

MXsecurity User Manual

Version 5.1, November 2025

www.moxa.com/product



© 2025 Moxa Inc. All rights reserved.

MXsecurity User Manual

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

Copyright Notice

© 2025 Moxa Inc. All rights reserved.

Trademarks

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

Disclaimer

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

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. Introduction	6
Key Features	6
Centralized Management	6
Unified, Error-free Mass Deployment	6
Real-time Visibility and Monitoring	6
Event Logs and Alert Notifications	6
Interactive Map View	6
Comprehensive Reports	6
System Requirements	7
2. Installation	8
Downloading MXsecurity	8
Setting Up the Virtual Machine	9
Installing MXsecurity on a VMware Workstation	9
Installing MXsecurity on a VMware ESXi System	12
Configuring the MXsecurity system	17
3. Migration	20
Migrating to a Newer Version of MXsecurity (VMware Workstation)	20
Migrating to a Newer Version of MXsecurity (ESXi)	24
Migrating Licenses	28
4. Getting Started	31
Getting Started Task List	31
Opening the Management Console	31
Connecting Secure Routers to MXsecurity	33
5. Dashboard and Widgets	34
Dashboard Widgets Overview	34
System Status	34
Licenses	34
Group Status	35
Top 5 Layer 3-7 Policy Events by Source IP	36
Top 5 Layer 3-7 Policy Events by Destination IP	37
Top 5 Layer 3-7 Policy Events by Severity	38
Top 5 Protocol Filter Policy Events by Source IP	39
Top 5 Protocol Filter Policy Events by Destination IP	39
Top 5 Protocol Filter Policy Events by Severity	40
Top 5 ADP Events by Source IP	41
Top 5 ADP Events by Destination IP	41
Top 5 IPS Events by Source IP	42
Top 5 IPS Events by Destination IP	43
Top 5 IPS Events by Severity	45
Top 5 IPS Events by Category	45
Connection Interface (Cellular Router)	46
Signal Quality (Cellular Router)	46
Device Log by Timeline	47
Firewall Log by Timeline	47
VPN Log by Timeline	48
Widget Management	49
Adding a Widget to the Dashboard	49
Removing a Widget from the Dashboard	50
Resizing a Widget	50
Moving the Widget Position	51
6. Management	52
Device Group Management	53
Creating a New Device Group	53
Deleting a Device Group	54
Editing a Device Group	55
Firmware Management	55
Uploading New Firmware	55
Deleting Firmware	56

Exporting Firmware	57
Software Package Management	57
Checking the Security Package Status.....	57
Uploading a New Software Package	58
Deleting a Software Package.....	59
Exporting Software Packages	59
Viewing Detailed Information of a Software Package.....	59
Viewing Network Security Package Logs.....	60
Setting Up a Scheduled Security Package Update Check.....	61
Object Management.....	61
Creating a New Filter Object	61
Creating a New Interface Object.....	63
Editing an Object.....	63
Deleting an Object.....	64
Policy Profile Management	64
Creating a New Layer 3-7 Policy Profile	64
Creating a New Session Control Policy Profile.....	67
Creating a New DoS Policy Profile	68
Creating a New IPS Policy Profile.....	70
Editing a Policy Profile.....	71
Deleting a Policy Profile.....	71
Device Configuration Management.....	71
Uploading a Device Configuration File From a Local Host	71
Uploading a Configuration From a Device	72
7. Deployment	74
Rebooting a Managed Device.....	74
Scheduling a Managed Device Reboot.....	75
Deleting a Managed Device Reboot Schedule.....	76
Removing a Managed Device.....	76
Deploying Policy Profiles to Managed Devices	77
Scheduling a Policy Profile Deployment for Managed Devices.....	78
Deleting a Policy Profile Deployment Schedule.....	80
Upgrading the Software Package of Managed Devices	80
Scheduling a Software Package Deployment for Managed Devices	81
Deleting a Software Package Deployment Schedule.....	83
Upgrading the Firmware of Managed Devices	83
Scheduling a Firmware Deployment for Managed Devices	84
Deleting a Firmware Deployment Schedule	85
Deploying a Configuration to Managed Devices.....	86
Scheduling a Configuration Deployment for Managed Devices	87
Deleting a Configuration Deployment Schedule.....	88
8. Map View	90
Viewing Detailed Device Information	91
Editing the Location of a Device.....	92
9. Report	94
Inventory Reports.....	94
Generating a Current Inventory Report	94
Scheduling an Inventory Report	95
Cellular Signal Reports	97
Scheduling a Cellular Signal Report	97
Data Usage Reports	98
Generating a Cellular Data Usage Report.....	98
Scheduling a Cellular Data Usage Report.....	100
Trail Reports	101
Generating a Trail Report	101
Scheduling a Trail Report	102
Viewing GPS Trajectories.....	103
Report Settings	104
Configure Report Time Zone Settings.....	104
Editing a Report Schedule.....	105

10. Logging.....	106
Event Log	106
Device Log	106
Firewall Log	108
VPN Log	112
Audit Log	113
Event Log Settings	115
Notifications.....	116
Adding a Notification.....	116
11. Administration.....	120
User Accounts	120
User Roles.....	120
Account Input Format	122
Adding a User Account	123
Editing an Existing User Account	124
Deleting a User Account	125
Configuring the Password Policy	125
Changing Your Account Password	126
Licenses	127
Introduction to Licenses	127
Viewing Your Product License Information	127
Alert Messages.....	128
Adding a New MXsecurity License	129
Settings.....	134
Configuring Preferences	134
Configuring the System Time.....	134
Editing Email Settings	135
Editing Syslog Settings	136

1. Introduction

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

Key Features

Centralized Management

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

Unified, Error-free Mass Deployment

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

Real-time Visibility and Monitoring

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

Event Logs and Alert Notifications

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

Interactive Map View

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

Comprehensive Reports

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

System Requirements

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

CPU (Virtual Cores)	4
RAM	8 GB
Hard Disk Space	64 GB
Supported Virtual Machines	VMWare ESXi 7.0 or above, VM Workstation 15 Pro or above

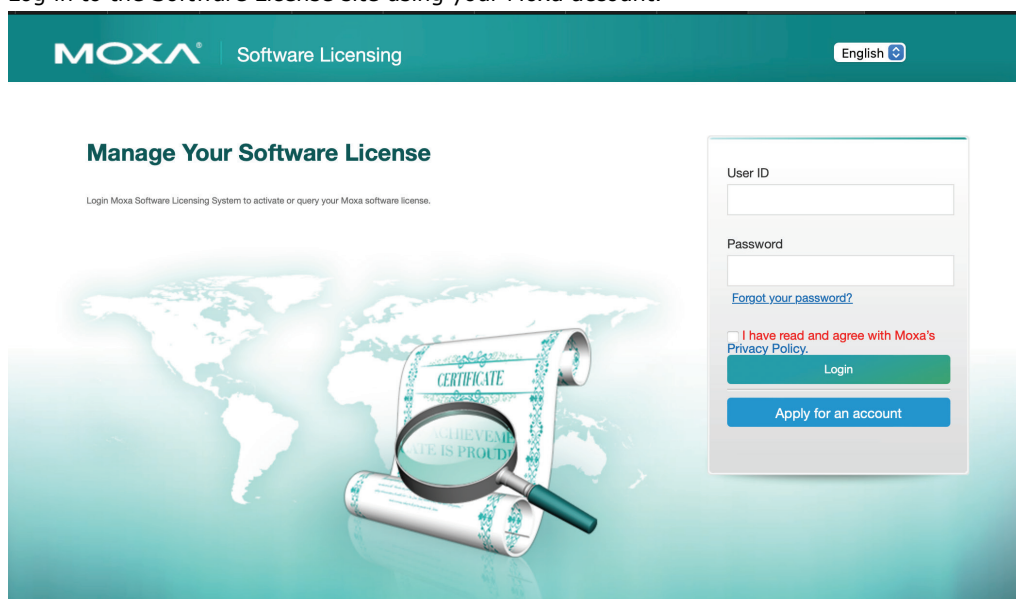
2. Installation

Downloading MXsecurity

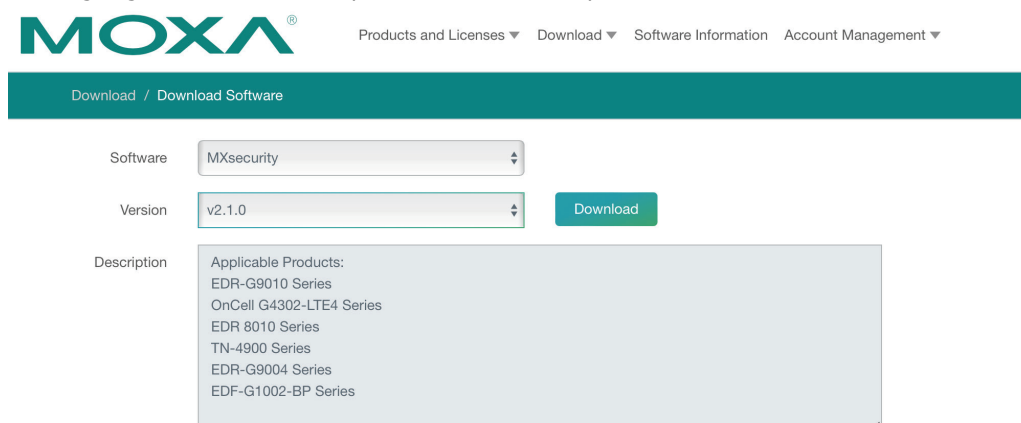
This section describes how to download the MXsecurity image file from the Moxa Software License site.

Steps:

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



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



5. Click **Download**.

Setting Up the Virtual Machine

Installing MXsecurity on a VMware Workstation

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

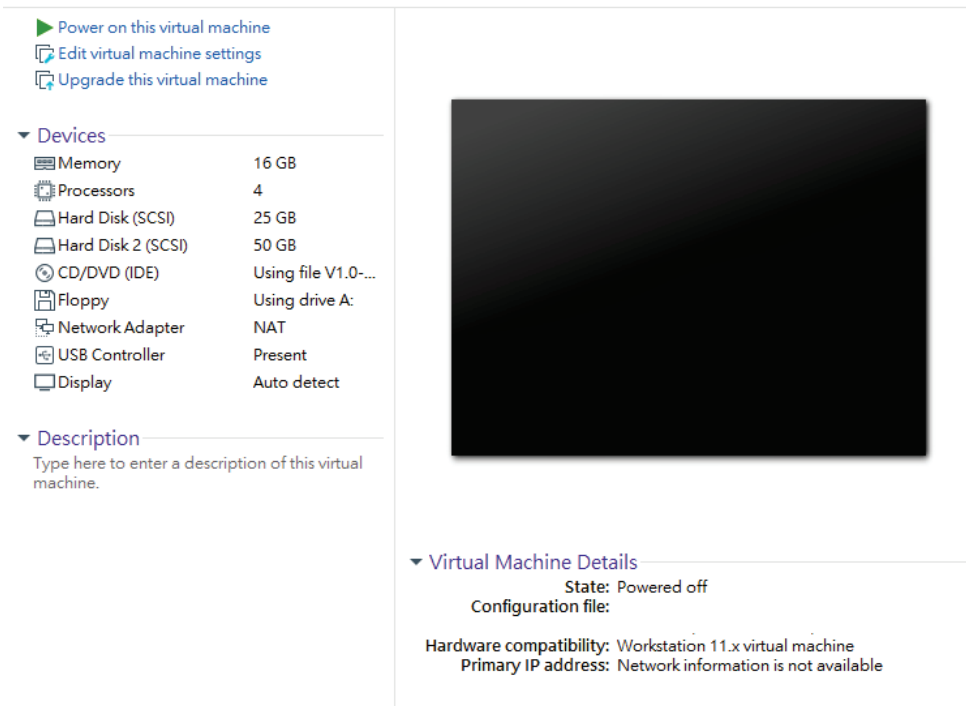
Prerequisites

- The OVA packages provided by Moxa must be available and accessible to the VMware Workstation.
- VMware Workstation 15 Pro or later is required.

Steps:

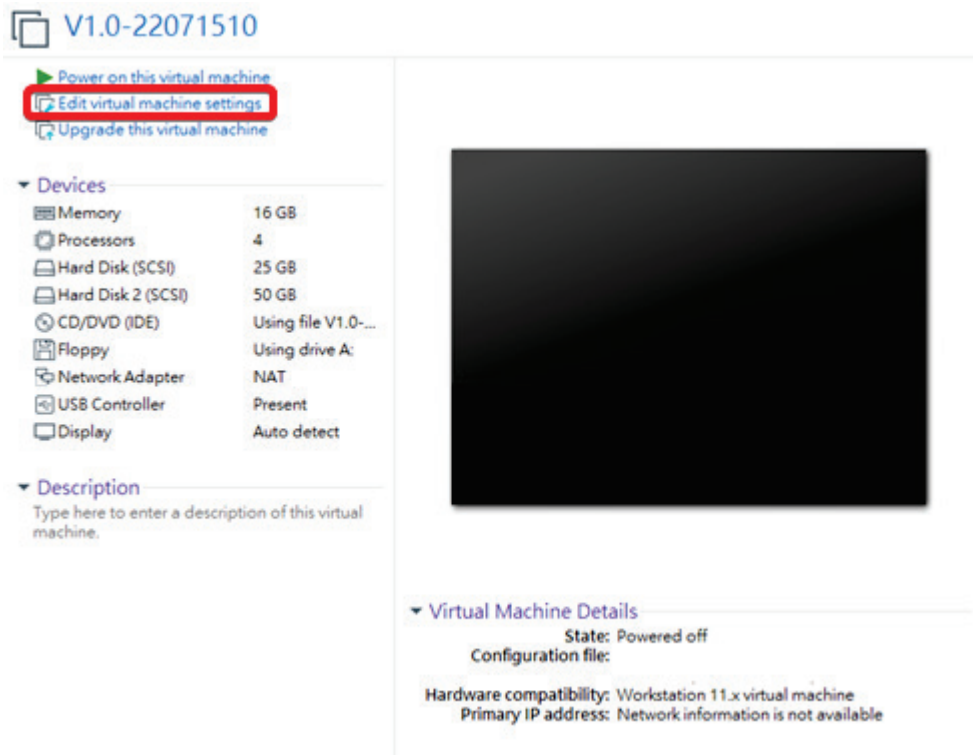
1. Start the VMware Workstation.
2. Go to **File > Open** in the menu bar.
3. Select the MXsecurity VM image file (*.ova) from your localhost file path and click **Open**.
4. Specify the name and the storage path for the new virtual machine and click **Import**.
5. Check the detailed VM information of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

 V1.0-22071510

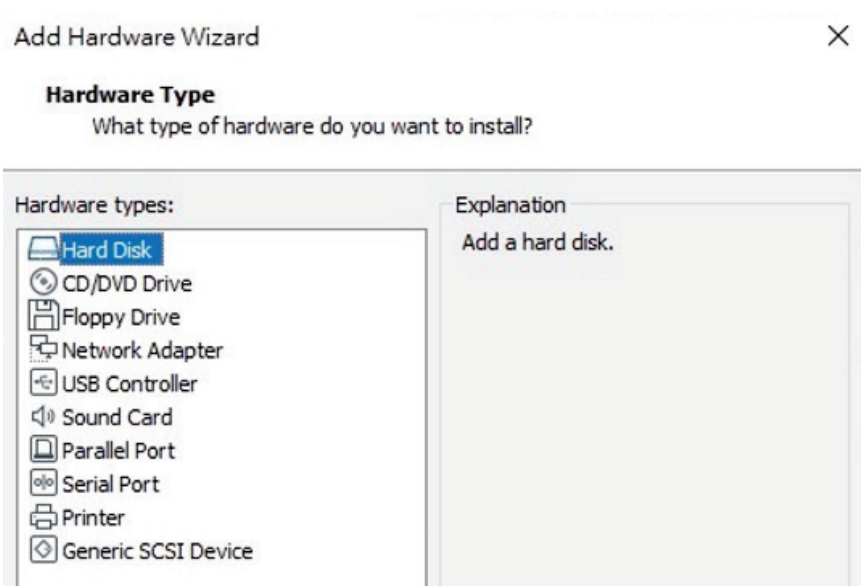


The screenshot displays the VMware Workstation interface for a virtual machine named 'V1.0-22071510'. On the left, there are three main sections: 'Actions' with links for 'Power on this virtual machine', 'Edit virtual machine settings', and 'Upgrade this virtual machine'; 'Devices' listing hardware components like Memory (16 GB), Processors (4), Hard Disks (25 GB and 50 GB), CD/DVD (IDE), Floppy, Network Adapter (NAT), USB Controller (Present), and Display (Auto detect); and 'Description' with a text input field. On the right, a large black rectangle represents the virtual machine's display. Below this, the 'Virtual Machine Details' section shows the 'State' as 'Powered off', the 'Configuration file' path, 'Hardware compatibility' as 'Workstation 11.x virtual machine', and the 'Primary IP address' as 'Network information is not available'.

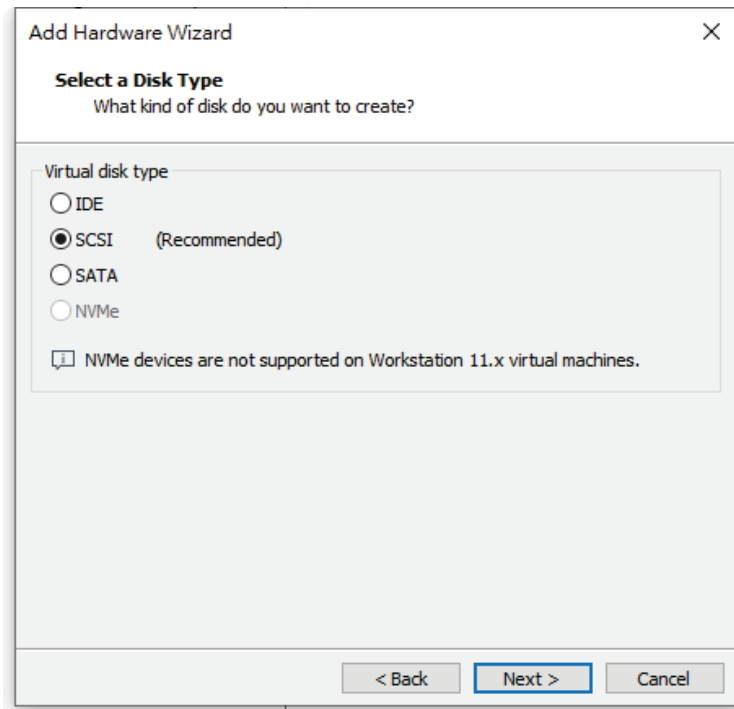
6. Add an external disk. MXsecurity requires one external disk with at least 20 GB of available storage, otherwise MXsecurity will not be able to finish initialization and the boot process will not be completed. The external disk is used to store the system configurations and event logs. You may attach 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**.



