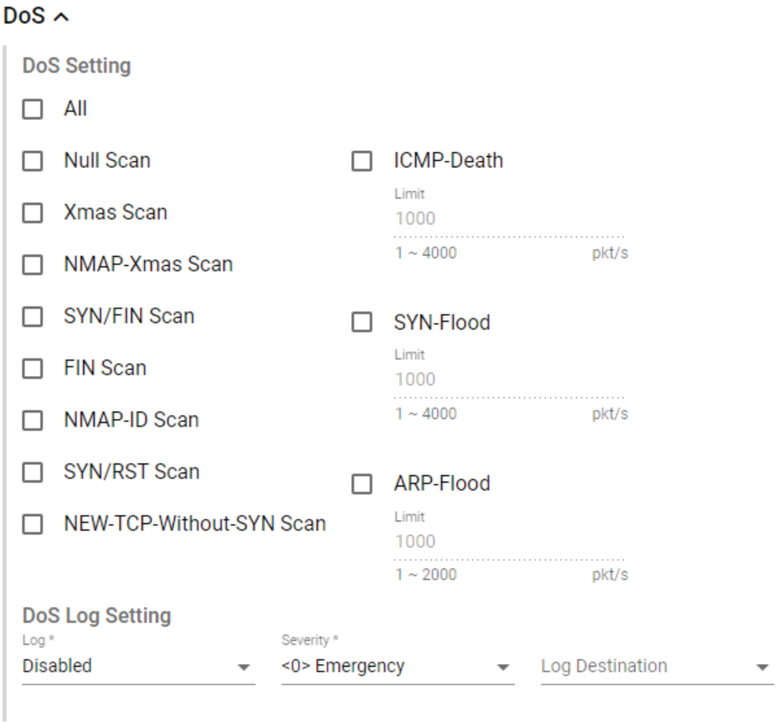
Policy Profiles

⊞ ⟳ 0 of 3 selected ⌄ Search

□		Profile Name ↑	Description	References
□	✎	1		0
□	✎	2		0
□	✎	xxx		0

Items per page: 10 1 - 3 of 3

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



DoS ^

DoS Setting

□ All

□ Null Scan

□ Xmas Scan

□ NMAP-Xmas Scan

□ SYN/FIN Scan

□ FIN Scan

□ NMAP-ID Scan

□ SYN/RST Scan

□ NEW-TCP-Without-SYN Scan

□ ICMP-Death

Limit 1000 1 ~ 4000 pkt/s

□ SYN-Flood

Limit 1000 1 ~ 4000 pkt/s

□ ARP-Flood

Limit 1000 1 ~ 2000 pkt/s

DoS Log Setting

Log * Disabled

Severity * <0> Emergency

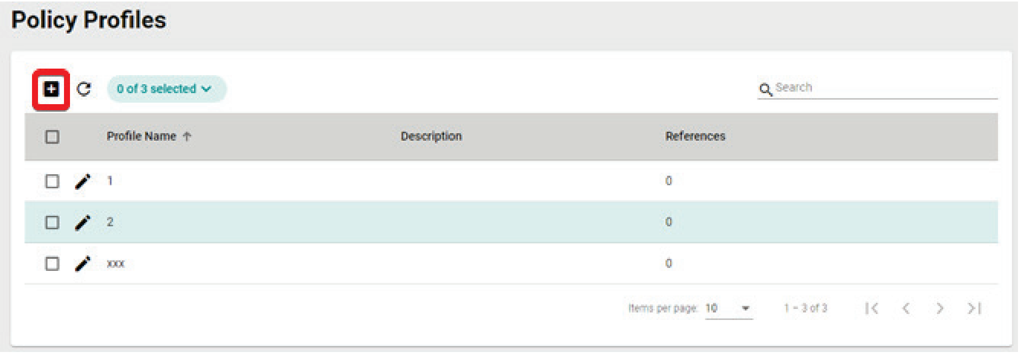
Log Destination

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

Creating a New IPS Policy Profile

Steps:

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



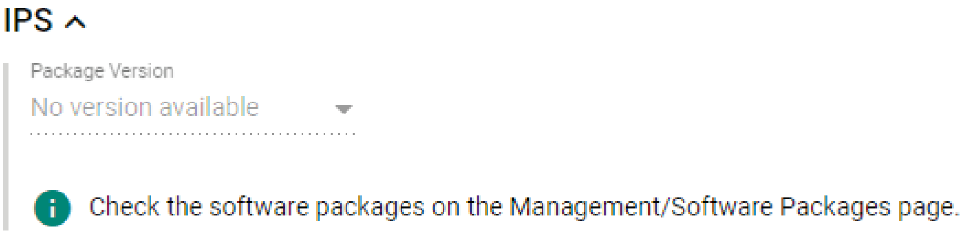
Policy Profiles

⊞ ⟳ 0 of 3 selected ⌄ Search

☐		Profile Name ↑	Description	References
☐	✎	1		0
☐	✎	2		0
☐	✎	xxx		0

Items per page: 10 ▾ 1 – 3 of 3 |< < > >|

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.

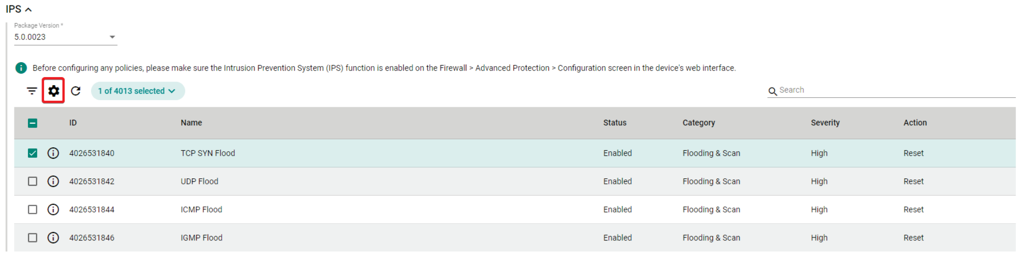


IPS ^

Package Version
No version available ▾

Check the software packages on the Management/Software Packages page.

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 ^

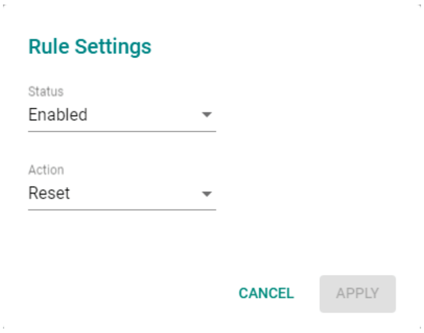
Package Version *
5.0.0023 ▾

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 ⌄ Search

☐		ID	Name	Status	Category	Severity	Action
☑	ⓘ	4026531840	TCP SYN Flood	Enabled	Flooding & Scan	High	Reset
☐	ⓘ	4026531842	UDP Flood	Enabled	Flooding & Scan	High	Reset
☐	ⓘ	4026531844	ICMP Flood	Enabled	Flooding & Scan	High	Reset
☐	ⓘ	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**.

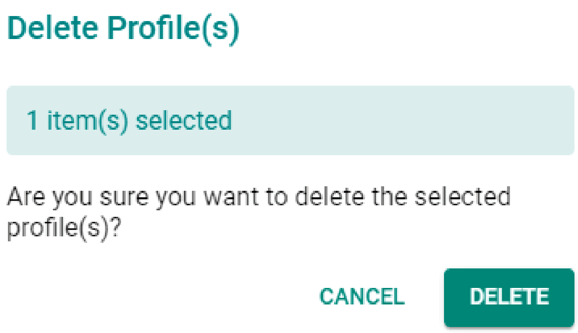
Editing a Policy Profile

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)?

6. Deployment

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

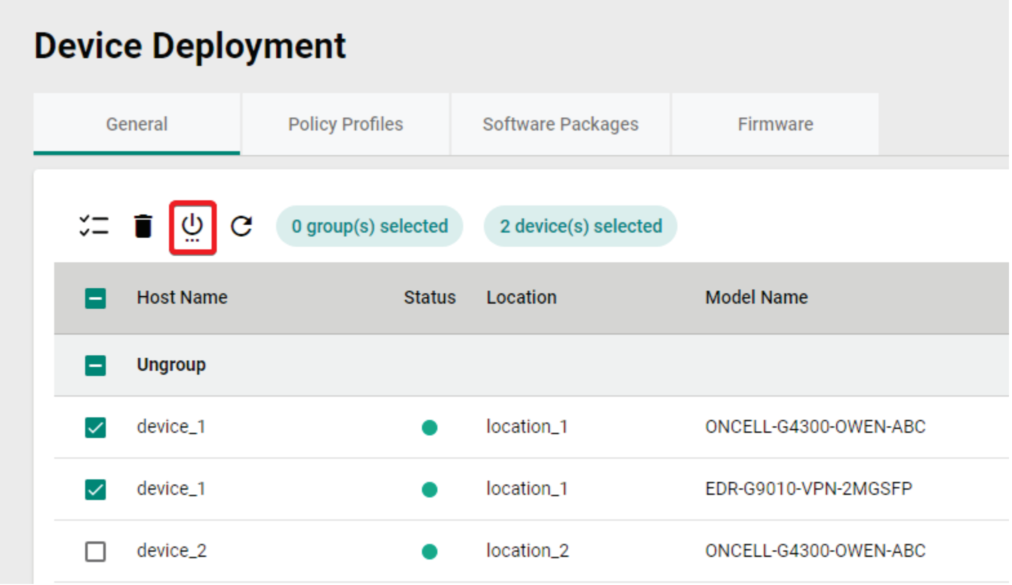
You can configure the following types of deployments in MXsecurity:

- **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.

Rebooting a Managed Device

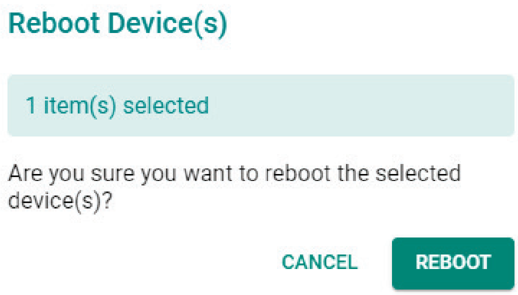
Steps:

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



⊟	Host Name	Status	Location	Model Name
⊟	Ungroup			
☑	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 reboot the selected device(s).
4. When prompted to confirm, click **REBOOT**.

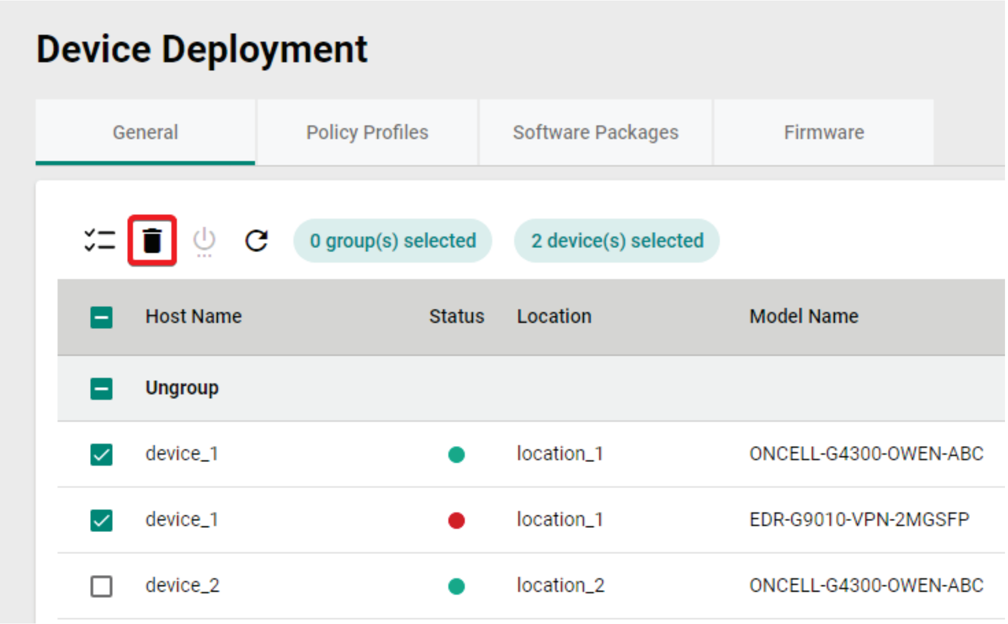


Are you sure you want to reboot the selected device(s)?

Removing a Managed Device

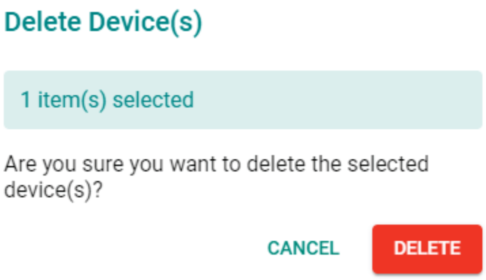
Steps:

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



▬	Host Name	Status	Location	Model Name
▬	Ungroup			
☑	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)?

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.

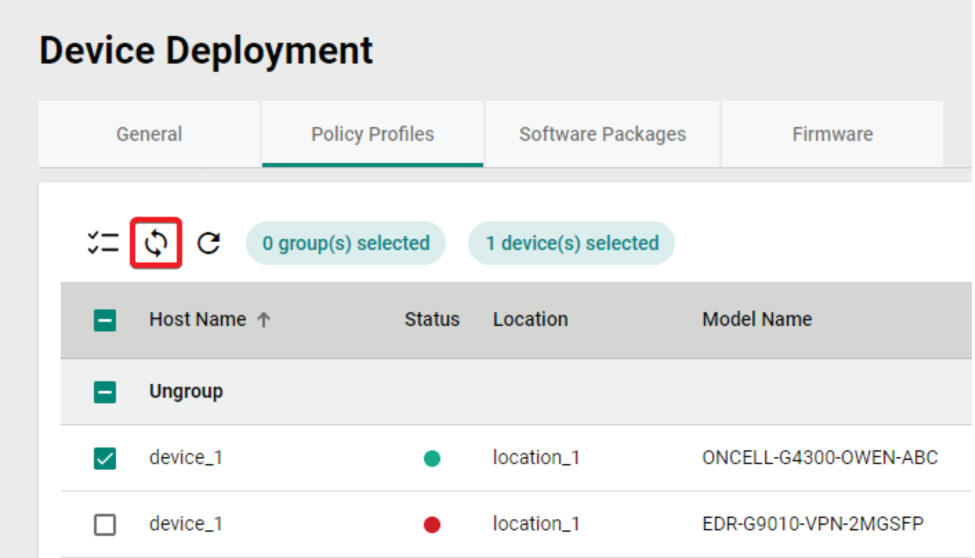
The synchronization status can be one of the following:

- **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.

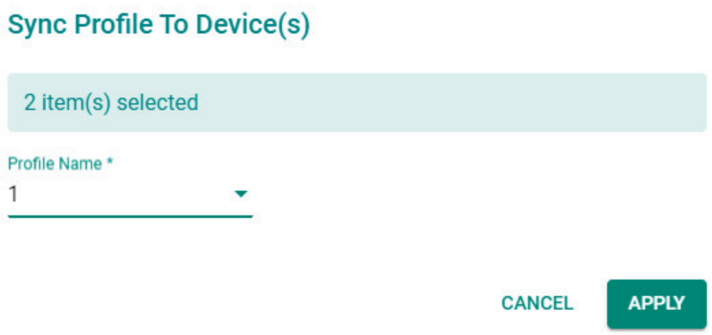
3. Click the 🔄 icon to deploy a policy profile to the selected device(s).