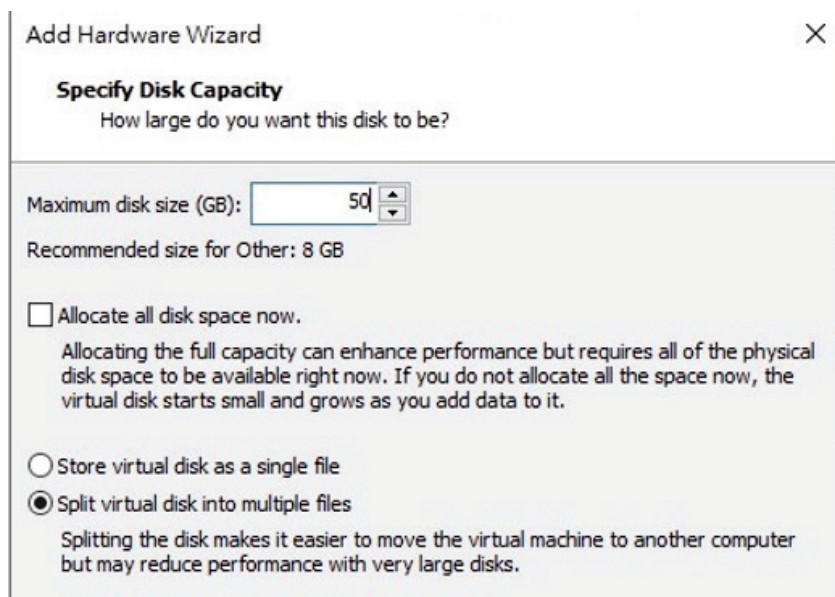
- b. Click **Add**, then choose **Hard Disk**.



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



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



- e. Select the path to store the disk.
- f. Click **Finish**.
- g. **(Optional)** If necessary, you can increase the disk size to hold a larger number of MXsecurity logs:
- Power off the MXsecurity instance.
 - Increase the external disk size based on your requirements.
 - Power the MXsecurity instance back on.
7. **(Optional)** Adjust your MX MXsecurity instance to use proper resource configurations (Minimum: 4 CPU cores, 8 GB of memory).
- Click **Edit virtual machine settings**.
 - Configure the amount of memory.
 - Configure the number of CPU cores.

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

Installing MXsecurity on a VMware ESXi System

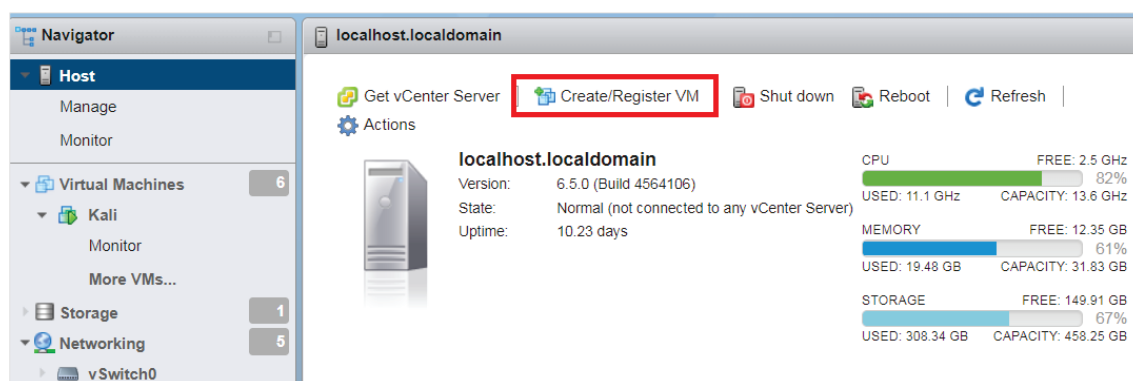
This section describes how to deploy MXsecurity to a VMware ESXi system.

Prerequisites

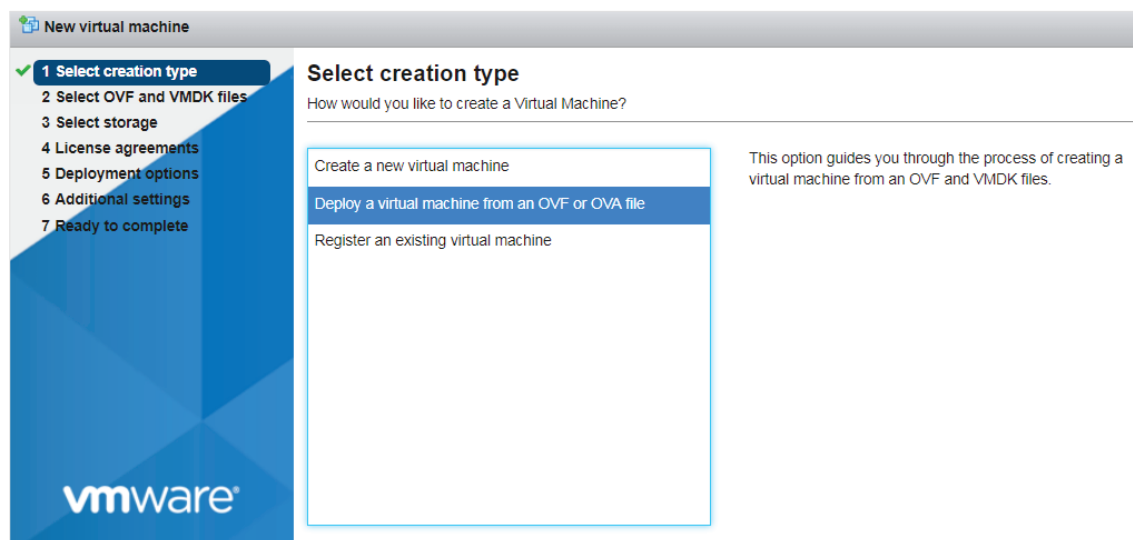
- The OVA packages provided by Moxa must be available and accessible to VMware ESXi.
- ESXi version 7.0 or above with the required specifications.
- The necessary networks have been properly created in ESXi.

Steps:

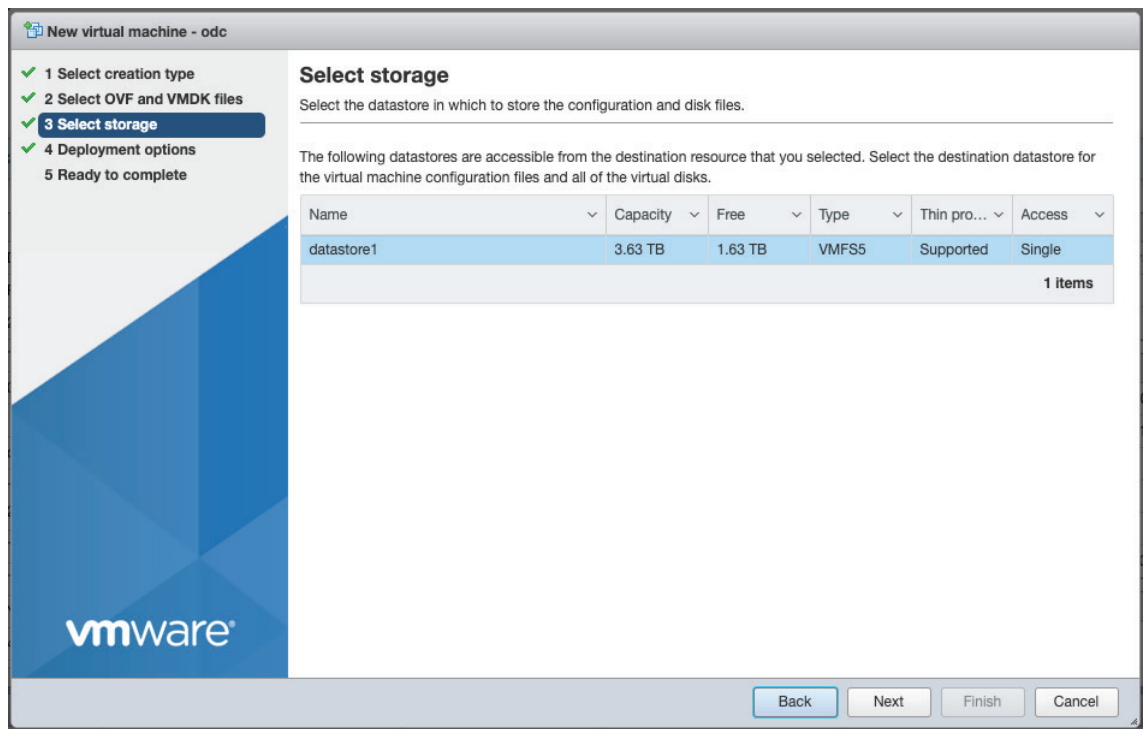
1. Log in to the VMware vSphere web client.
2. Under **Navigator**, click **Host** and then click **Create/Register VM**.



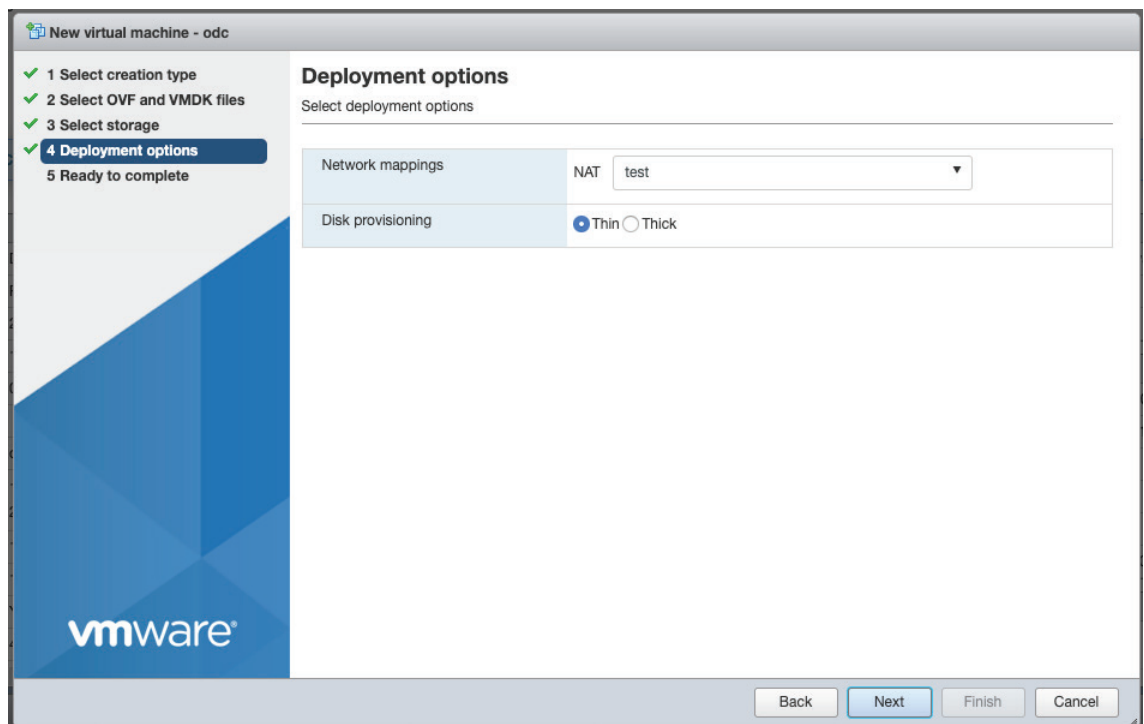
3. Select **Deploy a virtual machine from an OVF or OVA file**.



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



6. Select the deployment options.



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

New virtual machine - odc

✓ 1 Select creation type
✓ 2 Select OVF and VMDK files
✓ 3 Select storage
✓ 4 Deployment options
5 Ready to complete

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.

Back Next Finish Cancel

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**.

Edit settings - odc (ESXi 6.0 virtual machine)

Virtual Hardware VM Options

Add hard disk Add network adapter Add other device

New hard disk
Existing hard disk

8 MB

20480 MB

Hard disk 1 25 GB

SCSI Controller 0 LSI Logic Parallel

Network Adapter 1 test Connect

Video Card Specify custom settings

Save Cancel

- 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.

The screenshot shows the 'Edit settings' window for an ESXi 6.0 virtual machine named 'odc'. The 'Virtual Hardware' tab is active. In the 'Hard disk' section, 'New Hard disk' is selected, and its size is set to 50 GB. The 'Save' button at the bottom right is highlighted with a red box. Below the settings, the text 'Add an external disk' is displayed in red.

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

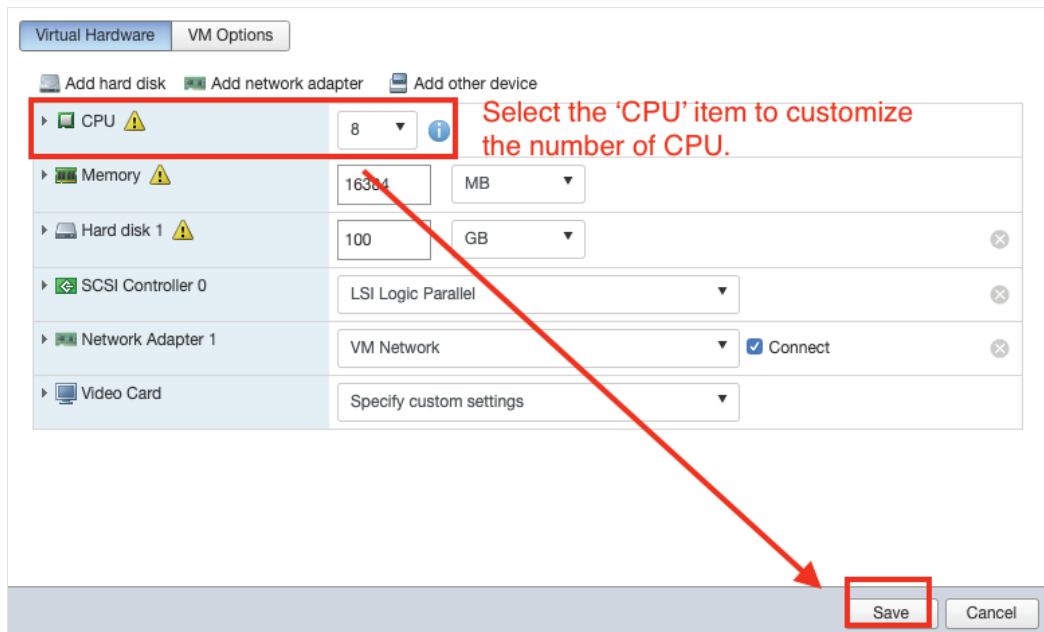
If you want to migrate the existing MXsecurity settings to the newly launched VM, please refer to [Migration](#).



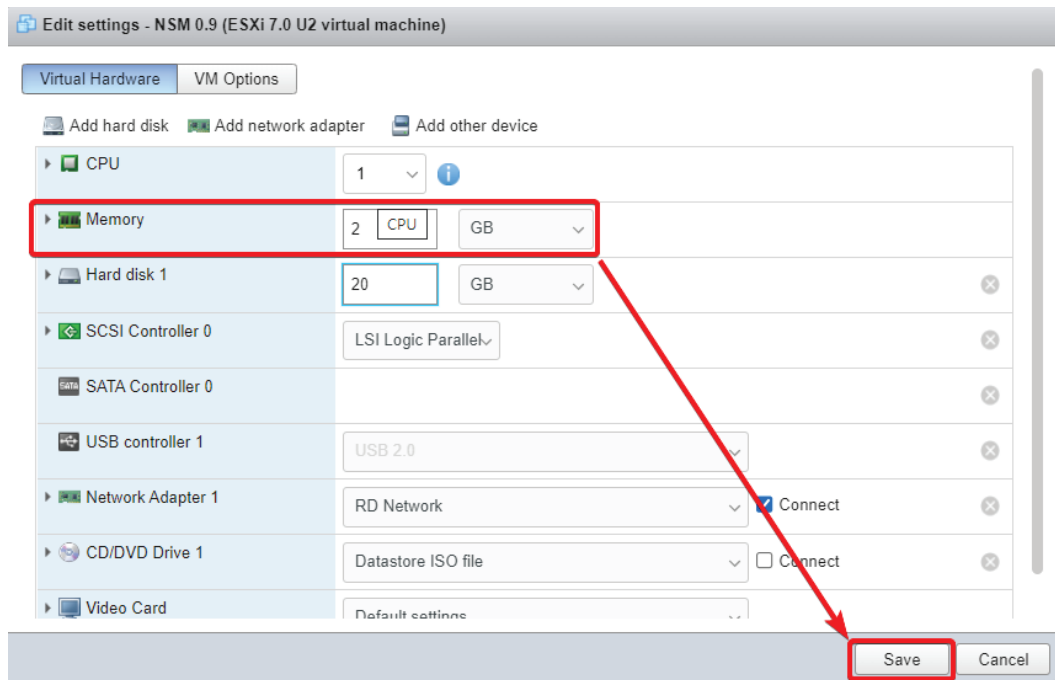
NOTE

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

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



- c. Configure the amount of memory.



- d. Click **Save**.
- e. Boot the MXsecurity instance.

Configuring the MXsecurity system

Accessing the MXsecurity CLI

Steps:

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

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

The password must meet the following requirements:

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

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

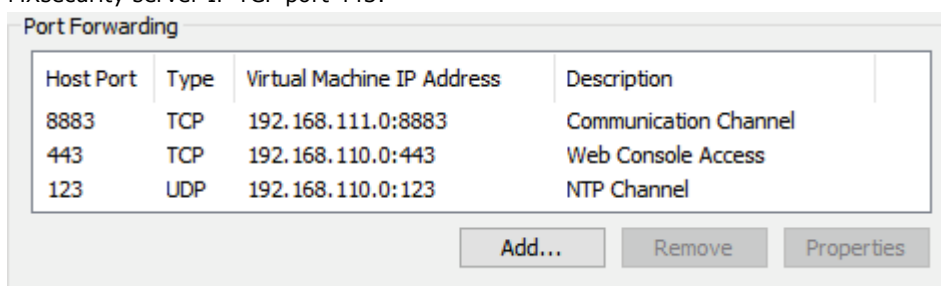
4. **(Optional)** After logging in to the MXsecurity, type the "help" command to see a list of available commands.

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

Getting the IP Address of the MXsecurity Instance

Steps:

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



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

Add... Remove Properties



NOTE

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

Configuring the IP Address Settings

You can manually configure the IP address if necessary.