Device Deployment

☐	Host Name ↑	Status	Location	Model Name
⊟	Ungroup			
☑	device_1	●	location_1	ONCELL-G4300-OWEN-ABC
☐	device_1	●	location_1	EDR-G9010-VPN-2MGSFP

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)

2 item(s) selected

Profile Name *: 1

5. Click **APPLY**.

Upgrading the Software Package of Managed Devices

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

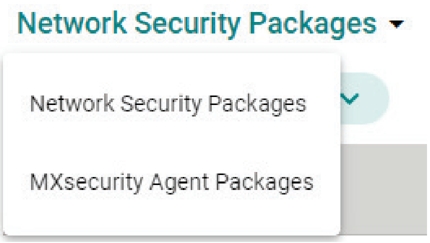
You can check the following software package information:

- **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:

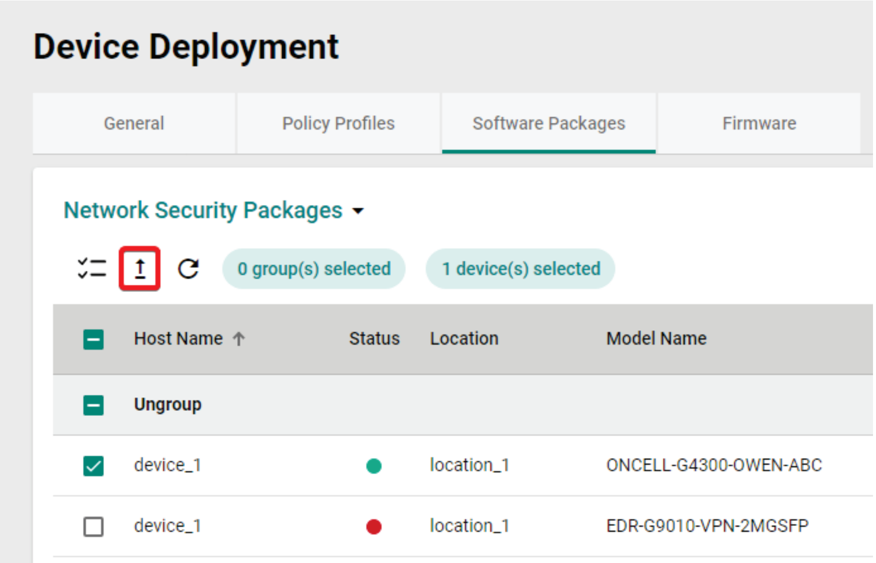
1. Navigate to **Device Deployment > Software Packages**.

2. Select the software package type from the drop-down menu.


Network Security Packages
Network Security Packages
MXsecurity Agent Packages

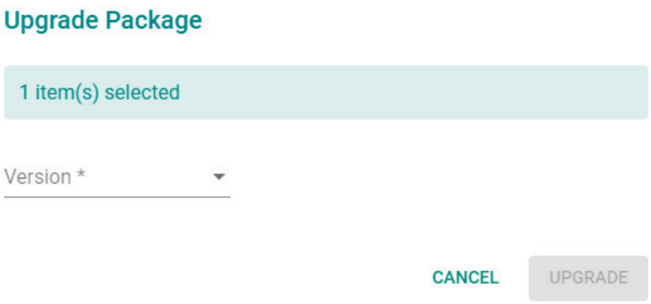
3. Check the box of the device(s) you want to upgrade the software package for.

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



	Host Name ↑	Status	Location	Model Name
☐	Ungroup			
☑	device_1	●	location_1	ONCELL-G4300-OWEN-ABC
☐	device_1	●	location_1	EDR-G9010-VPN-2MGSFP

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



6. Click **UPGRADE**.

Upgrading the Firmware of Managed Devices

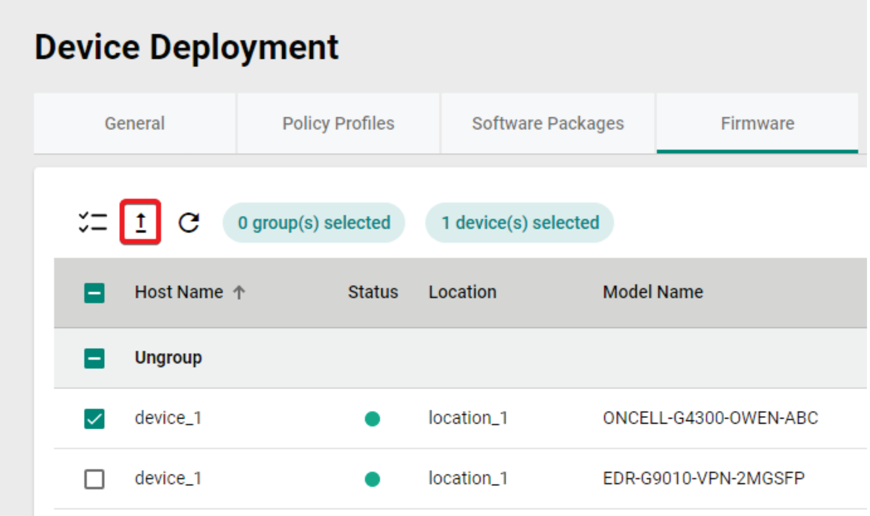
You can upgrade the firmware of managed devices and check basic firmware version information.

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:

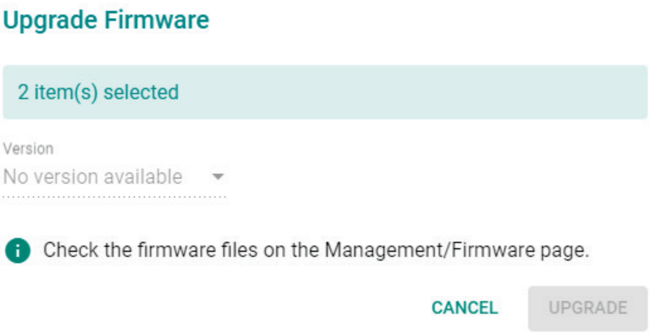
1. Navigate to **Device Deployment > Firmware**.
2. Check the box of the device(s) you want to upgrade the firmware for.
3. Click the ↥ icon to upgrade the firmware for the selected device(s).



Device Deployment

	Host Name ↑	Status	Location	Model Name
▬	Ungroup			
☑	device_1	●	location_1	ONCELL-G4300-OWEN-ABC
□	device_1	●	location_1	EDR-G9010-VPN-2MGSFP

4. 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.

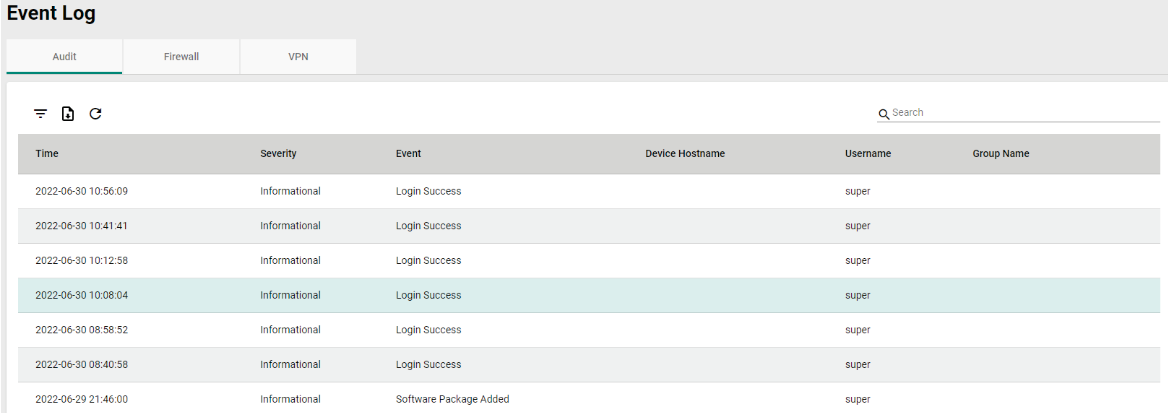
5. Click **UPGRADE**.

7. Logs

This chapter describes the audit, security, and VPN logs you can view in MXsecurity.

Viewing Audit Logs

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



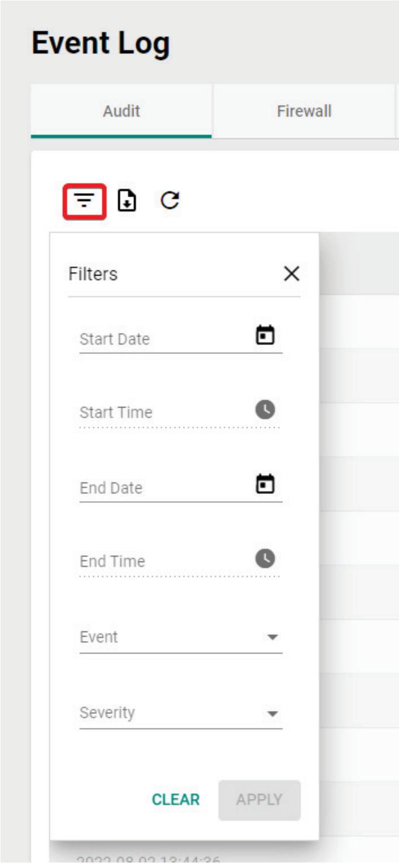
Event Log

Time	Severity	Event	Device Hostname	Username	Group Name
2022-06-30 10:56:09	Informational	Login Success		super	
2022-06-30 10:41:41	Informational	Login Success		super	
2022-06-30 10:12:58	Informational	Login Success		super	
2022-06-30 10:08:04	Informational	Login Success		super	
2022-06-30 08:58:52	Informational	Login Success		super	
2022-06-30 08:40:58	Informational	Login Success		super	
2022-06-29 21:46:00	Informational	Software Package Added		super	

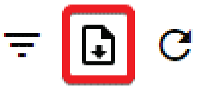
Steps:

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

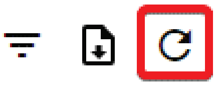
   a. Click the ☰ icon to open the filter menu. Select a start/end day and time, event category, or log severity from the respective drop-menu and click **APPLY**. The logs will renew immediately to reflect the selected criteria.



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



c. Click the ↻ button to renew the search results.

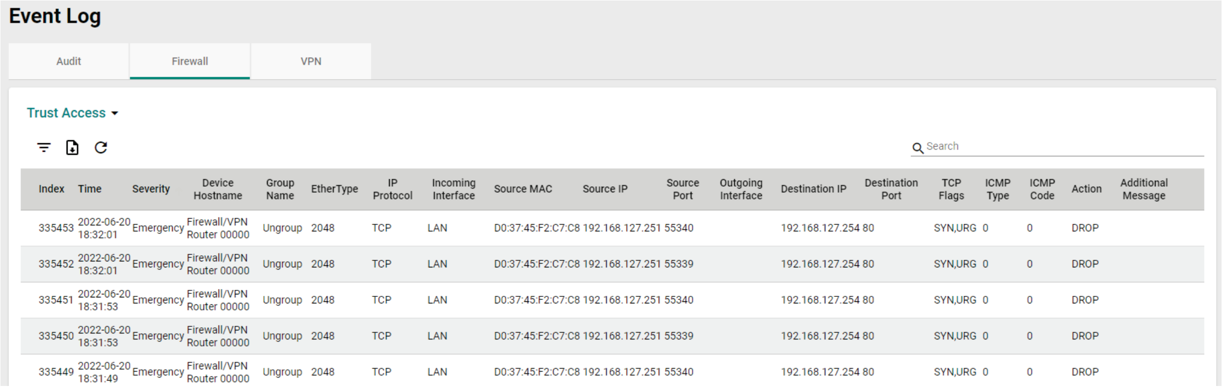


The following table describes the log's fields.

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.

Viewing Firewall Logs

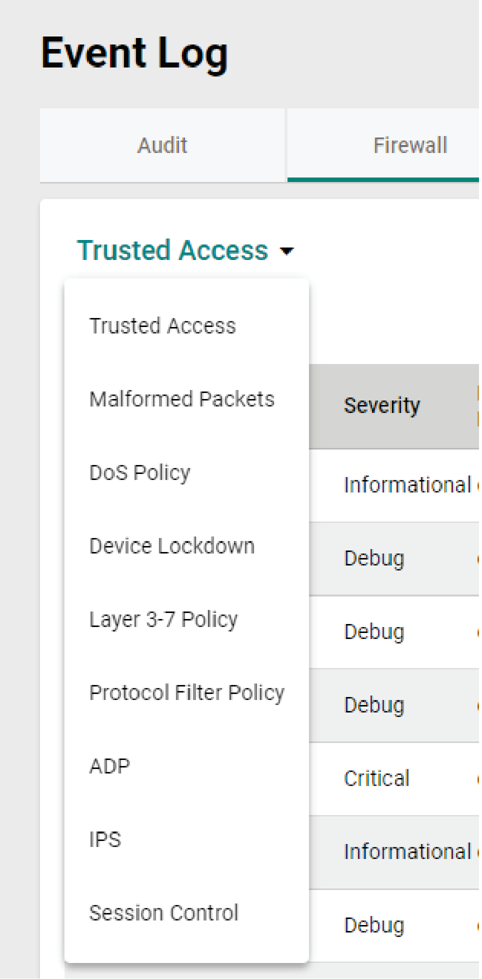
The firewall logs include logs detected by the Trusted Access, Malformed Packets, DoS policy, L3-L7 policies, protocol filter policies, ADP, IPS and Session Control features.



Index	Time	Severity	Device Hostname	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	Additional Message
335453	2022-06-20 18:32:01	Emergency	Firewall/VPN Router 00000	Ungroup	2048	TCP	LAN	D0:37:45:F2:C7:C8	192.168.127.251	55340		192.168.127.254	80	SYN,URG	0	0	DROP	
335452	2022-06-20 18:32:01	Emergency	Firewall/VPN Router 00000	Ungroup	2048	TCP	LAN	D0:37:45:F2:C7:C8	192.168.127.251	55339		192.168.127.254	80	SYN,URG	0	0	DROP	
335451	2022-06-20 18:31:53	Emergency	Firewall/VPN Router 00000	Ungroup	2048	TCP	LAN	D0:37:45:F2:C7:C8	192.168.127.251	55340		192.168.127.254	80	SYN,URG	0	0	DROP	
335450	2022-06-20 18:31:53	Emergency	Firewall/VPN Router 00000	Ungroup	2048	TCP	LAN	D0:37:45:F2:C7:C8	192.168.127.251	55339		192.168.127.254	80	SYN,URG	0	0	DROP	
335449	2022-06-20 18:31:49	Emergency	Firewall/VPN Router 00000	Ungroup	2048	TCP	LAN	D0:37:45:F2:C7:C8	192.168.127.251	55340		192.168.127.254	80	SYN,URG	0	0	DROP	

Steps:

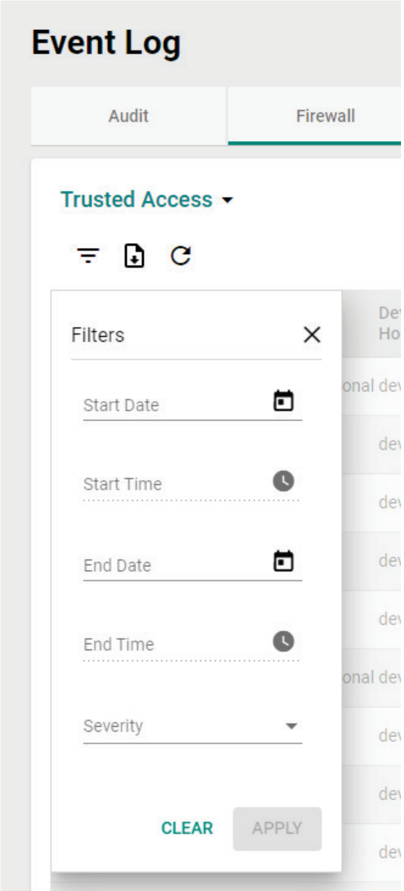
1. Navigate to **Logging > Event Log > Firewall**.
2. Select the firewall function event log type from the drop-down menu.