Steps:

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

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

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

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

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

```
$ interface --ls
```

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

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

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

```
$ resolve --ls
```

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

```
$ reboot
```

3. Migration

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

Migrating to a Newer Version of MXsecurity (VMware Workstation)

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



NOTE

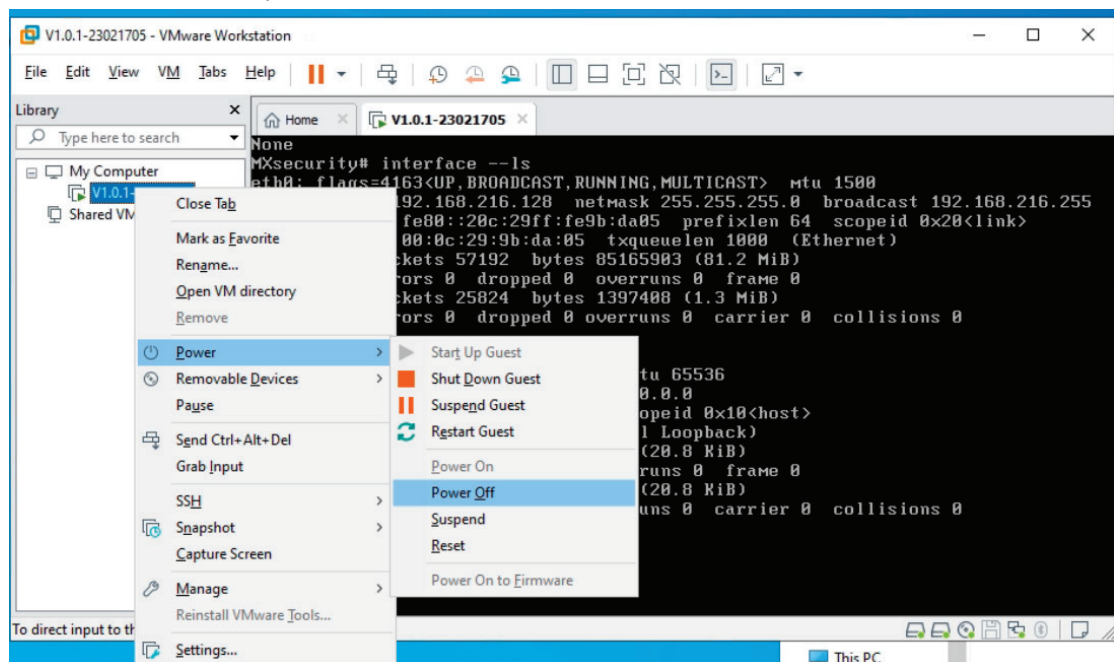
MXsecurity v1.1.0 has implemented enhanced connection security measures. To avoid issues, managed devices should be upgraded to a firmware version and MXsecurity Agent Package which is compatible with MXsecurity v1.1.0. The following device firmware versions are compatible with MXsecurity v1.1.0:

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

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

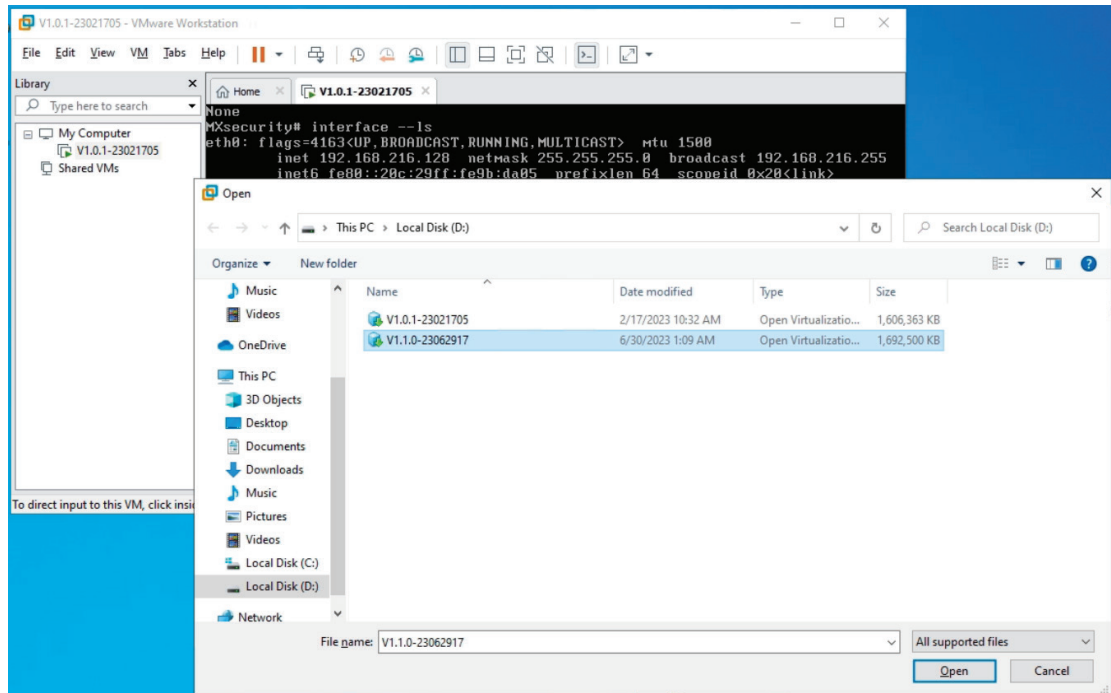
Steps:

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

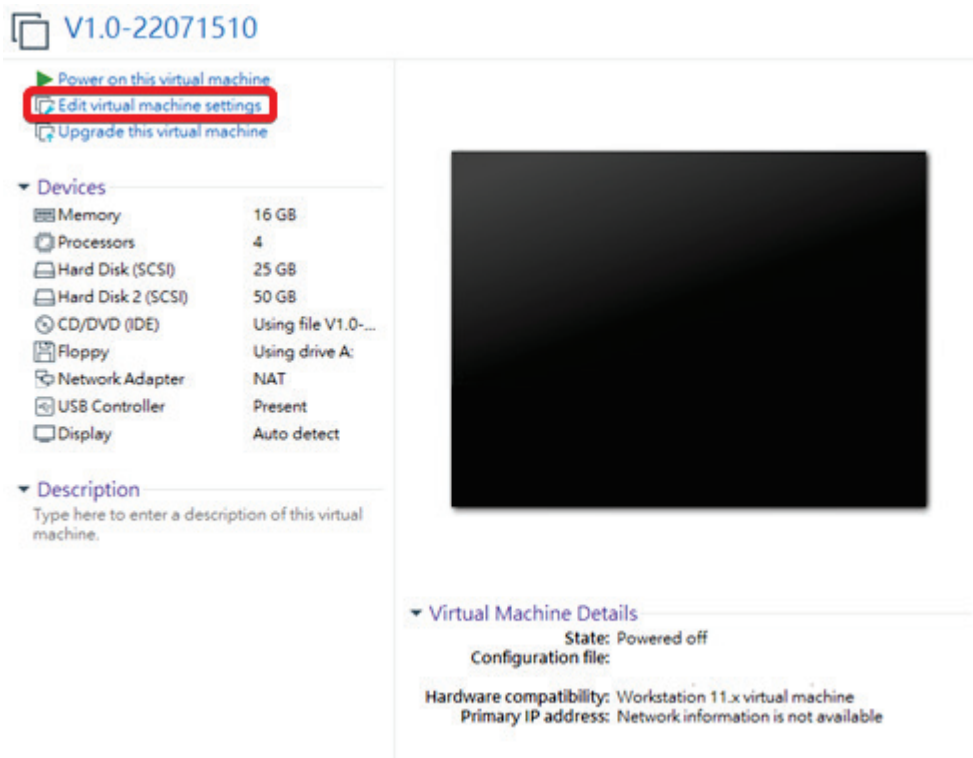


3. Go to **File > Open** in the menu bar.

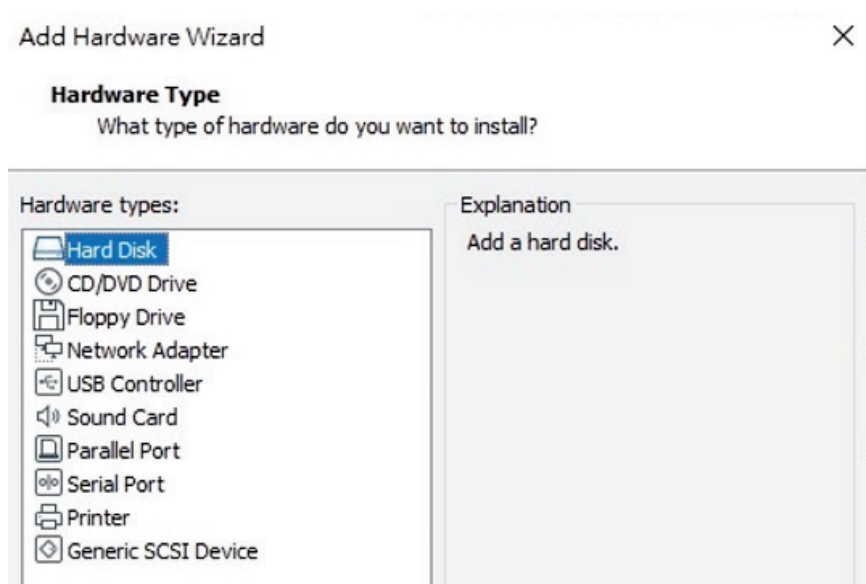
4. Select the VM image file (*.ova) of the new MXsecurity version from your localhost file path and click **Open**.



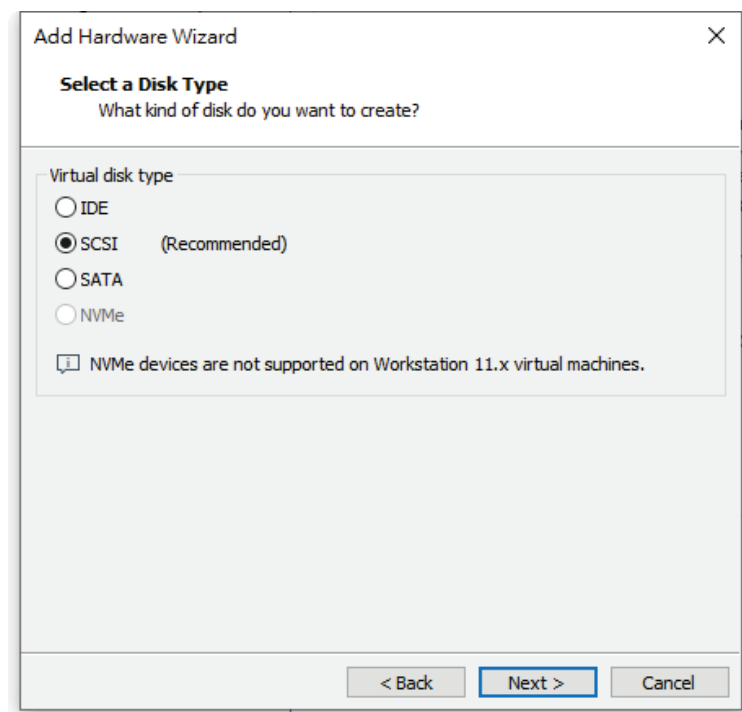
5. Add an existing Hard Disk.
a. Click **Edit virtual machine settings**.



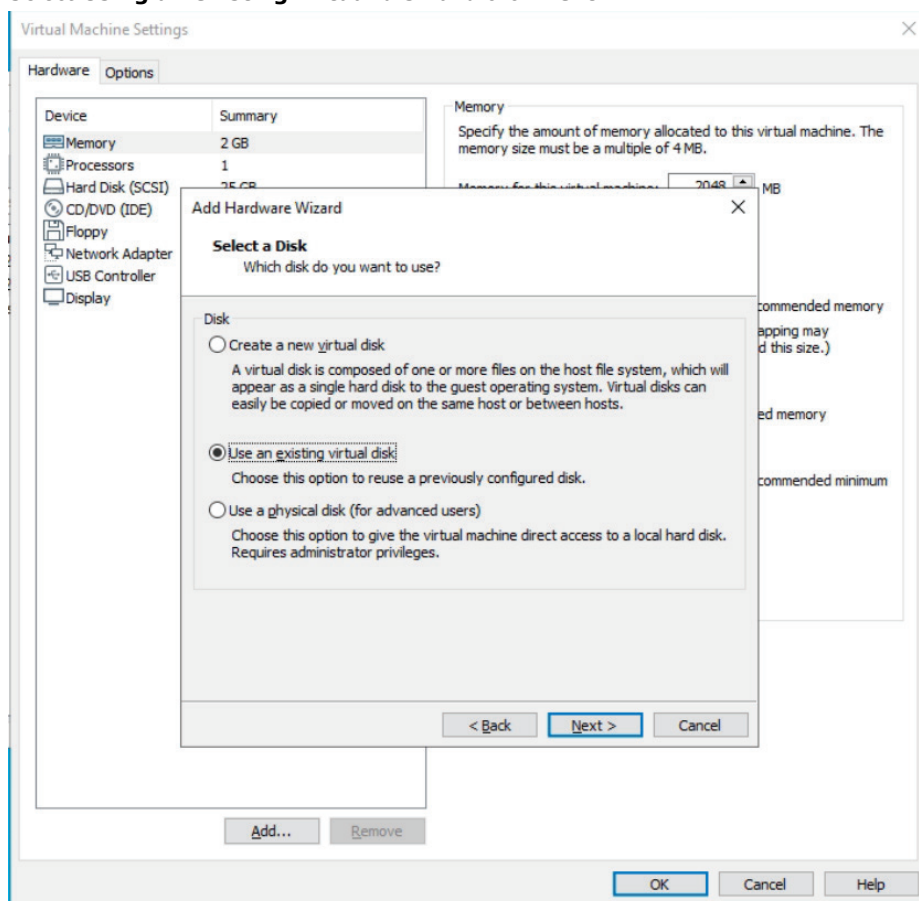
- b. Click **Add**, then choose **Hard Disk**.



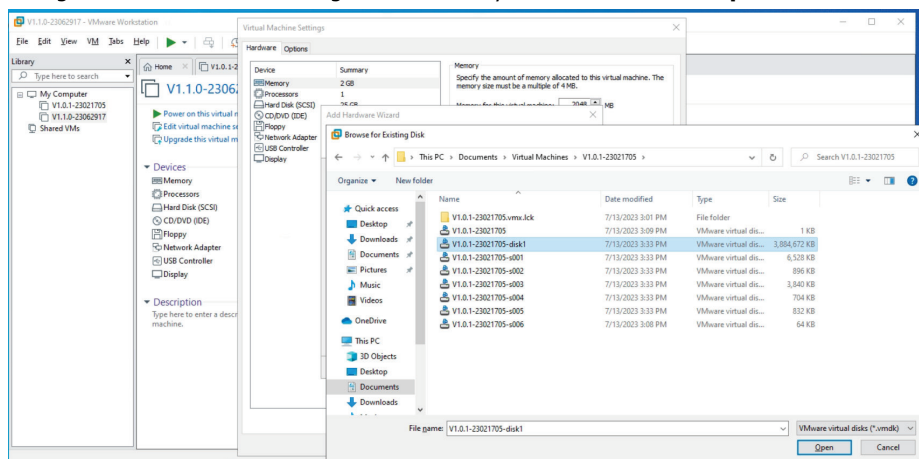
- c. Select a disk type and click **Next**.



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



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



6. Click **Finish**.



NOTE

After installing the new MXsecurity instance, you may need to reconfigure the IP address of the MXsecurity server. Refer to [Configuring the IP Address Settings](#) for instructions.

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

Migrating to a Newer Version of MXsecurity (ESXi)

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



NOTE

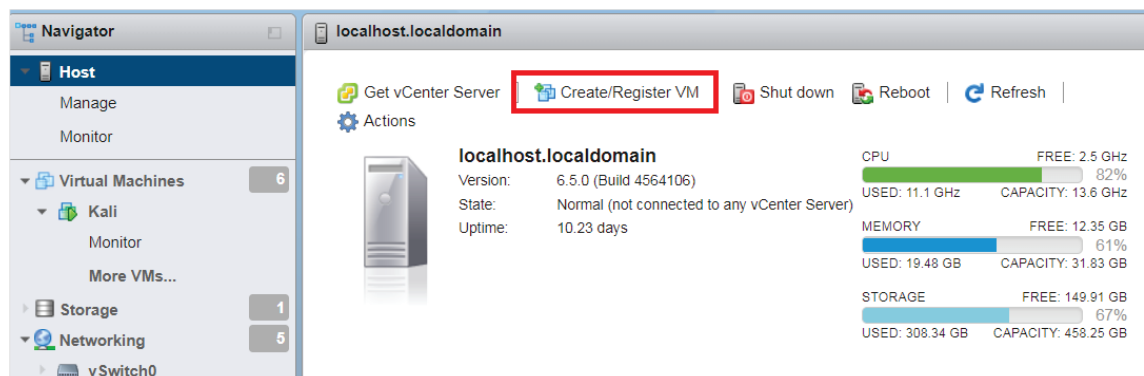
MXsecurity v1.1.0 has implemented enhanced connection security measures. To avoid issues, managed devices should be upgraded to a firmware version and MXsecurity Agent Package which is compatible with MXsecurity v1.1.0. The following device firmware versions are compatible with MXsecurity v1.1.0:

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

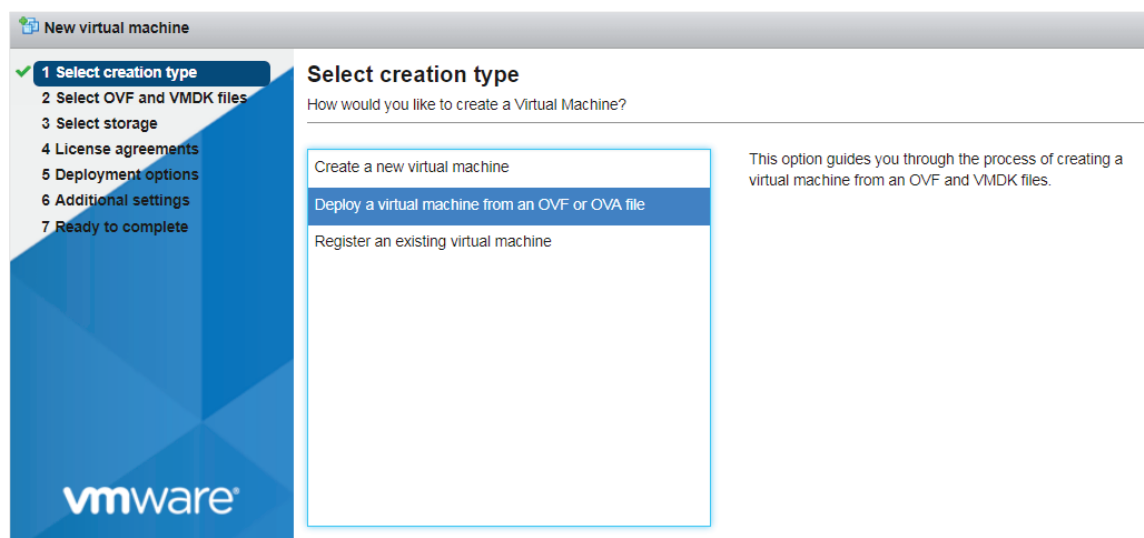
If you have an older version of the MXsecurity Agent Package installed, you will need to manually upgrade it to v2.0.13 on the managed device first. To manually upgrade the software package, navigate to **System > System Management > Software Package Management > MXsecurity Agent Package** in the Secure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

Steps:

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



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



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

The screenshot shows the 'New virtual machine - odc' wizard at the 'Select storage' step. On the left, a progress bar indicates the steps: 1 Select creation type, 2 Select OVF and VMDK files, 3 Select storage (highlighted), 4 Deployment options, and 5 Ready to complete. The main area is titled 'Select storage' and instructs the user to 'Select the datastore in which to store the configuration and disk files.' Below this, it states: '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.' A table lists the available datastores:

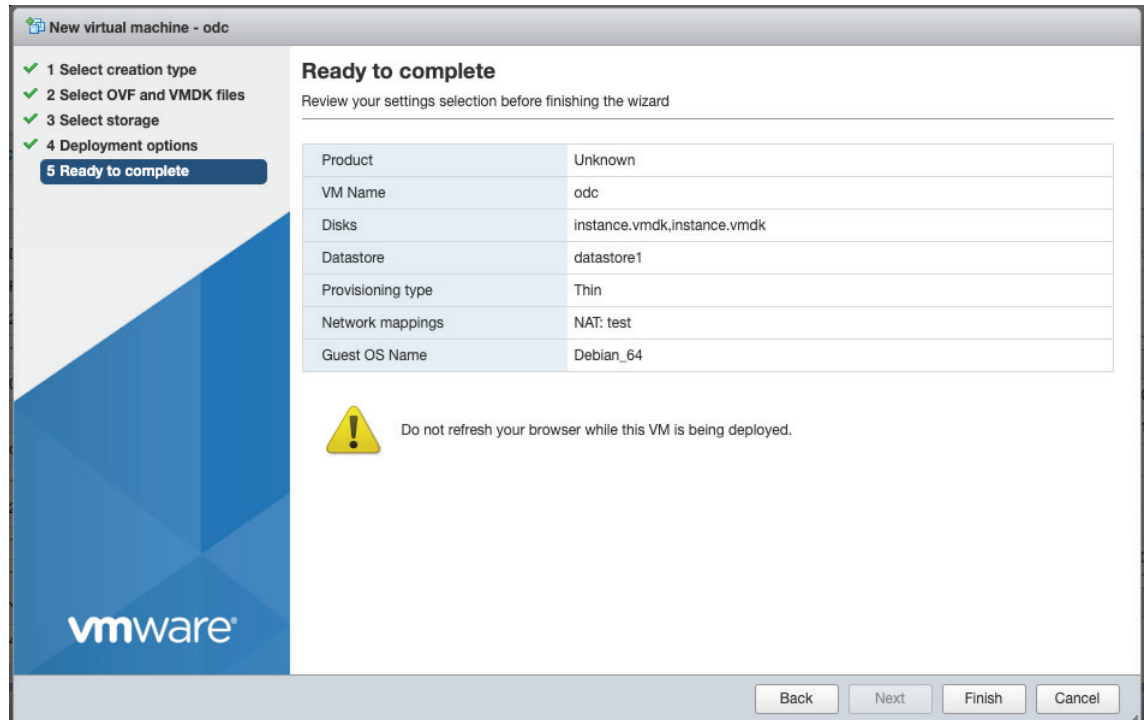
Name	Capacity	Free	Type	Thin pro...	Access
datastore1	3.63 TB	1.63 TB	VMFS5	Supported	Single

At the bottom right of the table, it says '1 items'. At the bottom of the wizard, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

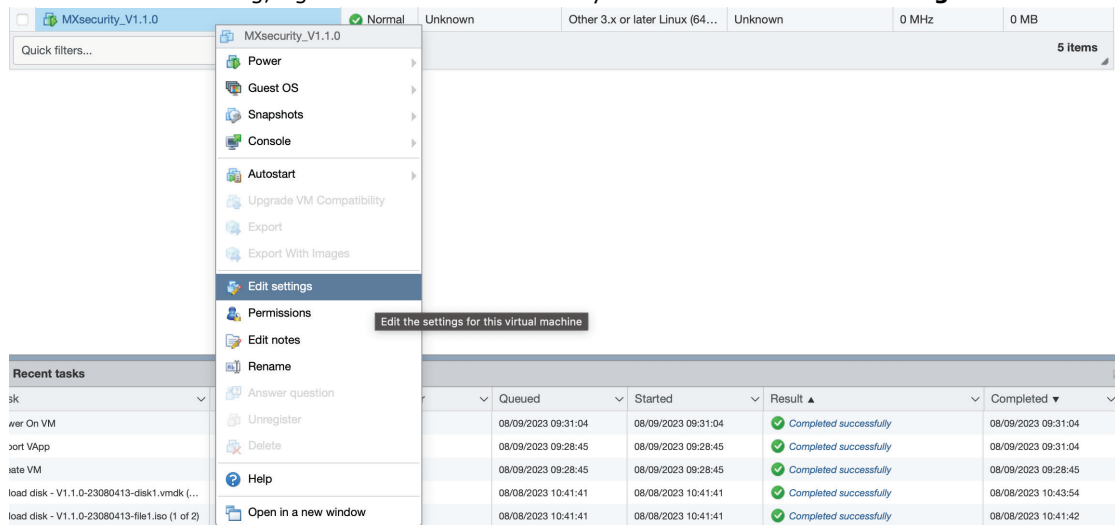
7. Select the deployment options.

The screenshot shows the 'New virtual machine - odc' wizard at the 'Deployment options' step. On the left, the progress bar shows: 1 Select creation type, 2 Select OVF and VMDK files, 3 Select storage, 4 Deployment options (highlighted), and 5 Ready to complete. The main area is titled 'Deployment options' and instructs the user to 'Select deployment options.' Below this, there are two sections: 'Network mappings' and 'Disk provisioning'. The 'Network mappings' section shows 'NAT' selected from a dropdown menu with the value 'test'. The 'Disk provisioning' section shows 'Thin' selected with a radio button, and 'Thick' is unselected. At the bottom of the wizard, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

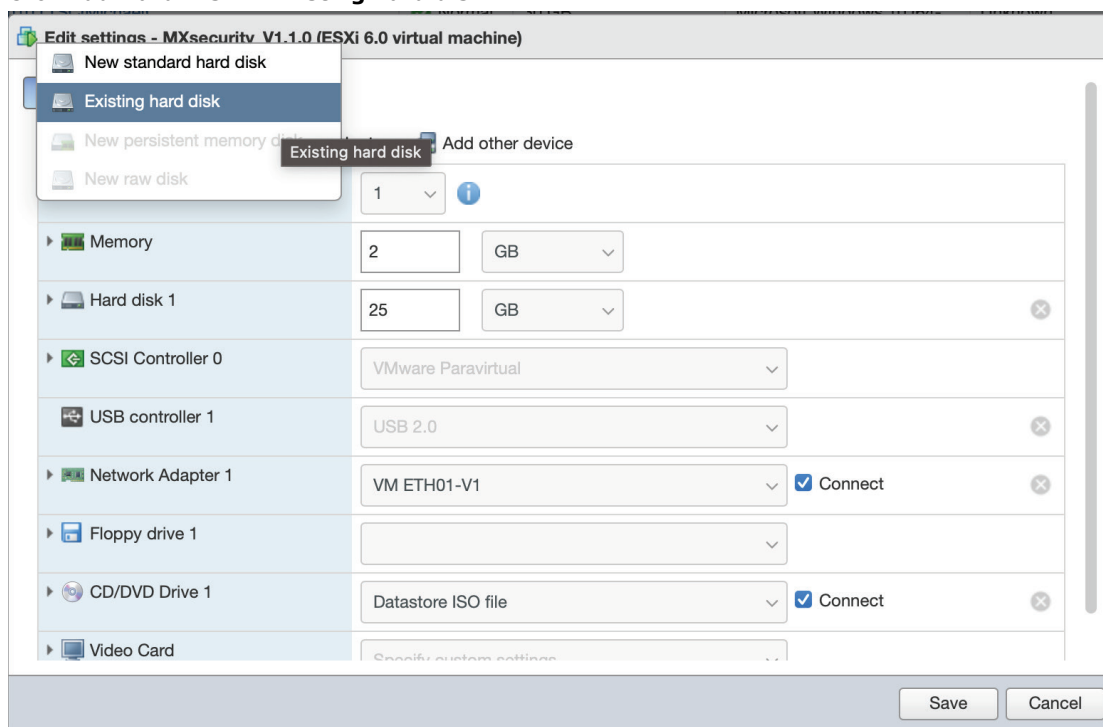
When you see the **Ready to complete** screen, click **Finish** to start the deployment.



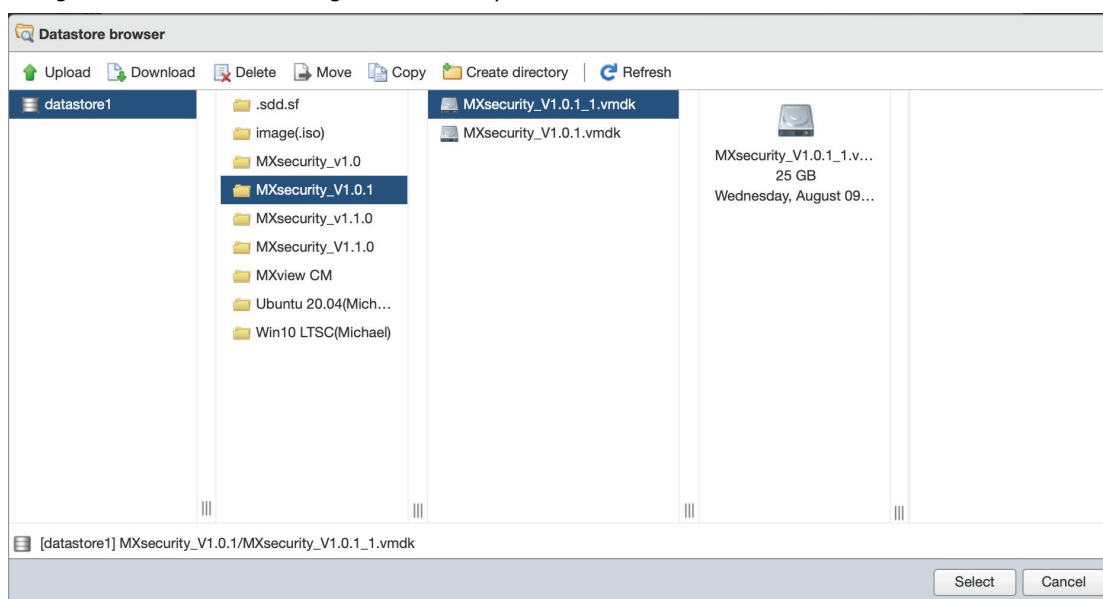
8. Under the **Recent tasks** pane, you will see a progress bar indicating that the MXsecurity image is being uploaded. Wait until the upload has finished.
9. When finished installing, right-click the new MXsecurity instance and click **Edit Settings**.



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



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



12. Click **Save**.



NOTE

After installing the new MXsecurity instance, you may need to reconfigure the IP address of the MXsecurity server. Refer to [Configuring the IP Address Settings](#) for instructions.

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

Migrating Licenses

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



NOTE

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

Steps:

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

Type	Activate Time	Activation code	License Type	License Duration (days)	License Nodes
MXsecurity	2024-06-01 10:00:00		Trial	365	100
MXsecurity	2024-05-15 09:30:00		Trial	180	50
MXsecurity	2024-04-20 14:45:00		Trial	30	10

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

Type	Activate Time	Activation code	License Type	License Duration (days)	License Nodes
MXsecurity	2024-06-01 10:00:00	ABC123XYZ	Trial	365	100
MXsecurity	2024-05-15 09:30:00	DEF456UVW	Trial	180	50
MXsecurity	2024-04-20 14:45:00	GHI789RST	Trial	30	10

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

License Migration

1

Go to the Moxa License Site

2

Copy UUID

3

Activate

1. Log in to the [Moxa License Site](#).

2. Choose "Migrate a Product License".

3. Enter the "UUID" on the Moxa License Site. The UUID can be obtained in the next step.

CANCEL

NEXT

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

License Migration

Go to the Moxa License Site

2

Copy UUID

3

Activate

Copy and paste the UUID into the [Moxa License Site](#).

UUID: SD8408334B0

BACK

NEXT

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

MOXA

Products and Licenses ▾ Download ▾ Software Information Account Management ▾

English Account

Products and Licenses

Migrate a Product License

UUID: SD8408334B0

Query

License Type	Registration Code	v2.1.0 ActivationCode	v2.2.0 ActivationCode
MXsecurity			
Security Package (PS (w/ MXSecurt Y))			
Security Package (PS (w/ MXSecurt Y))			
Security Package (PS (w/ MXSecurt Y))			

Hint 1: Due to changes in the license mechanism, users who activated the license before MXsecurity v2.2.0 are advised to transfer the license to a new format. Failure to do so may result in license reassignment failure for IPS.

Hint 2: The transferred license will be sent as a .csv file, and users can import it into the MXsecurity server.

Hint 3: Display only the licenses that need to be transferred, such as those under the old mechanism and not yet expired.

Migrate

Download

About to expired:

SDC - 0

IEF - 0

IEC - 0

MRC Quick Link - 0

MXview One - 0

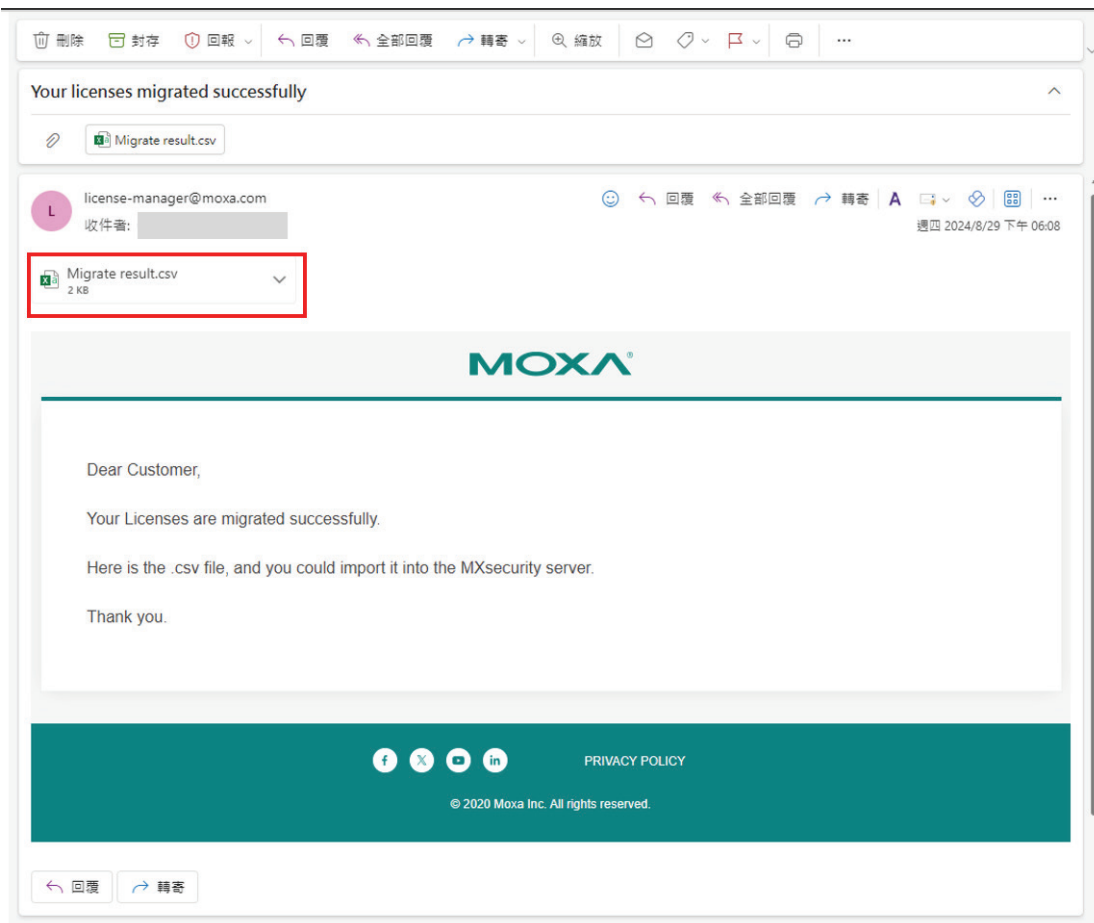
MXview One CM - 0

MXsecurity - 1

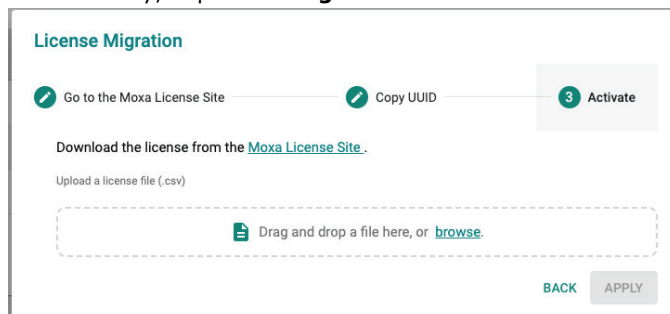
Security Package - 1

Privacy Policy

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



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



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

4. Getting Started

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

Getting Started Task List

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

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

Opening the Management Console

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



NOTE

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

Steps:

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



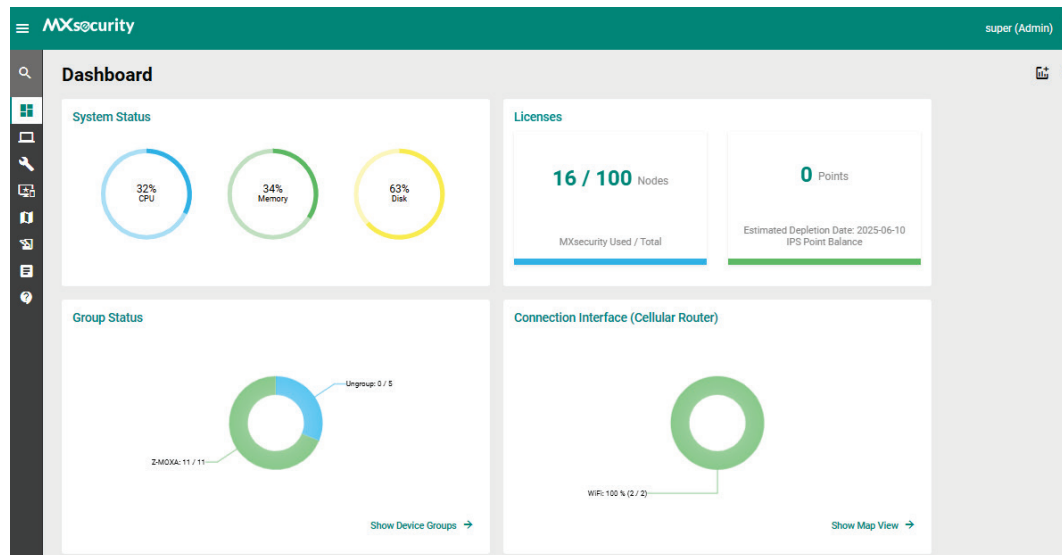
NOTE

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

- a. Enter your new login details.
 - i. Current Password
 - ii. New Password
 - iii. Confirm New Password
- b. Click **Confirm**.

You will be automatically logged out of the system. The login screen will appear again.
- c. Log in again using your new credentials.

The dashboard screen will appear.



Connecting Secure Routers to MXsecurity

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

Steps:

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

MXsecurity

Connection Status

Status: **Connecting** Package Version: **1.0.0017**

Service Address: **192.168.127.1** Profile Synchronization: **---**

New Connection

Service Address: _____ 0 / 64

HTTPS Port: **443**

1 - 65535

Communication Port: **8883**

1 - 65535

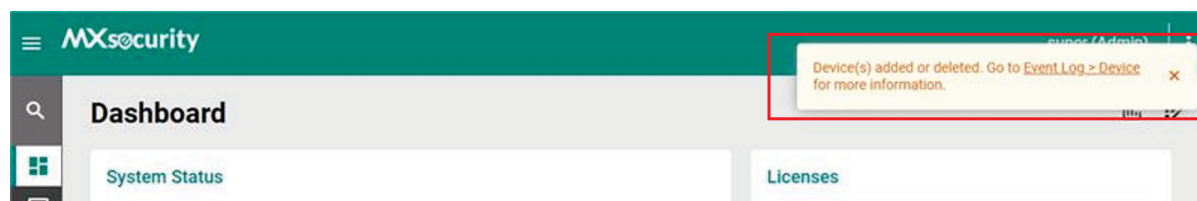
CONNECT

5. Click **CONNECT**.

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

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

After the device is successfully connected to MXsecurity, a message will appear in the top-right corner when users log in to notify them that new devices have been added to MXsecurity.