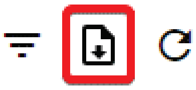
Severity
Informational
Debug
Debug
Debug
Critical
Informational
Debug

3. You can perform the following actions:

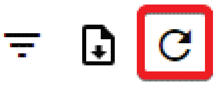
   a. Click the ☰ icon to open the filter menu. Select a start/end day and time or log severity from the respective drop-menu and click **APPLY**. The logs will renew immediately to reflect the selected criteria.



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



c. Click the ↻ button to renew the search results.



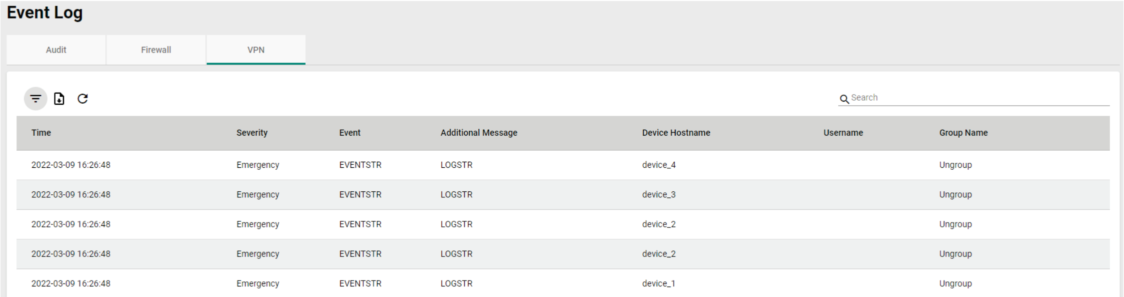
The following table describes the log's fields.

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.

Viewing VPN Logs

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



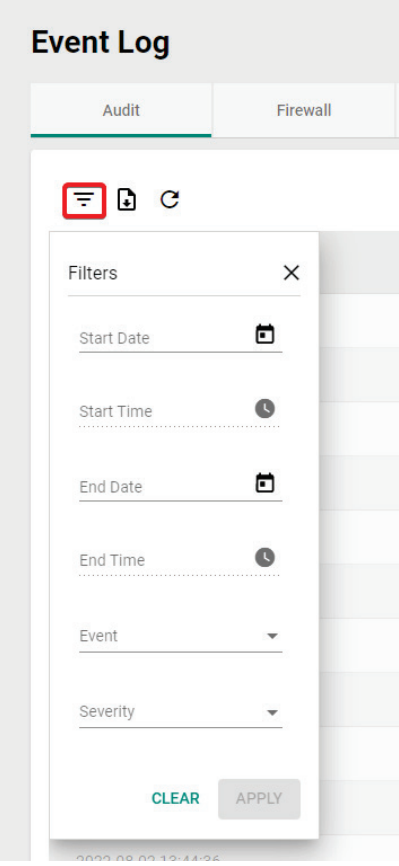
Event Log

Time	Severity	Event	Additional Message	Device Hostname	Username	Group Name
2022-03-09 16:26:48	Emergency	EVENTSTR	LOGSTR	device_4		Ungroup
2022-03-09 16:26:48	Emergency	EVENTSTR	LOGSTR	device_3		Ungroup
2022-03-09 16:26:48	Emergency	EVENTSTR	LOGSTR	device_2		Ungroup
2022-03-09 16:26:48	Emergency	EVENTSTR	LOGSTR	device_2		Ungroup
2022-03-09 16:26:48	Emergency	EVENTSTR	LOGSTR	device_1		Ungroup

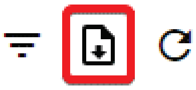
Steps:

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

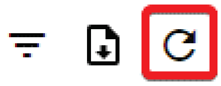
   a. Click the ≡ icon to open the filter menu. Select a start/end day and time, event category, or log severity from the respective drop-menu and click **APPLY**. The logs will renew immediately to reflect the selected criteria.

   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.

8. Administration

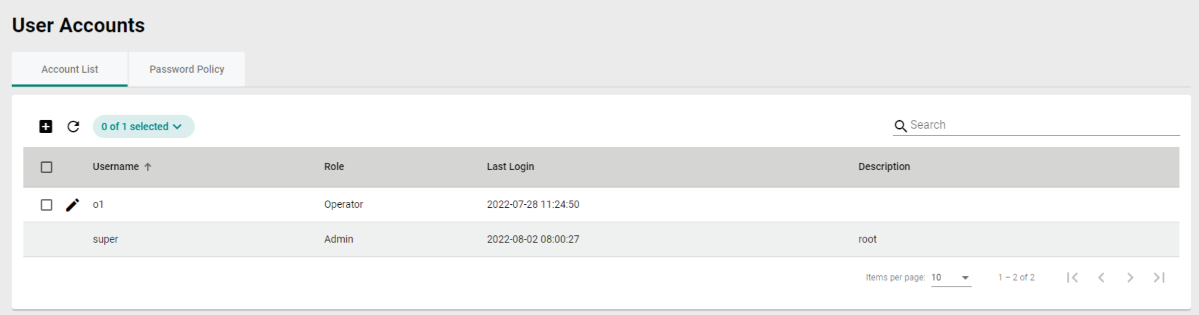
This chapter describes the available administrative settings for MXsecurity.

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.



User Accounts

Account List | Password Policy

⊞ ↻ 0 of 1 selected ⌄ 🔍 Search

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

Items per page: 10 ▾ 1 – 2 of 2 |< < > >|

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

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

System Tab

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

Management Tabs

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

NOTE

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

Device Deployment

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

NOTE

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

Logging

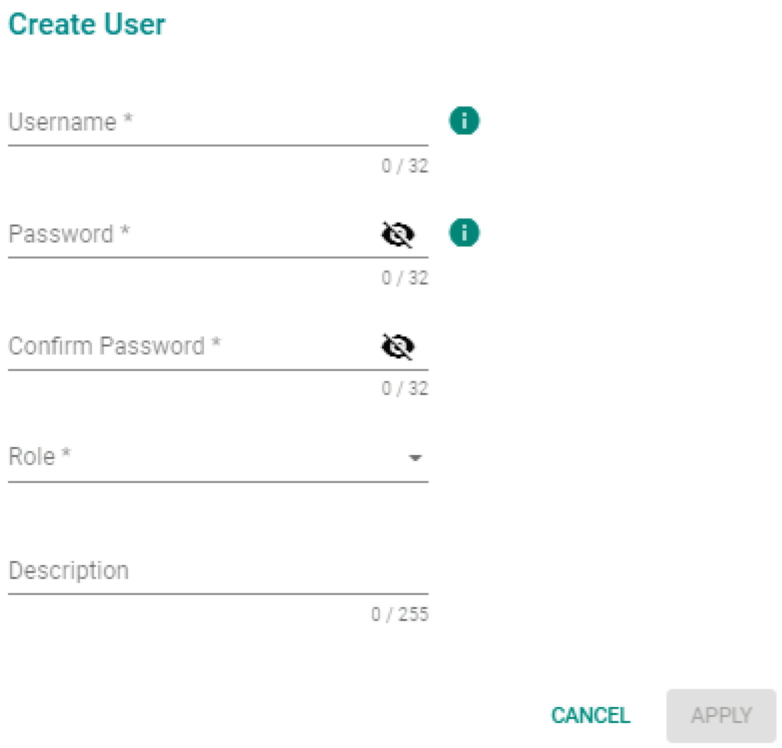
		User Roles		
Configuration Screen	**Action**	**Admin**	**Operator**	**Viewer**
Event Log	View	Yes	VG	VG
	All operations	Yes	VG	No

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 Logging/Event Log pages.

Account Input Format

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



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

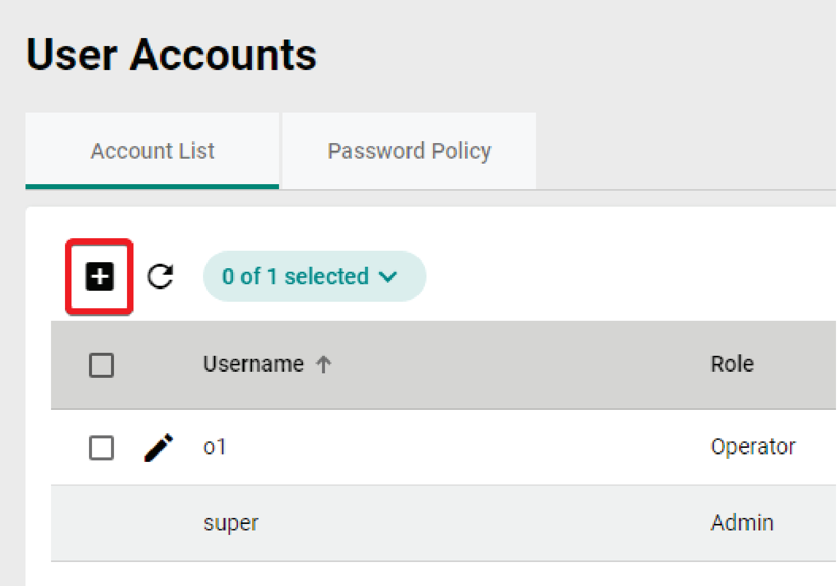
Adding a User Account

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

Steps:

1. Navigate to **System > User Accounts > Account List**.

2. Click the ⊞ icon.



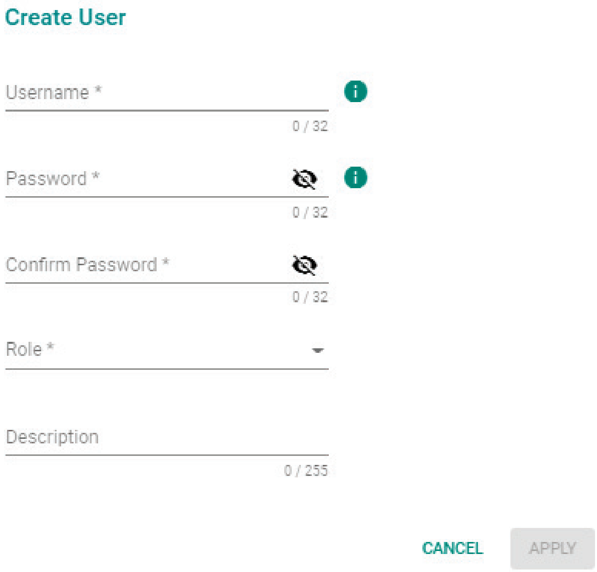
User Accounts

Account List | Password Policy

0 of 1 selected

□	Username ↑	Role
□	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

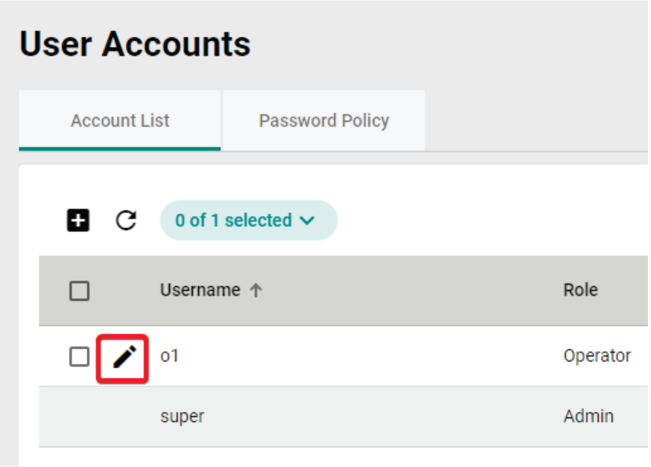
CANCEL APPLY

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

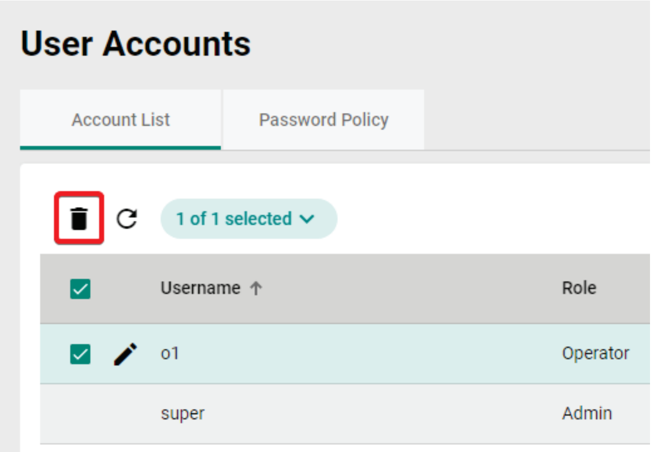
☐		Username ↑	Role
☐	✏	o1	Operator
		super	Admin

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

Deleting a User Account

Steps:

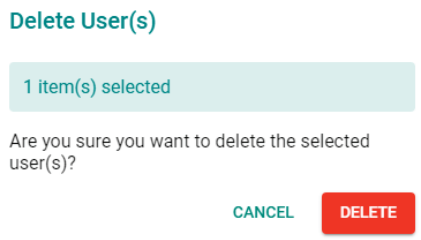
1. Navigate to **System > User Accounts > Account List**.
2. Check the box of the user account(s) you want to delete.
3. Click the 🗑 icon to delete the selected user account(s).



User Accounts

☑		Username ↑	Role
☑	✏	o1	Operator
		super	Admin

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



Delete User(s)

1 item(s) selected

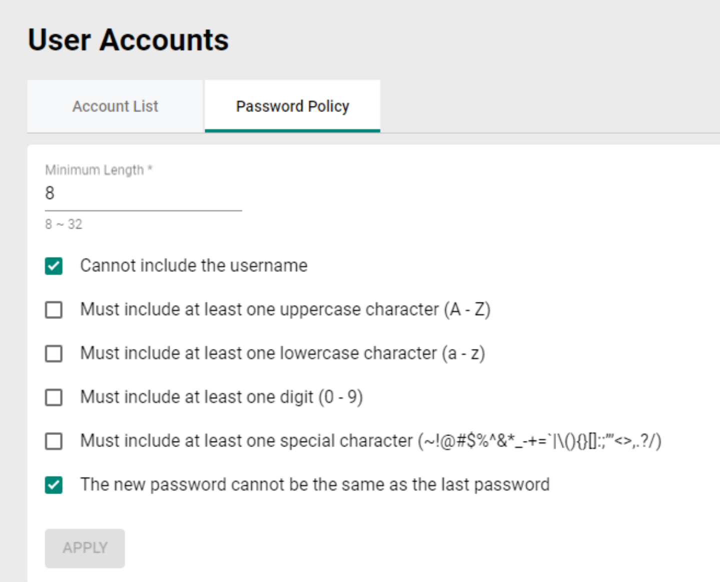
Are you sure you want to delete the selected user(s)?

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.