5. Dashboard and Widgets

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



NOTE

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

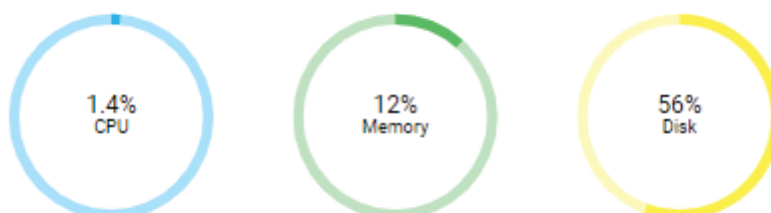
Dashboard Widgets Overview

This section describes available widgets on the dashboard.

System Status

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

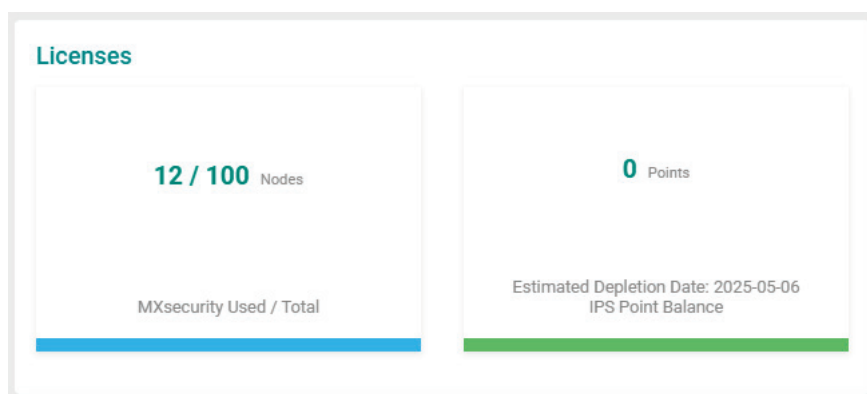
System Status



Licenses

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

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



Group Status

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

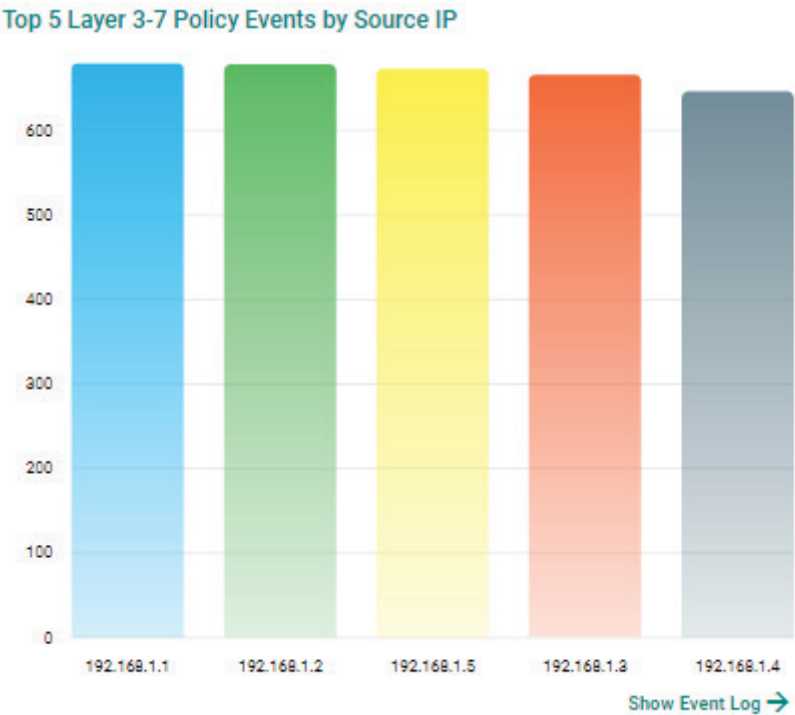
Group Status



[Show Device Group →](#)

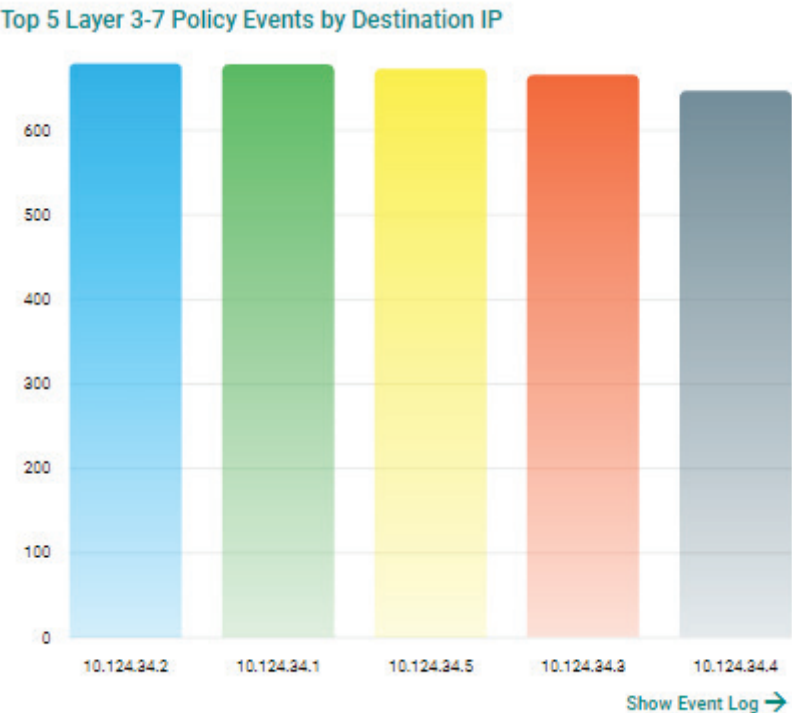
Top 5 Layer 3-7 Policy Events by Source IP

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



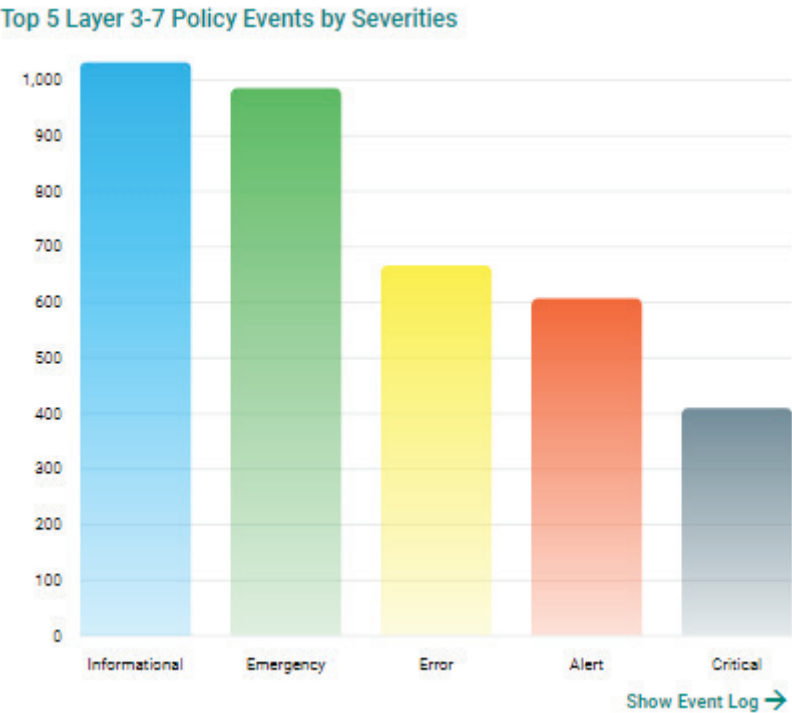
Top 5 Layer 3-7 Policy Events by Destination IP

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



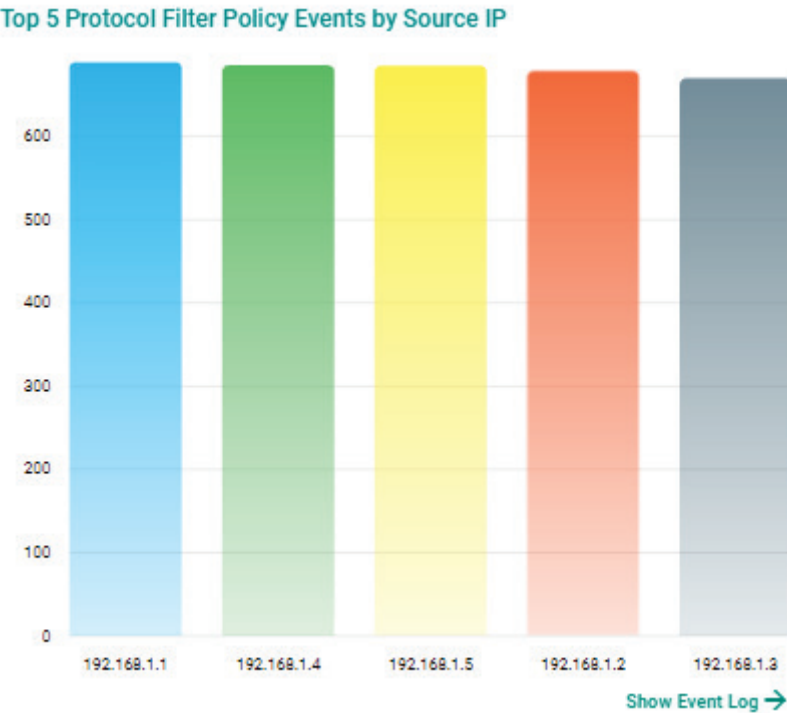
Top 5 Layer 3-7 Policy Events by Severity

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



Top 5 Protocol Filter Policy Events by Source IP

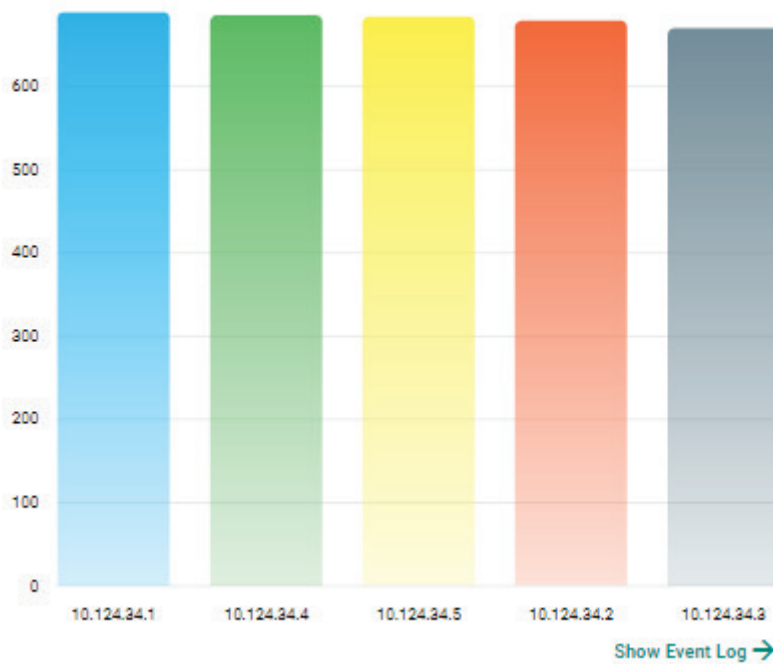
This widget displays the top 5 source IP addresses in the selected device group(s) where the most Protocol Filter Policy Events were detected within the last 24 hours



Top 5 Protocol Filter Policy Events by Destination IP

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

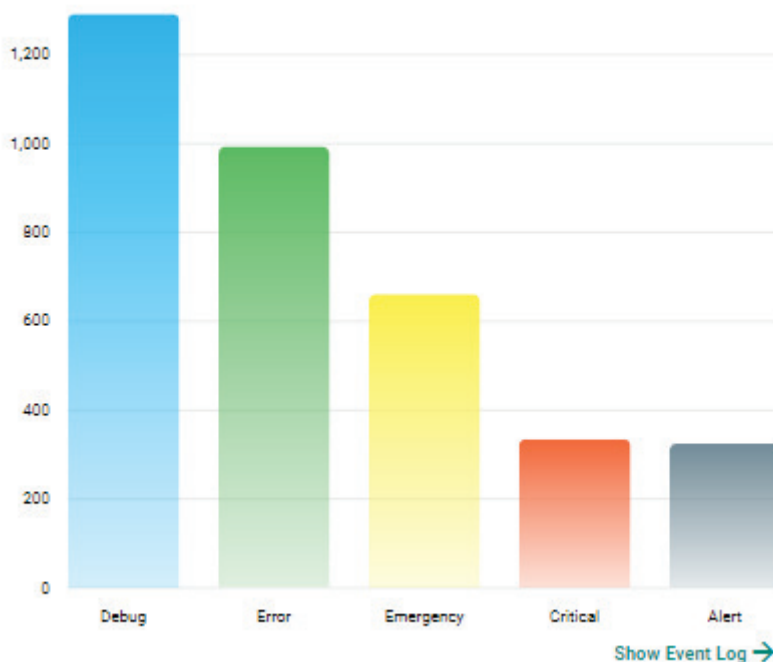
Top 5 Protocol Filter Policy Events by Destination IP



Top 5 Protocol Filter Policy Events by Severity

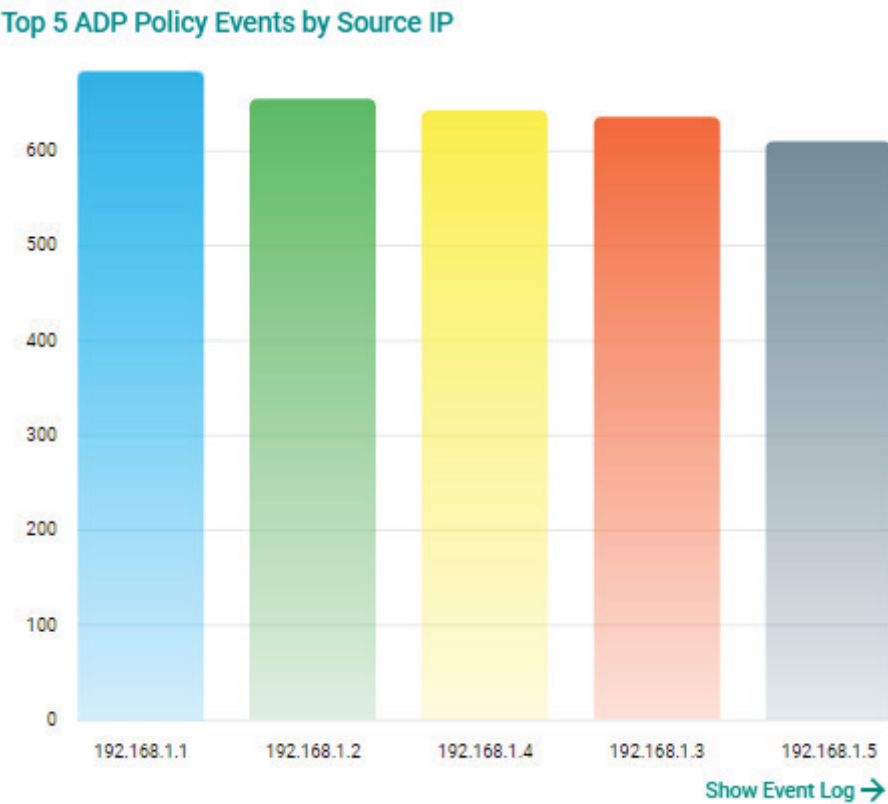
This widget displays the number of the Protocol Filter Policy Events in the selected device group(s) within the last 24 hours categorized by severity level.

Top 5 Protocol Filter Policy Events by Severities



Top 5 ADP Events by Source IP

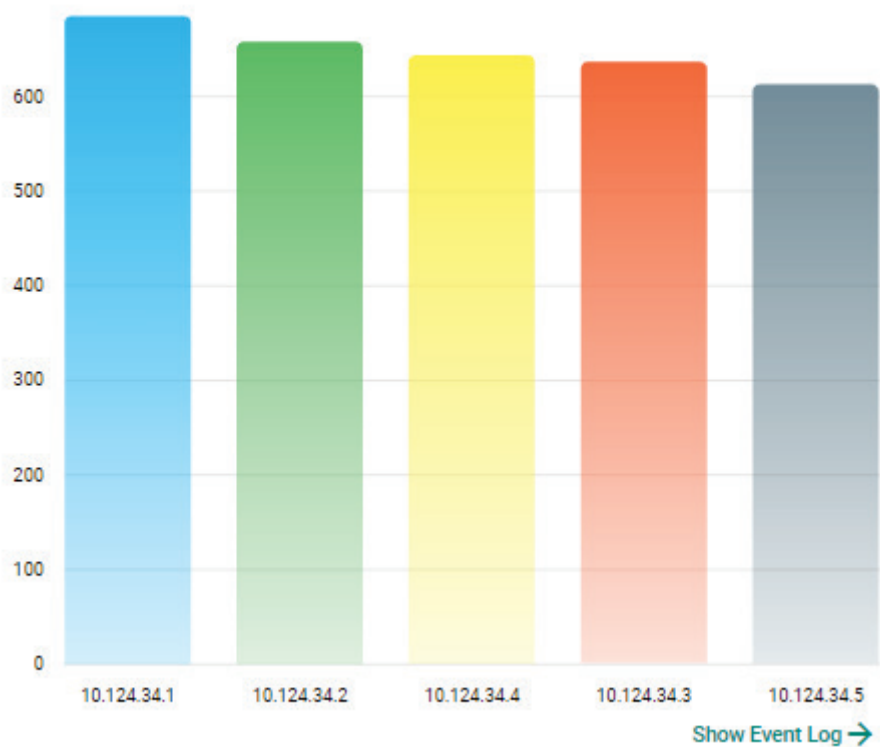
This widget displays the top 5 source IP addresses in the selected device group(s) where the most ADP Events were detected within the last 24 hours.