User Accounts

Account List | Password Policy

Minimum Length *
8
8 ~ 32

☑ Cannot include the username

☐ Must include at least one uppercase character (A - Z)

☐ Must include at least one lowercase character (a - z)

☐ Must include at least one digit (0 - 9)

☐ Must include at least one special character (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

☑ The new password cannot be the same as the last password

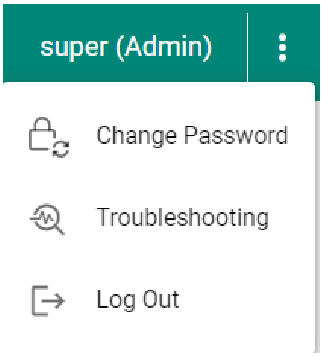
APPLY

3. Click **APPLY**.

Changing Your Account Password

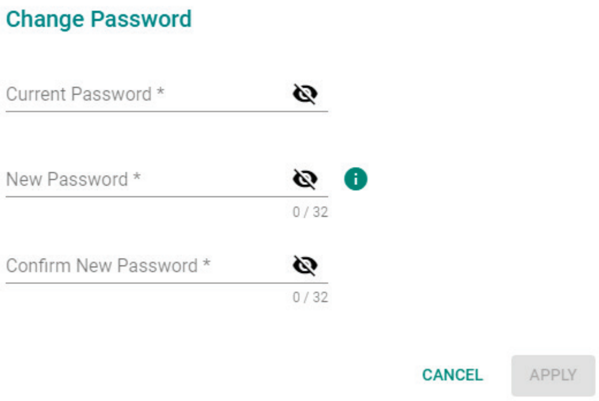
Steps:

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



2. Click **Change Password**.

The **Change Password** screen will appear.



Change Password

Current Password *

New Password *

0 / 32

Confirm New Password *

0 / 32

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

Log in to the management console using an administrator account to 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

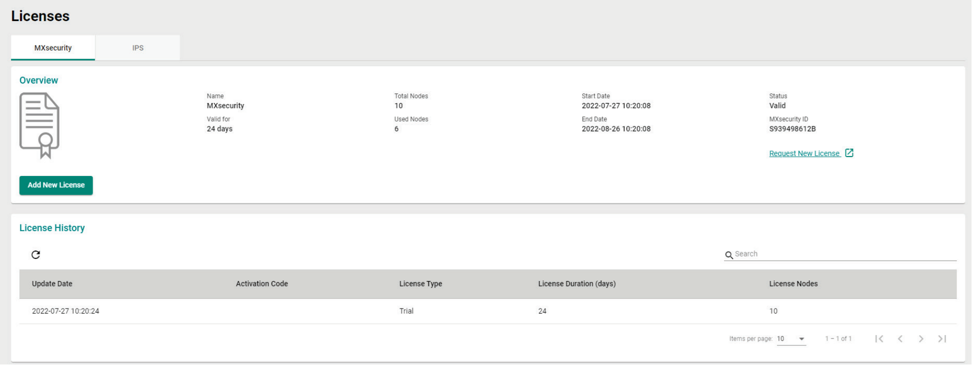
Only one MXsecurity and IPS license can be used at any given time. When more than one MXsecurity and IPS license is applied to MXsecurity, only the latest one will be kept.

Viewing Your Product License Information

Steps:

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

The **License** screen will appear.



Name: MXsecurity
Valid for: 24 days
Total Nodes: 10
Used Nodes: 6
Start Date: 2022-07-27 10:20:08
End Date: 2022-08-26 10:20:08
Status: Valid
MXsecurity ID: S939498612B

Update Date	Activation Code	License Type	License Duration (days)	License Nodes
2022-07-27 10:20:24		Trial	24	10

Items per page: 10 1 – 1 of 1

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.

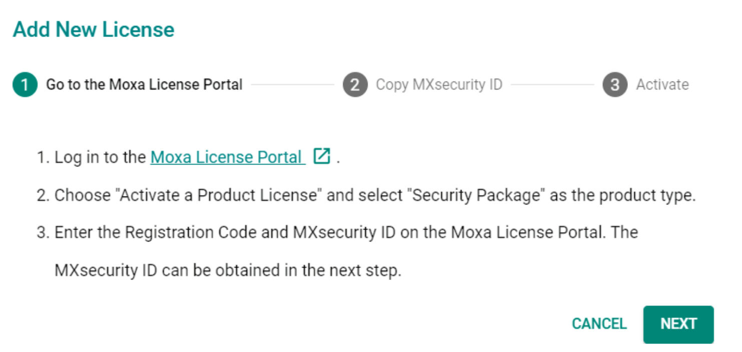
Message	Description
The (category) license expires in (days) days. To continue using all features, enter a new license code.	This message appears 30 days before the license expiration date. The (days) represents the days remaining before the license expires.
The (category) license has expired. To continue 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 Add New License button.
   The **Add New License** screen will appear.



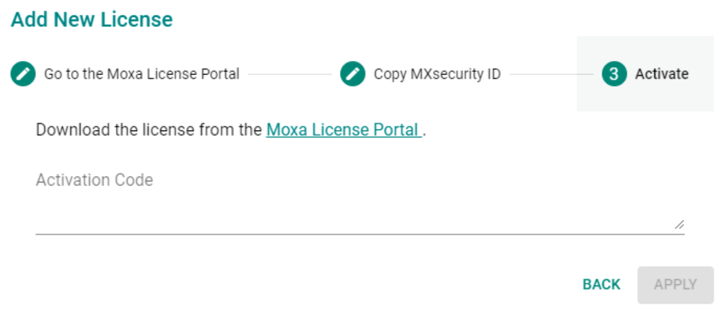
Add New License

1 Go to the Moxa License Portal — 2 Copy MXsecurity ID — 3 Activate

1. Log in to the Moxa License Portal ↗ .
2. Choose "Activate a Product License" and select "Security Package" as the product type.
3. Enter the Registration Code and MXsecurity ID on the Moxa License Portal. The MXsecurity ID can be obtained in the next step.

CANCEL NEXT

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.



Add New License

✓ Go to the Moxa License Portal — ✓ Copy MXsecurity ID — 3 Activate

Download the license from the Moxa License Portal .

Activation Code

BACK APPLY

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

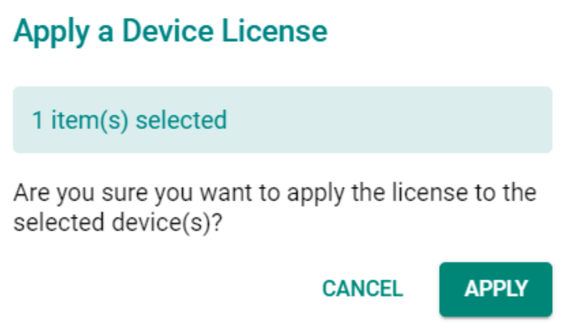
Binding a License to a Device

In order 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).

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



Apply a Device License

1 item(s) selected

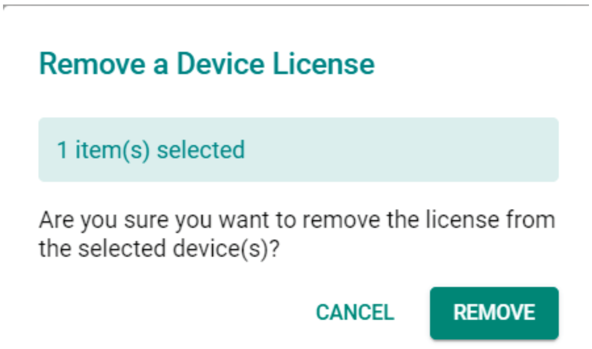
Are you sure you want to apply the license to the selected device(s)?

Unbinding a License From a Device

If necessary, you unbind a license from a managed device in order to bind to another device. Note that unbinding a license will cause the relevant function to become unavailable on that device.

Steps:

1. Navigate to **System > Licenses**.
2. Click the **IPS** tab.
3. Check the box of the device(s) you want to unbind the license from.
4. Click the icon to unbind the license from the selected device(s).
5. 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)?