Top 5 ADP Events by Destination IP

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

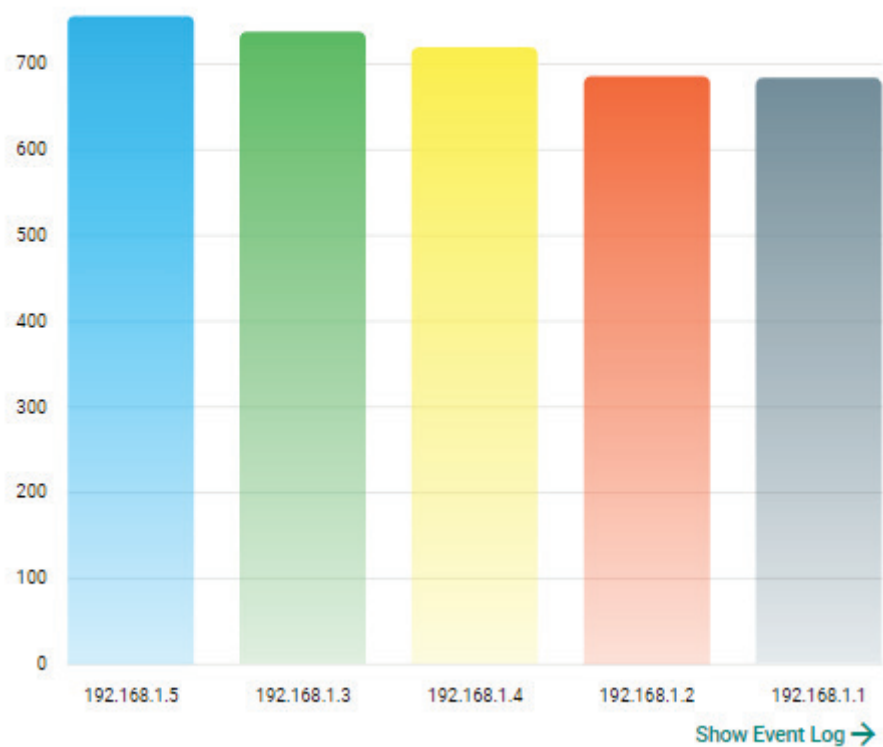
Top 5 ADP Policy Events by Destination IP



Top 5 IPS Events by Source IP

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

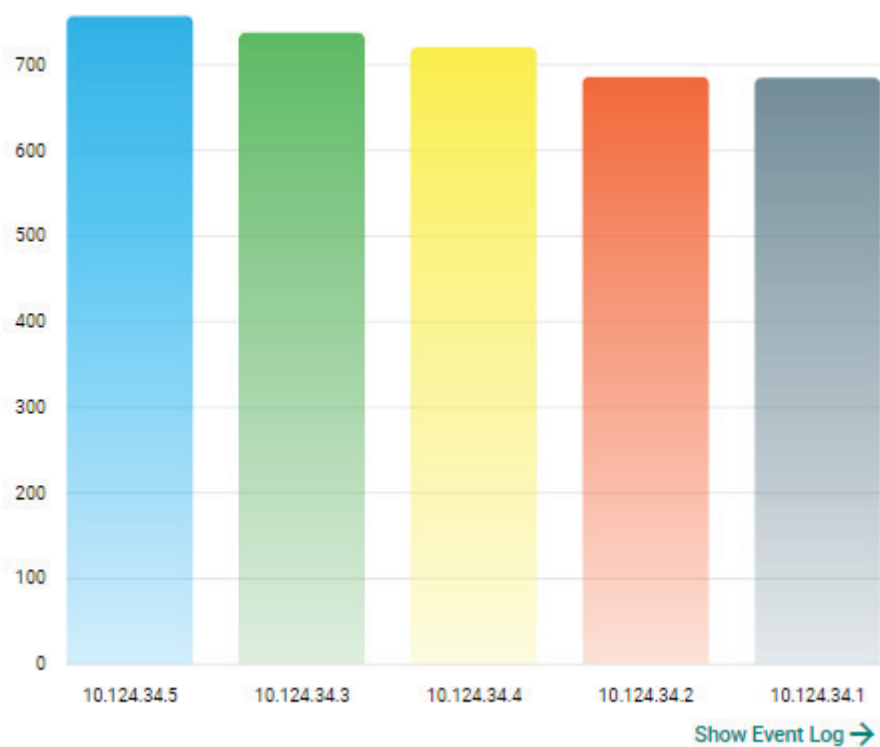
Top 5 IPS Policy Events by Source IP



Top 5 IPS Events by Destination IP

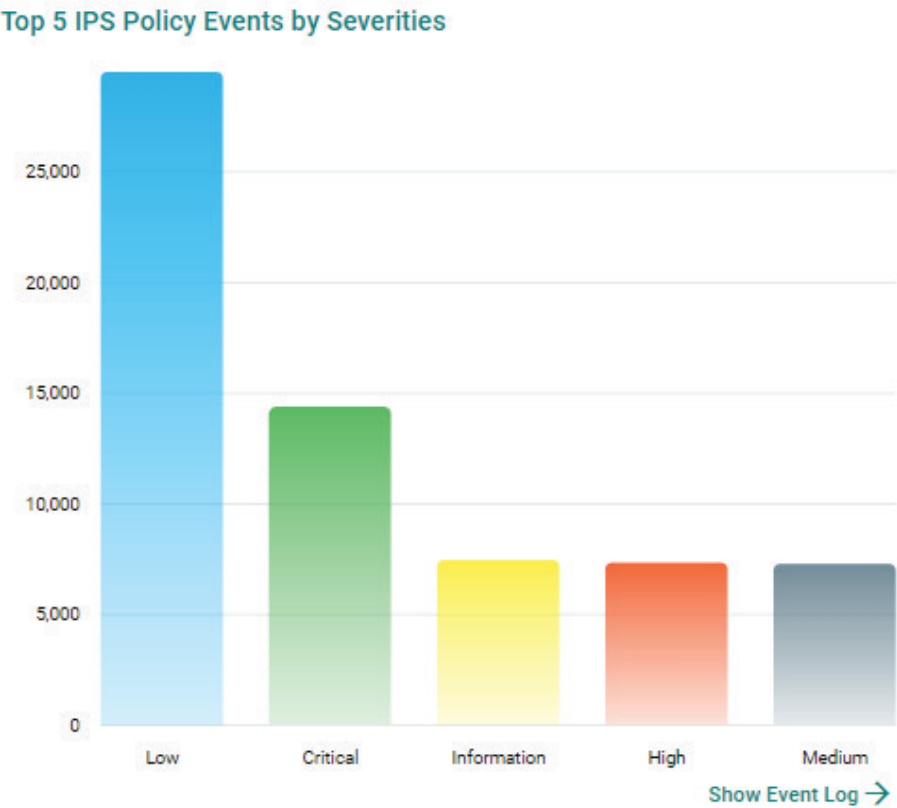
This widget displays the top 5 destination IP addresses in the selected device group(s) where the most IPS Events were detected within the last 24 hours.

Top 5 IPS Policy Events by Destination IP



Top 5 IPS Events by Severity

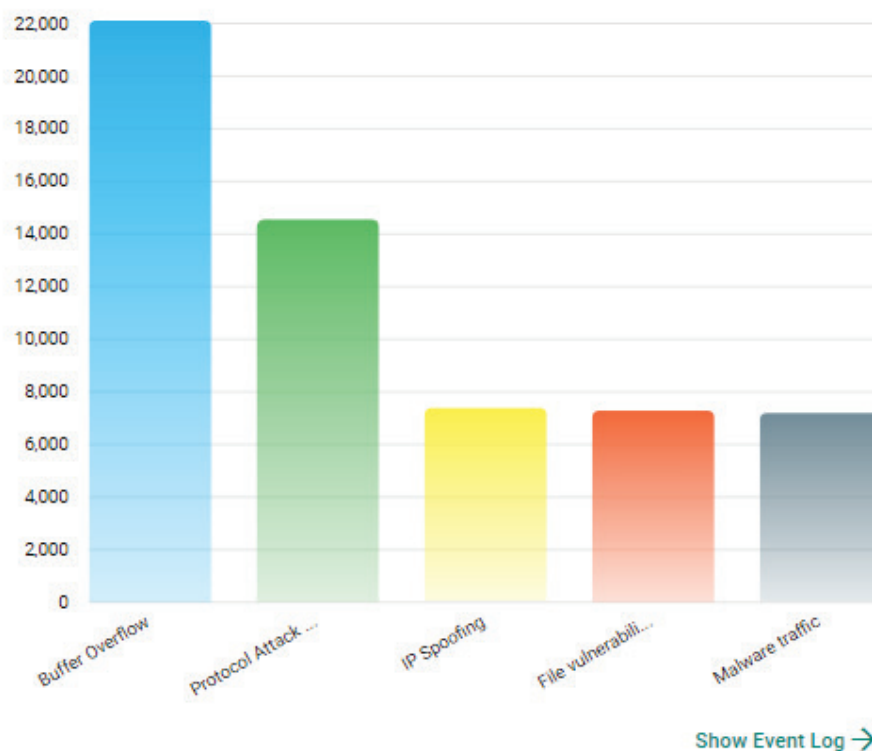
This widget displays the number of IPS Events in the selected device group(s) within the last 24 hours categorized by severity level.



Top 5 IPS Events by Category

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

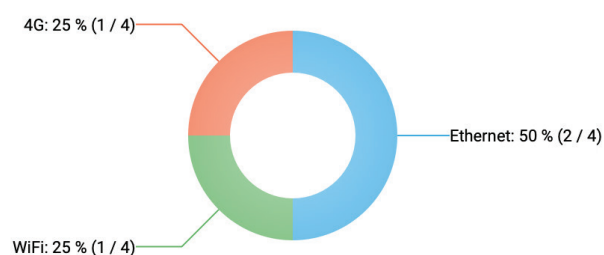
Top 5 IPS Policy Events by Category



Connection Interface (Cellular Router)

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

Connection Interface (Cellular Router)

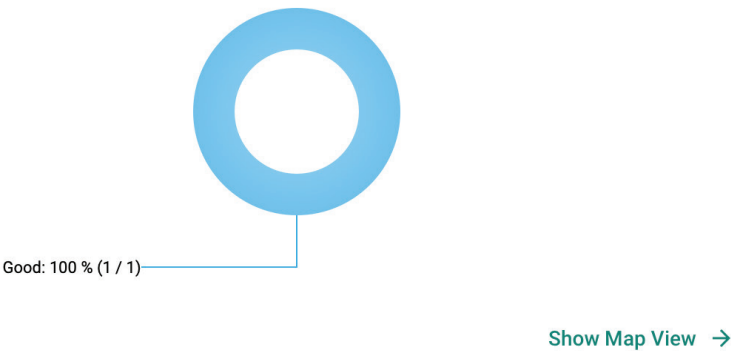


[Show Map View →](#)

Signal Quality (Cellular Router)

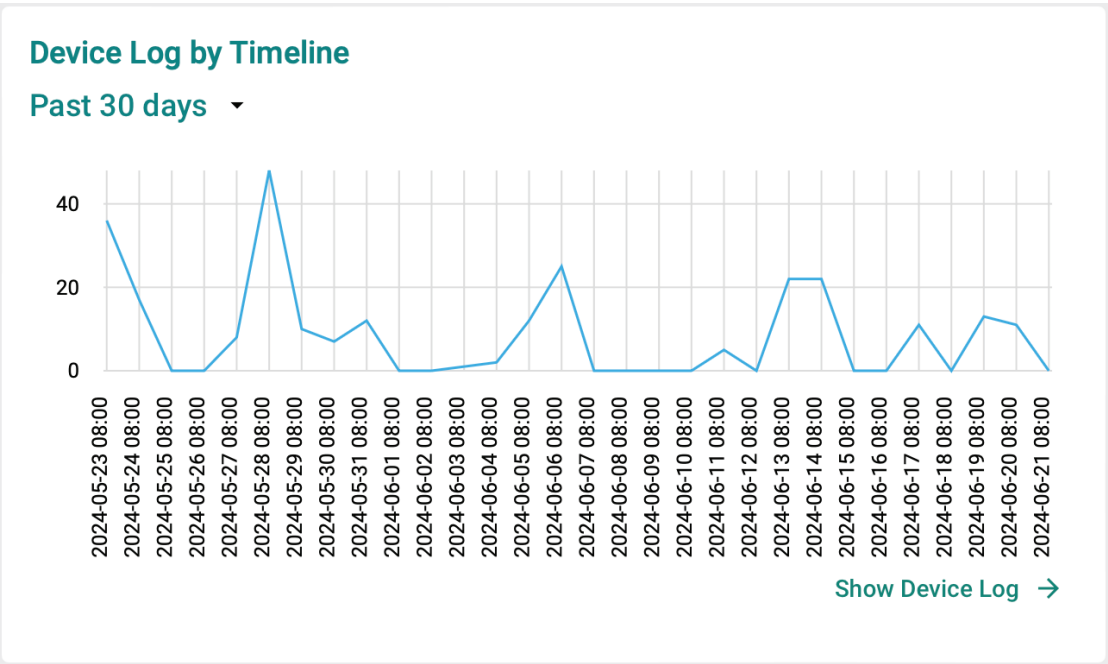
This widget displays a summary of the cellular interface signal quality across all OnCell Series routers, including Good, Fair, Poor, and No Signal.

Signal Quality (Cellular Router)



Device Log by Timeline

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

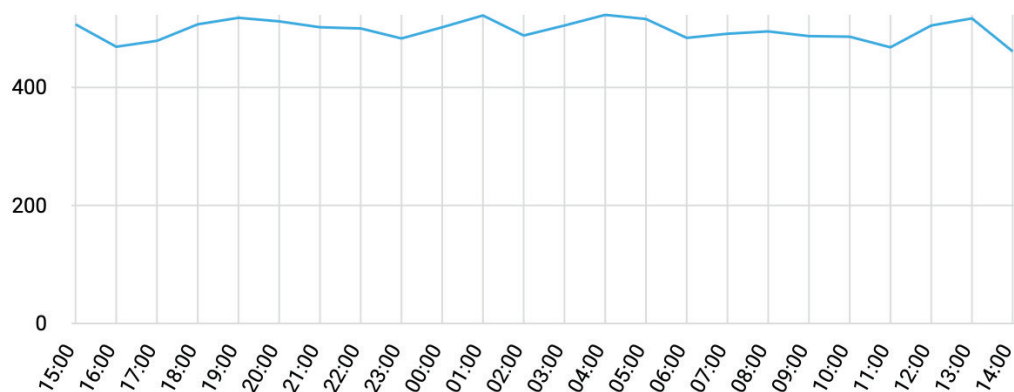


Firewall Log by Timeline

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

Firewall Log by Timeline

Trusted Access ▾ Past 24 hours ▾



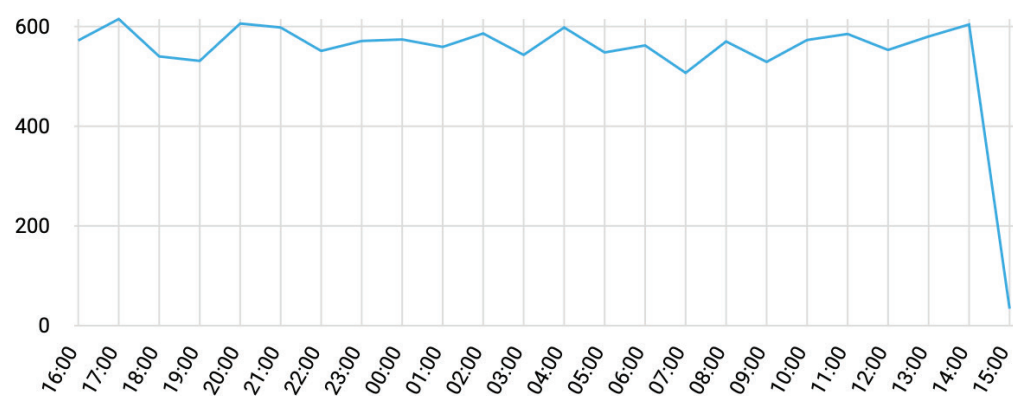
[Show Firewall Log →](#)

VPN Log by Timeline

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

VPN Log by Timeline

Past 24 hours ▾



[Show VPN Log →](#)

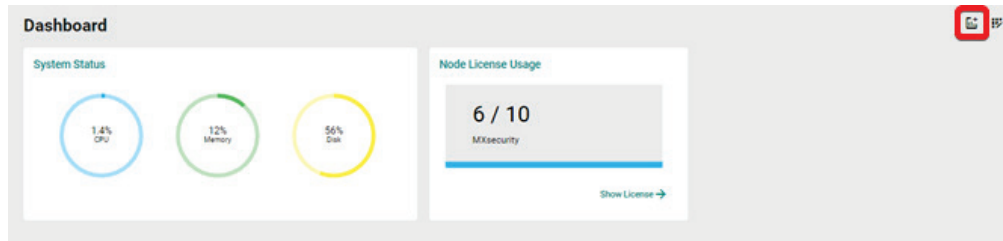
Widget Management

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

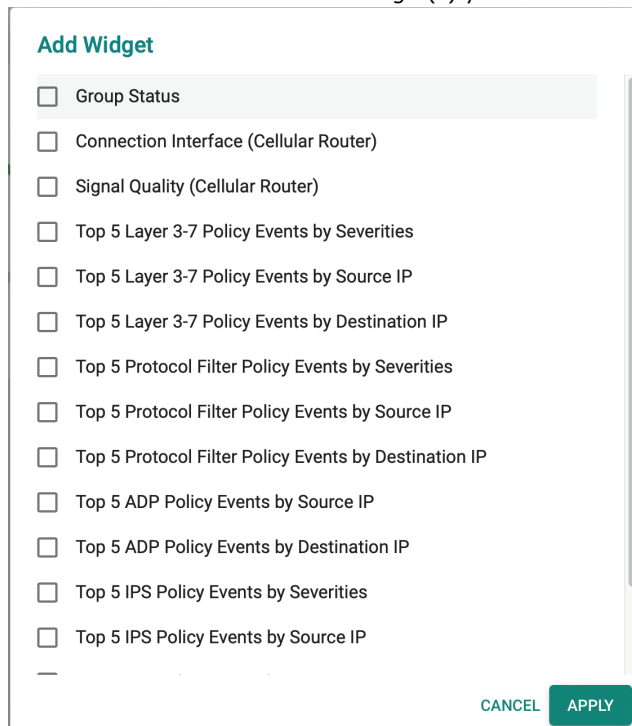
Adding a Widget to the Dashboard

Steps:

1. Click the  icon to add widgets.



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

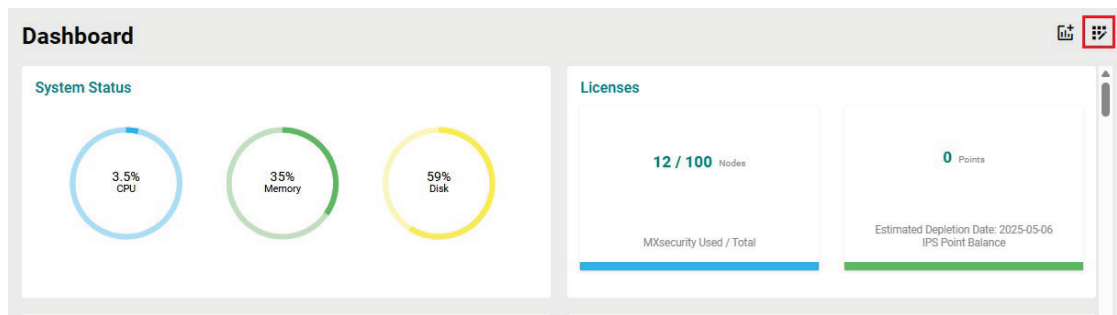


3. Click **APPLY** to add the selected widget(s) to the tab.

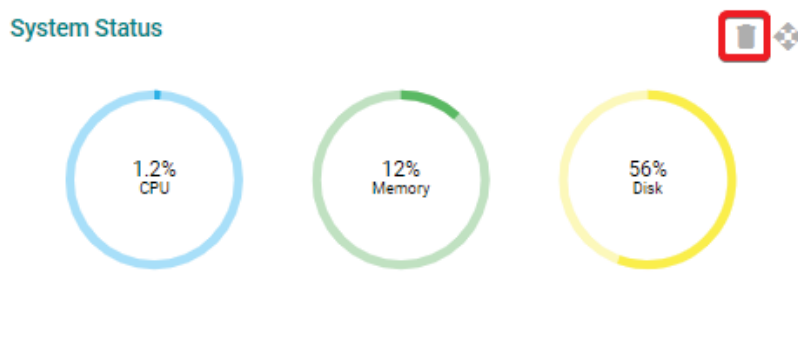
Removing a Widget from the Dashboard

Steps:

1. Click the  icon to edit the dashboard.



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

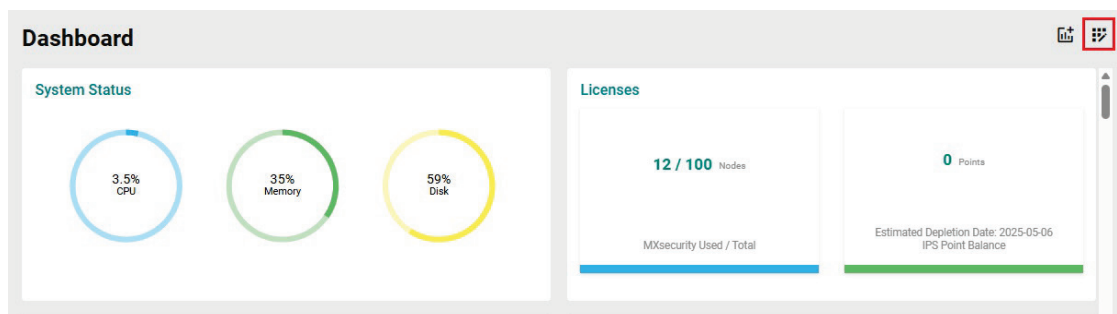


3. Click the  icon again to save your changes and leave edit mode.

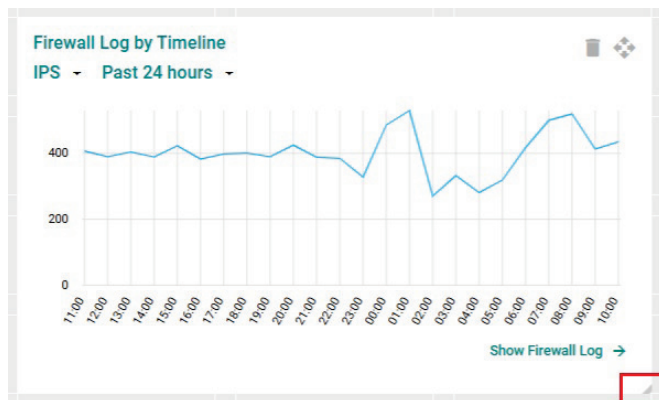
Resizing a Widget

Steps:

1. Click the  icon to edit the dashboard.



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



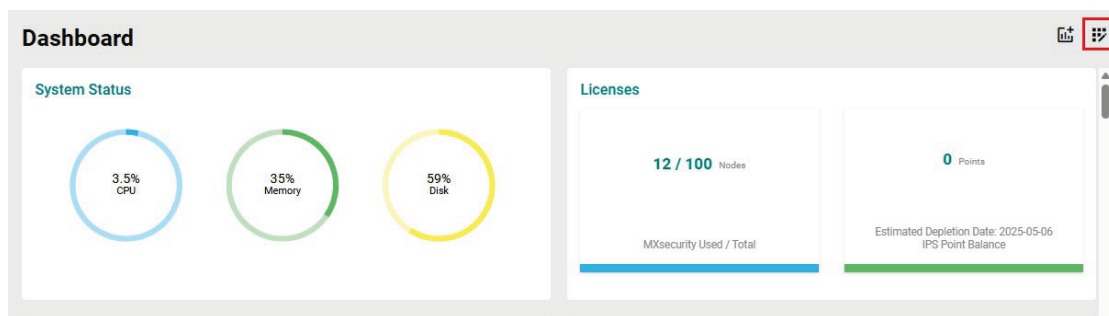
3. Click and drag the corner of the widget to the desired size, then release the mouse. The dark grey area in the Dashboard background indicates the final size of the widget.

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

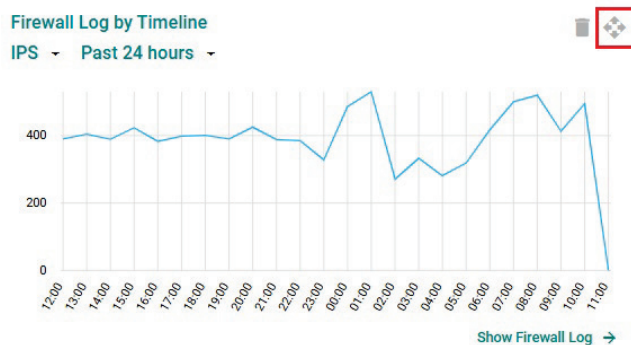
Moving the Widget Position

Steps:

1. Click the  icon to edit the dashboard.



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



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

6. Management

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



NOTE

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

Device Group Management

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

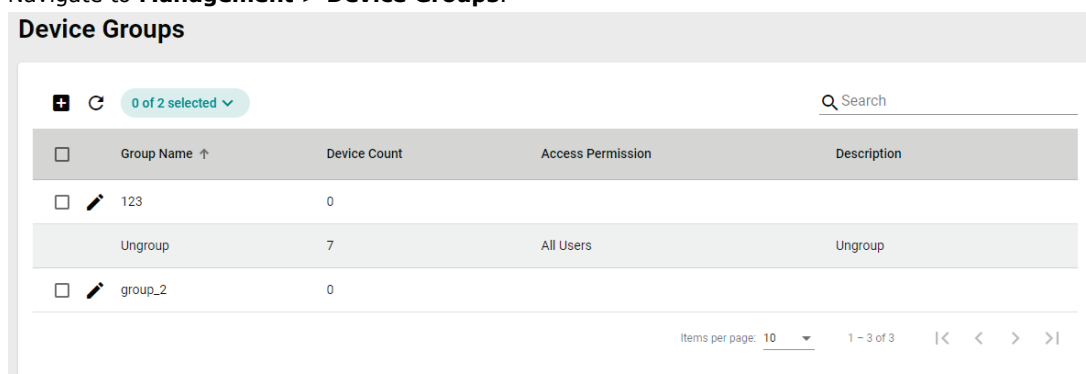
The configurations and policies that can be shared are:

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

Creating a New Device Group

Steps:

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



2. Click the  icon to create a new group.
3. Provide a name and description for the group and click **NEXT**.
The group name can be up to 32 characters long and supports a-z, A-Z, 0-9, periods (.), and underscores (_).

Create Group

1 Enter Group Information 2 Add Devices 3 Grant Access Permission

Group Name *  0 / 32

Description 0 / 255

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

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

Create Group

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

0 of 6 Selected

Search

☐	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

Items per page: 10 1 – 6 of 6

BACK NEXT

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

Create Group

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

0 of 2 Selected

Search

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

Items per page: 10 1 – 3 of 3

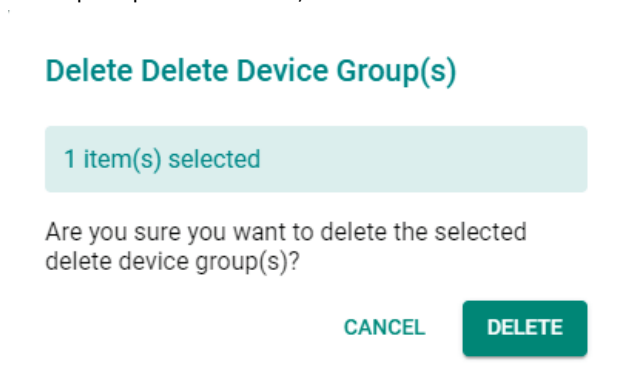
BACK APPLY

Deleting a Device Group

Steps:

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

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

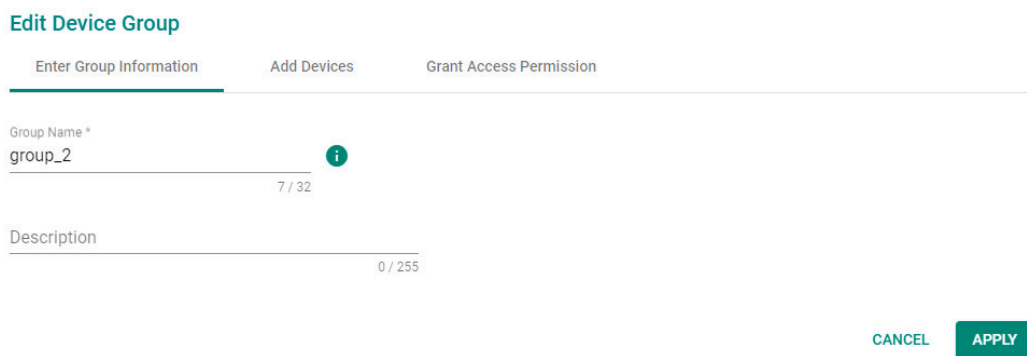


A confirmation dialog box titled "Delete Delete Device Group(s)" in teal. Below the title is a teal box with the text "1 item(s) selected". The main text asks, "Are you sure you want to delete the selected delete device group(s)?". At the bottom right are two buttons: "CANCEL" and "DELETE".

Editing a Device Group

Steps:

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



The "Edit Device Group" form has three tabs: "Enter Group Information", "Add Devices", and "Grant Access Permission". The "Enter Group Information" tab is active. It contains a "Group Name *" field with the text "group_2" and a character count "7 / 32". There is an information icon (i) next to the field. Below it is a "Description" field with a character count "0 / 255". At the bottom right are "CANCEL" and "APPLY" buttons.

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

Firmware Management

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

Uploading New Firmware

Steps:

- Navigate to **Management > Firmwares**.

- Click the  icon to add a new firmware.

Firmwares					
  0 of 3 selected		 Search			
☐	Model Series ↑	Version	Build Time	Description	Schedule In Use
☐	 EDR-G9010	V2.1	2021-05-19 16:00:00		Yes
☐	 EDR-G9010	V3.1	2021-05-19 16:00:00		Yes
☐	 OnCell G4302	V1.1	2021-05-19 16:00:00		
Items per page: 10 1 - 3 of 3 < < > >					



NOTE

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

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

Upload Firmware

Description 0 / 255

Upload a firmware file (.rom)

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

[CANCEL](#) [UPLOAD](#)

- Click **UPLOAD**.

Deleting Firmware

Steps:

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

Delete Firmware(s)

1 item(s) selected

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

[CANCEL](#)

[DELETE](#)

Exporting Firmware

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

Steps:

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

Software Package Management

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

The following packages can be managed in MXsecurity:

- Network Security Package

This section contains the following tabs:

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

Checking the Security Package Status

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

Software Packages Update Check 

Server

:  Connected [CHECK NOW](#)

Last Connection Check

: 2024-06-21 15:11:58

Last Software Package Update Result

: No new version detected (2024-06-21 15:11:58, manually)

CHECK SOFTWARE PACKAGE

The widget shows the following information:

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

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

the **Sync Settings** tab. Refer to [Setting Up a Scheduled Security Package Update Check](#).

Software Package Check

0 of 0 selected

Search

☐ Version
EDF-G1002
Software Package already up-to-date.
EDR-8010
Software Package already up-to-date.
EDR-G9004
Software Package already up-to-date.
EDR-G9010
Software Package already up-to-date.
OnCell-G4302

CLOSE

Uploading a New Software Package

Steps:

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

Software Packages

Network Security Packages

0 of 5 selected

Search

☐	Version	Supported Series	Build Time	Description	Profile In Use	Schedule In Use
☐	5.5.0009	OnCell-G4302	2023-05-26 18:00:00		0	
☐	8.0.0001	EDR-8010	2023-06-27 18:00:00		1 ...	Yes
☐	7.0.0008	EDR-8010	2023-06-27 18:00:00		0	
☐	6.0.0009	EDR-G9010	2023-05-26 18:00:00		0	
☐	7.0.0008	OnCell-G4302	2023-06-27 18:00:00		0	

Items per page: 10 1 - 5 of 5 |< < > >|



NOTE

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



NOTE

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

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

Upload Package

Description 0 / 255

Upload a package file (.pkg)

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

[CANCEL](#) [UPLOAD](#)

4. Click **UPLOAD**.

Deleting a Software Package

Steps:

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

Delete Software Package(s)

1 item(s) selected

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

[CANCEL](#) [DELETE](#)

Exporting Software Packages

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

Steps:

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

Viewing Detailed Information of a Software Package

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

Steps:

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

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

Software Packages

Network Security Packages

0 of 6 selected

Search

☐	Version	Supported Series	Build Time	Description	Profile in Use	Schedule in Use
☐	  5.5.0007	OnCell-G4302	2023-04-12 02:00:00		0	Yes
☐	  5.5.0012	OnCell-G4302	2023-06-28 02:00:00		0	
☐	  6.0.0012	EDR-G9010	2023-06-09 02:00:00		1 ...	Yes
☐	  6.0.0013	EDR-G9010	2023-06-28 02:00:00		0	
	Supported Functions: Modbus(TCP), DNP3, IEC-104, MMS, IPS					
☐	  7.0.0001	EDR-8010	2023-04-22 02:00:00		0	
☐	  6.0.0006	EDR-8010	2023-04-27 02:00:00		0	Yes

Items per page: 10 1 - 6 of 6 {< >}



NOTE

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



NOTE

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

Viewing Network Security Package Logs

Steps:

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

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



- Click the  button to renew the search results.



The following table describes the log's fields.

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

Setting Up a Scheduled Security Package Update Check

Steps:

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

The screenshot shows the 'Sync Settings' tab in a web interface. At the top, there are three tabs: 'Software Packages File', 'Log', and 'Sync Settings', with 'Sync Settings' being the active tab. Below the tabs, there is a 'Product Model *' dropdown menu with the value 'EDF-G1002,EDR-8010,EDR-G9004,E...'. Under the 'Scheduling' section, there is a sub-header 'Sync Software Package by Schedule' and two radio buttons: 'Enabled' (selected) and 'Disabled'. Below this, there is a 'Scheduling Mode' section with two radio buttons: 'Daily' (selected) and 'Weekly'. A 'Time *' field is set to '20:30' with a clock icon. At the bottom, there is a 'Period *' field showing the date range '2024-06-21 - 2025-06-21' with a calendar icon and a close button. An 'APPLY' button is located at the bottom left of the form.

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

Object Management

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

You can configure the following types of objects in MXsecurity:

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

Creating a New Filter Object

Steps:

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

3. Click the  icon to create a new object.

Objects

Filter Interface

 0 of 13 selected

Search

☐	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.

Create Object

Object Name * 

0 / 32

Object Type *

CANCEL **CREATE**

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

Create Object

Object Name * 

0 / 32

Object Type *

- IP Address & Subnet
- Network Service
- Industrial Application Service
- User-defined Service

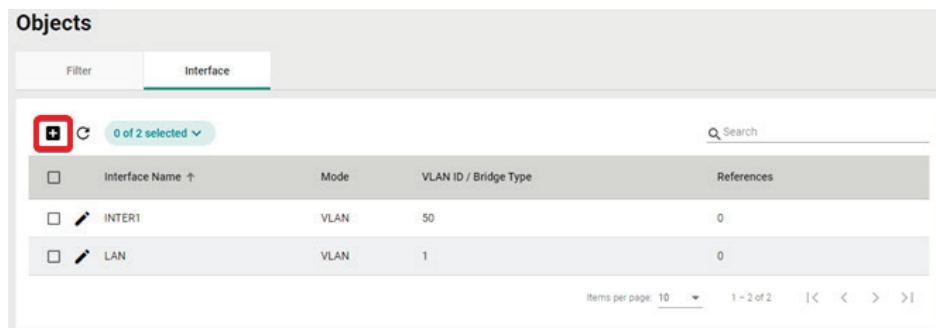
CANCEL **CREATE**

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

Creating a New Interface Object

Steps:

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



4. Enter a name for the object.

Create Interface

Interface Name 
0 / 32

Mode

☒ VLAN ☐ Bridge

VLAN *
1 ~ 4094

CANCEL

APPLY

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

Editing an Object

Steps:

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

Deleting an Object

Steps:

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

Delete Interface(s)

2 item(s) selected

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

CANCEL

DELETE

Policy Profile Management

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

You can configure the following types of policies in MXsecurity:

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

Creating a New Layer 3-7 Policy Profile

Steps:

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

- Click the  icon to create a policy profile.

Policy Profiles

0 of 11 selected Search

☐	Profile Name ↑	Description	Device In Use	Schedule In Use
☐	Dos		0	
☐	Dos2		0	
☐	abcd		1 ...	Yes
☐	br-test		0	
☐	fsafdfad		4 ...	Yes
☐	ips		0	
☐	test321	123321	0	
☐	testprofile2222		0	
☐	testsestie		0	
☐	testsestterfdrd		0	

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



NOTE

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



NOTE

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

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

Layer 3 - 7 ^

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

0 of 0 Selected Search

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

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

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

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

Create Layer 3-7 Policy

Index *
1
1 ~ 1024

Status *
Enabled ▼

Name *
0 / 32

Description
0 / 128

Log *
Disabled ▼

Severity *
<4> Warning ▼

Log Destination
Local Storage ▼

Incoming Interface *
Any ▼

Outgoing Interface *
Any ▼

Action *
Allow ▼

Filter Mode *
IP and Port Filtering ▼

Source IP Address *
Any ▼ +

Source Port *
Any ▼ +

Destination IP Address *
Any ▼ +

Destination Port or Protocol *
Any ▼ +

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

IP and Source MAC Binding:

- i. **Source MAC Address:** Specify the source MAC address.
- ii. **Source IP Address:** Select a preconfigured Filter Object. Refer to [Creating a New Filter Object](#).