Settings

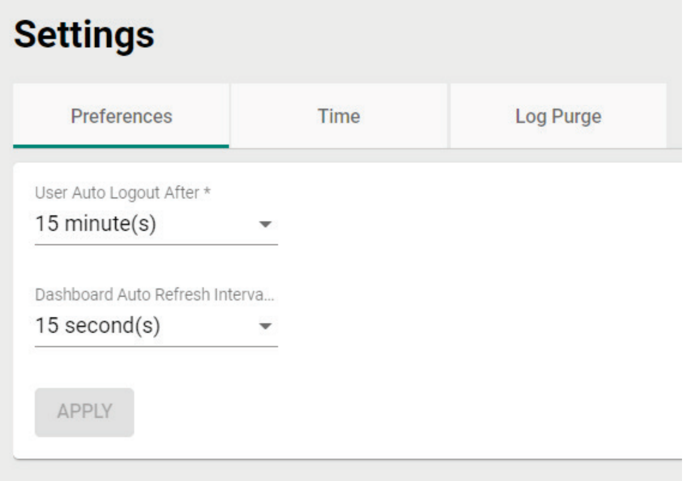
From the **Settings** page, you can configure system preferences, time, and log purge settings.

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.



User Auto Logout After *
15 minute(s)

Dashboard Auto Refresh Interva...
15 second(s)

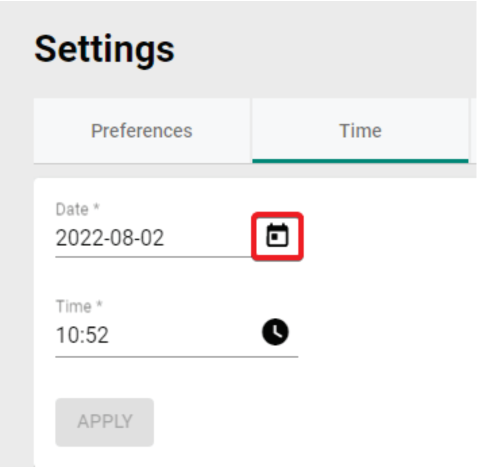
3. Click **APPLY**.

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:

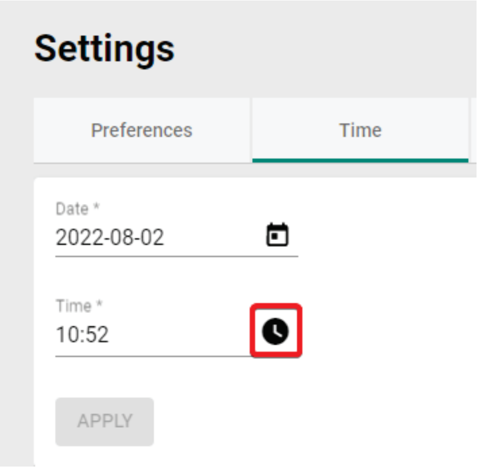
1. Navigate to **System > Settings > Time**.
2. Click the 📅 icon to select the date.



Date *
2022-08-02

Time *
10:52

3. Click the ● icon to select the time.



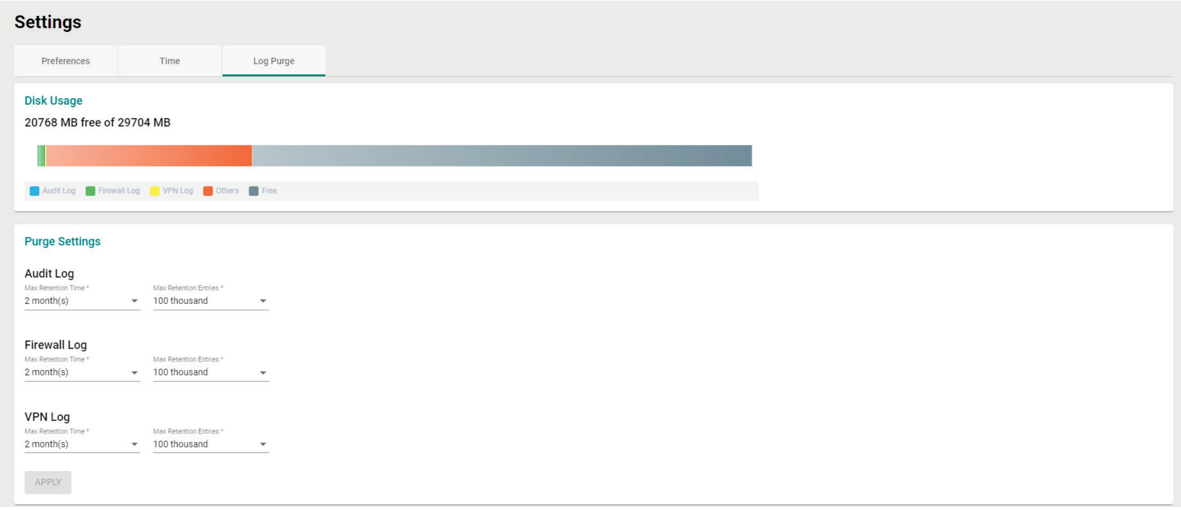
Date *
2022-08-02

Time *
10:52

4. Click **APPLY**.

Purging Logs

From the **Log Purge** window, you can view the status of the logs stored on the hard drive of the system running MXseurity and configure log purging methods. Purging logs may be useful when the system generates a lot of event logs, which may impact network performance.



Disk Usage

20768 MB free of 29704 MB

Purge Settings

Audit Log

Max Retention Time *: 2 month(s)

Max Retention Entries *: 100 thousand

Firewall Log

Max Retention Time *: 2 month(s)

Max Retention Entries *: 100 thousand

VPN Log

Max Retention Time *: 2 month(s)

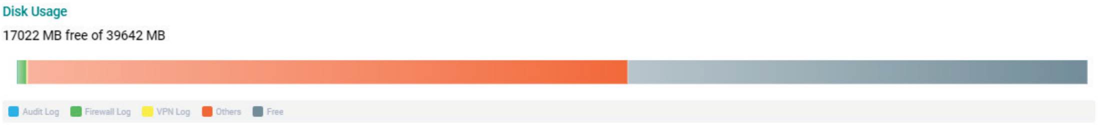
Max Retention Entries *: 100 thousand

You can purge the logs in the following ways:

- Automatically purge logs: Logs are automatically deleted based on a specified threshold number of log entries, a retention period for log data, or both.

Steps:

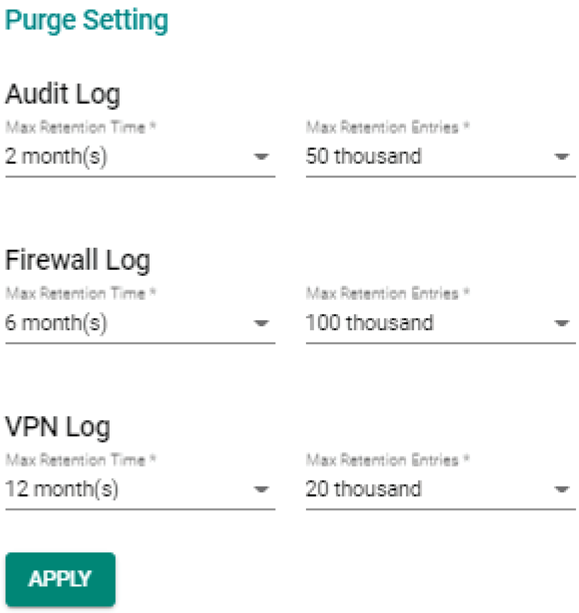
1. Navigate to **System > Settings > Log Purge.**
2. In the Disk Usage section, check the current used and available disk space.



Disk Usage

17022 MB free of 39642 MB

3. In the Purge Setting section, select the log retention time and maximum retention entries for each log type.



Purge Setting

Audit Log

Max Retention Time *: 2 month(s)

Max Retention Entries *: 50 thousand

Firewall Log

Max Retention Time *: 6 month(s)

Max Retention Entries *: 100 thousand

VPN Log

Max Retention Time *: 12 month(s)

Max Retention Entries *: 20 thousand

4. Click **APPLY**.

NOTE

When the number of entries for a log type reaches the set threshold value, MXsecurity will start clearing the logs, beginning with the oldest records.