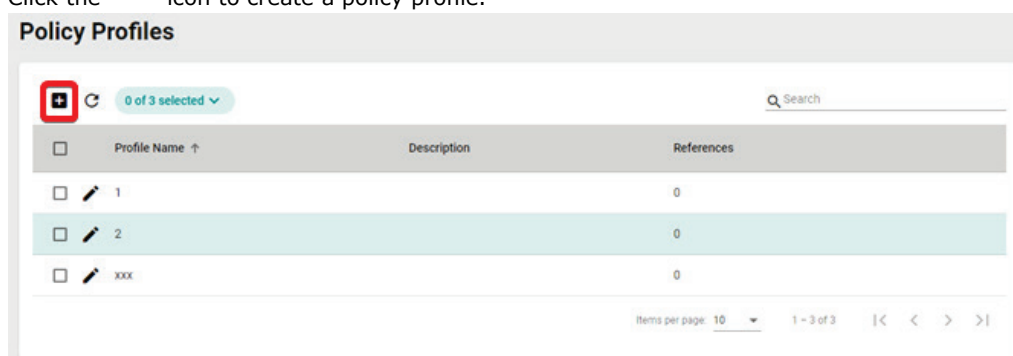
Source MAC Filtering:

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

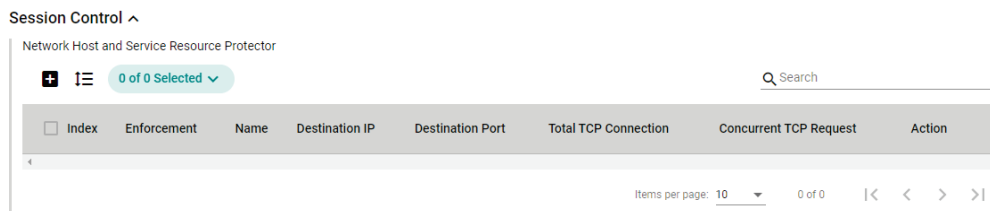
Creating a New Session Control Policy Profile

Steps:

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



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



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

6. Configure the Session Control Profile settings:

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

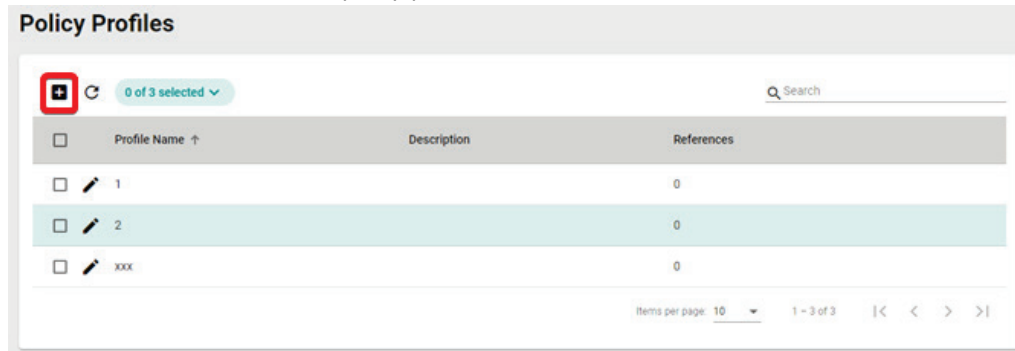
- a. **Index:** Specify the index for the policy profile.
 - b. **Status:** Enable or disable the policy profile.
 - c. **Name:** Enter a description for the policy profile.
 - d. **Severity:** Select the log severity level.
 - e. **Log Destination:** If logging is enabled, choose where the logs will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

Creating a New DoS Policy Profile

Steps:

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

- Click the  icon to create a policy profile.



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

DoS ^

DoS Settings

☒ All

Session SYN Protection

☒ TCP-Without-SYN Scan 

Port-Scan Protection Flood Protection

☒ Null Scan ☒ ICMP-Flood

☒ Xmas Scan Limit

☒ NMAP-Xmas Scan 1000

☒ SYN/FIN Scan 1 - 4000 pkt/s

☒ FIN Scan ☒ SYN-Flood

☒ NMAP-ID Scan Limit

☒ SYN/RST Scan 1000

☒ ARP-Flood

Limit

1 - 2000 pkt/s

DoS Log Settings

Log * Severity * Log Destination *

Disabled Emergency

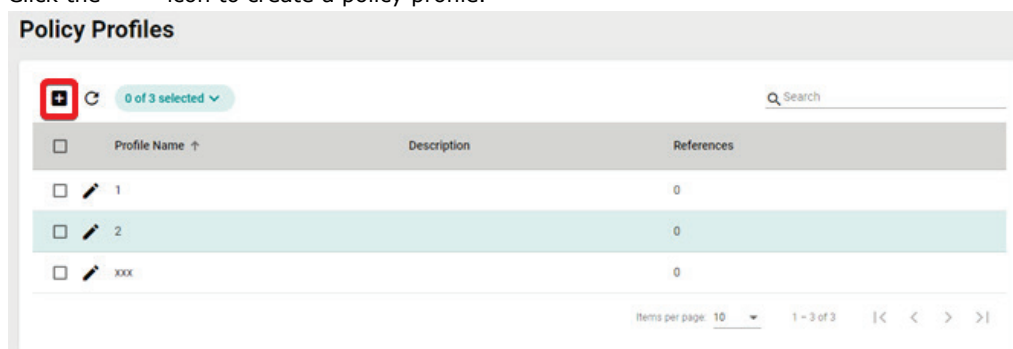
- DOS Setting:** Check the box of the DoS types you want to enable. If you selected ICMP-Death, SYN-Flood, or ARP-Flood, specify the packet limit.
 - Log:** Enable or disable event logs.
 - Severity:** Select the log severity level.
 - Log Destination:** If logging is enabled, choose where the logs will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

Creating a New IPS Policy Profile

Steps:

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

2. Click the  icon to create a policy profile.



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

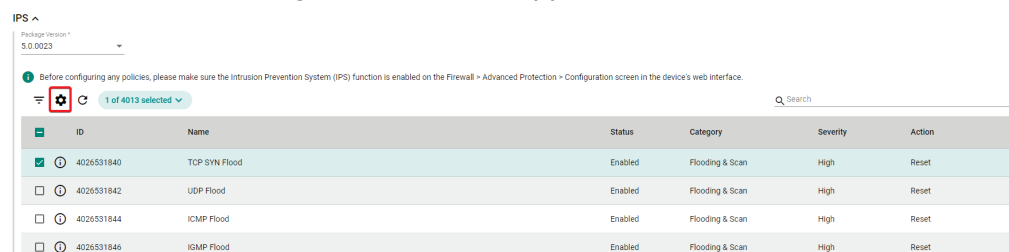
IPS ^

Package Version *

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

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

7. Click the  icon to configure the selected rule(s).



8. Configure the following settings:

Rule Settings

Status
Enabled

Action
Reset

CANCEL

APPLY

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

Editing a Policy Profile

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

Deleting a Policy Profile

Steps:

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

Delete Profile(s)

1 item(s) selected

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

CANCEL

DELETE

Device Configuration Management

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

Uploading a Device Configuration File From a Local Host

Steps:

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

EDR-G9010-VPN-2MGSPF ^

 0 of 3 selected ▾ Search				
☐	Configure Name ↑	Last Modified Time	Description	Schedule In Use
☐	 20230101_configure	2023-07-15 18:24:15	First version of PoC	Yes
☐	 20230201_configure	2023-07-15 18:22:52		
☐	 20230301_configure	2023-07-15 18:23:30	Network setting ok	

1 - 3 of 3

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

Upload Device Configuration File

1 Enter Configuration File Information 2 Select Configuration File

Configuration Model
EDR-G9010-VPN-2MGSFP

Configure Name *
20230601_configure 18 / 50

Description
PoC complete 12 / 255

CANCEL NEXT

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

Upload Device Configuration File

1 Enter Configuration File Information 2 Select Configuration File

Upload Configuration Method *
Upload Configuration from Local

Upload Configuration File (.ini)

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

BACK APPLY

7. Click **APPLY**.

Uploading a Configuration From a Device

Steps:

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

EDR-G9010-VPN-2MGSFP ^

 0 of 3 selected

Search

☐	Configure Name ↑	Last Modified Time	Description	Schedule In Use
☐	 20230101_configure	2023-07-15 18:24:15	First version of PoC	Yes
☐	 20230201_configure	2023-07-15 18:22:52		
☐	 20230301_configure	2023-07-15 18:23:30	Network setting ok	

1 - 3 of 3

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

Upload Device Configuration File

1 Enter Configuration File Information

2 Select Configuration File

Configuration Model
EDR-G9010-VPN-2MGSFP

Configure Name *
20230601_configure 18 / 50

Description
PoC complete 12 / 255

CANCEL NEXT

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

Upload Device Configuration File

1 Enter Configuration File Information

2 Select Configuration File

Upload Configuration Method *
Upload Configuration from Device

Search

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

7. Click **APPLY**.



NOTE

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

7. Deployment

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

You can configure the following types of deployments in MXsecurity:

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

Rebooting a Managed Device

Steps:

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

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

Device Deployment

General Policy Profiles Software Packages Firmware Device Configuration

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

Device Name	Status	Location	Product Model	Serial Number	MAC	Firmware Version	Scheduling Reboot	Last Reboot Time
Ungroup								
☐ OnCellCellularRouter999	●	120.25, 25.35	OnCell-G4302-LTE4-EU	MOXA60004302	60:60:60:60:43:02	V2.5.0		
☐ Owen 4302	●	OOOOOwenn1	OnCell-G4302-LTE4-EU	MOXA00000000	10:71:98:43:02:01	V3.0.0		
☐ device_4	●	location_4	OnCell G4302-LTE4-AU	TEST-DEV-4	43:00:00:00:00:04	V1.0.0	Weekly Mon. Tue. 07:55	Manually 2023-04-26 17:37:05
☐ Firewall/VPN Router 55160	●	Device Location	EDR-G9010-VPN-2MGSFP-T	TBZKB1155160	00:90:E8:91:86:7D	V3.0.0		Schedule 2023-05-11 04:00:25
☐ OOOwen 9010	●	122, 25	EDR-G9010-VPN-2MGSFP-T	MOXA00112233	00:90:E8:90:10:06	V3.0.0		Schedule 2023-07-12 16:10:24
☒ device_3	●	location_3	EDR-G9010-VPN-2MGSFP-T	TEST-DEV-3	90:10:00:00:00:03	V1.0.0	One Time 2023-07-12 16:10	Schedule 2023-07-12 16:10:24
☐ Firewall/VPN Router Hades	●	Device Location	EDR-G9010-VPN-2MGSFP-T	MOXA95275487	00:01:02:03:04:05	V3.0.0		

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

Reboot Device(s)

1 item(s) selected

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

CANCEL

REBOOT

Scheduling a Managed Device Reboot

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

Steps:

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

Device Deployment

General

Policy Profiles

Software Packages

Firmware

Device Configuration

0 group(s) selected

2 device(s) selected

Search

	Device Name	Status	Location	Product Model	Serial Number	MAC	Firmware Version	Scheduling Reboot	Last Reboot Time
	Ungroup								
	device_1		120.0, 20.5	EDR-G9010-VPN-2MGSFP	TEST-DEV-1	90:10:00:00:00:01	V1.0.0		Manually 2023-05-29 13:44:20
	device_2		125.0, 25.5	EDR-G9010-VPN-2MGSFP	TEST-DEV-2	90:10:00:00:00:02	V1.0.0		Manually 2023-03-06 11:32:45
	OnCellCellularRouter999		120.25, 25.35	OnCell-G4302-LTE4-EU	MOXA60004302	60:60:60:60:43:02	V2.5.0		
	grace		123, 32	EDR-G9010-VPN-2MGSFP	TBAIB1134586	00:90:E8:9D:EA:B7	V3.0.0	Daily 07:55	Schedule 2023-07-15 07:55:25
	device_4		location_4	OnCell G4302-LTE4-AU	TEST-DEV-4	43:00:00:00:00:04	V1.0.0	Weekly Mon. Tue. 07:55	Manually 2023-04-26 17:37:05
	Owen 4302		00000wenn1	OnCell-G4302-LTE4-EU	MOXA000000000	10:71:98:43:02:01	V3.0.0		

4. Select a scheduling mode:

Schedule Settings

2 item(s) selected

Scheduling Mode *

One Time

Daily

Weekly

CANCEL

APPLY

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

Schedule Settings

1 item(s) selected

Scheduling Mode *

One Time

Date * 2023-07-15

Time * 16:05

CANCEL

APPLY

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

through October 13.

Schedule Settings

1 item(s) selected

Scheduling Mode *

Daily

Time *

05:00



Period *

2023-07-15 – 2023-10-13



CANCEL

APPLY

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

Schedule Settings

1 item(s) selected

Scheduling Mode *

Weekly

Weekly Day *

Mon. Wed. Fri.

Time *

05:00



Period *

2023-07-15 – 2023-10-13



CANCEL

APPLY

5. Click **APPLY**.

Deleting a Managed Device Reboot Schedule

Steps:

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

Delete Scheduling

2 item(s) selected

Are you sure you want to delete the selected scheduling?

CANCEL

DELETE

Removing a Managed Device

Steps:

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

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

Device Deployment

General

Policy Profiles

Software Packages

Firmware

0 group(s) selected

2 device(s) selected

	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)?

CANCEL

DELETE

Deploying Policy Profiles to Managed Devices

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

The synchronization status can be one of the following:

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

Steps:

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

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

Device Deployment

General

Policy Profiles

Software Packages

Firmware

Device Configuration

0 group(s) selected

1 device(s) selected

Search

	Device Name ↑	Status	Location	Product Model	Serial Number	MAC	Status / Profile Name	Scheduling	Last Update Time
Ungroup									
☐	Firewall/VPN Router 55160		Device Location	EDR-G9010-VPN-2MGSP-T	TBZKB1155160	00:90:E8:91:86:7D			
☒	Firewall/VPN Router 77777		Device Location	EDR-G9010-VPN-2MGSP	MOXA77777777	00:01:02:03:04:77			

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

Sync Profile To Device(s)

2 item(s) selected

Profile Name *

1

CANCEL

APPLY

5. Click **APPLY**.

Scheduling a Policy Profile Deployment for Managed Devices

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

Steps:

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

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

Device Deployment

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

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

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

4. Select a scheduling mode:

Schedule Settings

2 item(s) selected

Scheduling Mode *

One Time

Daily

Weekly

CANCEL APPLY

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

Schedule Settings

1 item(s) selected

Scheduling Mode *

One Time

Date * 2023-07-15

Time * 16:05

CANCEL APPLY

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

Schedule Settings

1 item(s) selected

Scheduling Mode *

Daily

Time * 05:00

Period * 2023-07-15 – 2023-10-13

CANCEL APPLY

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

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

Schedule Settings

1 item(s) selected

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

CANCEL APPLY

5. Click **APPLY**.

Deleting a Policy Profile Deployment Schedule

Steps:

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

Delete Scheduling

2 item(s) selected

Are you sure you want to delete the selected scheduling?

CANCEL DELETE

Upgrading the Software Package of Managed Devices

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

You can check the following software package information:

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

Steps:

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

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

Device Deployment

General

Policy Profiles

Software Packages

Firmware

Device Configuration

1

0 group(s) selected

1 device(s) selected

Search

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

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

Upgrade Package

1 item(s) selected

Version *

CANCEL

UPGRADE

- Click **UPGRADE**.

Scheduling a Software Package Deployment for Managed Devices

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

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

Steps:

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

Device Deployment

General

Policy Profiles

Software Packages

Firmware

Device Configuration

Network Security Packages

1

0 group(s) selected

2 device(s) selected

Search

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

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

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

5. Select a scheduling mode:

Schedule Settings

2 item(s) selected

Scheduling Mode *

One Time

Daily

Weekly

CANCEL APPLY

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

Schedule Settings

1 item(s) selected

Scheduling Mode *

One Time

Date *

2023-07-15

Time *

16:05

CANCEL APPLY

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

Schedule Settings

1 item(s) selected

Scheduling Mode *

Daily

Time *

05:00

Period *

2023-07-15 - 2023-10-13

CANCEL APPLY

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

Schedule Settings

1 item(s) selected

Scheduling Mode *

Weekly

Weekly Day *

Mon. Wed. Fri.

Time *

05:00

Period *

2023-07-15 - 2023-10-13

CANCEL APPLY

6. Click **APPLY**.

Deleting a Software Package Deployment Schedule

Steps:

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

Delete Scheduling

2 item(s) selected

Are you sure you want to delete the selected scheduling?

CANCEL

DELETE

Upgrading the Firmware of Managed Devices

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

You can check the following firmware information:

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

Steps:

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

Device Deployment

General

Policy Profiles

Software Packages

Firmware

Device Configuration

1

0 group(s) selected

1 device(s) selected

Search

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

- ## Upgrade Firmware

5. Click **UPGRADE**.

Scheduling a Firmware Deployment for Managed Devices

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

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

Steps:

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

Device Deployment

General
Policy Profiles
Software Packages
Firmware
Device Configuration

≡
1

0 group(s) selected

1 device(s) selected

🔍 Search

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

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

Schedule Settings

2 item(s) selected

Scheduling Mode

One Time

Daily

Weekly

CANCEL

APPLY

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

Schedule Settings

1 item(s) selected

Scheduling Mode *
One Time

Date *
2023-07-15

Time *
16:05

CANCEL APPLY

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

Schedule Settings

1 item(s) selected

Scheduling Mode *
Daily

Time *
05:00

Period *
2023-07-15 – 2023-10-13

CANCEL APPLY

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

Schedule Settings

1 item(s) selected

Scheduling Mode *
Weekly

Weekly Day *
Mon. Wed. Fri.

Time *
05:00

Period *
2023-07-15 – 2023-10-13

CANCEL APPLY

6. Click **APPLY**.

Deleting a Firmware Deployment Schedule

Steps:

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

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

Delete Scheduling

2 item(s) selected

Are you sure you want to delete the selected scheduling?

CANCEL

DELETE

Deploying a Configuration to Managed Devices

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

Steps:

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

Device Deployment

GeneralPolicy ProfilesSoftware PackagesFirmwareDevice Configuration

0 group(s) selected1 device(s) selected

Search

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

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

Sync Configuration To Device(s)

1 item(s) selected

Select Configuration File *

20230101_configuration

CANCEL

APPLY

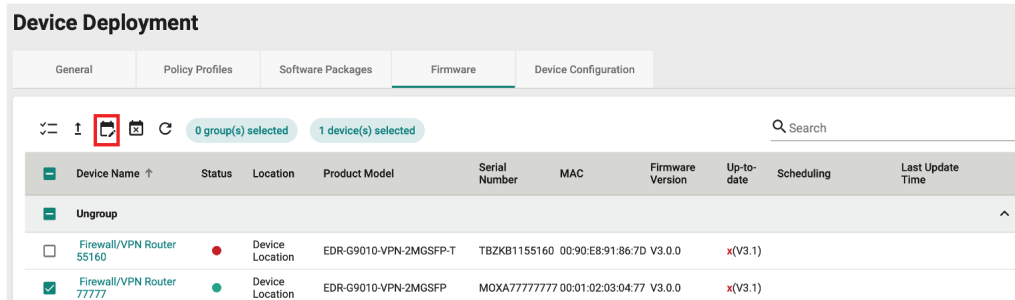
- Click **APPLY**.

Scheduling a Configuration Deployment for Managed Devices

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

Steps:

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



Device Deployment

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

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

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

4. Select a previously uploaded configuration file to deploy.



Schedule Settings

1 item(s) selected

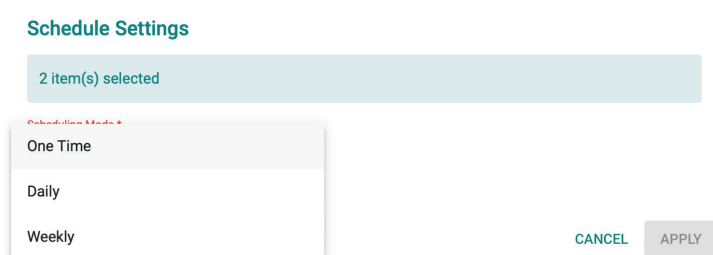
Select File *

20230101_configuration

Scheduling Mode *

CANCEL APPLY

5. Select a scheduling mode:



Schedule Settings

2 item(s) selected

Scheduling Mode *

One Time

Daily

Weekly

CANCEL APPLY

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

example 16:05.

Schedule Settings

1 item(s) selected

Scheduling Mode *
One Time

Date *
2023-07-15

Time *
16:05

CANCEL

APPLY

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

Schedule Settings

1 item(s) selected

Scheduling Mode *
Daily

Time *
05:00

Period *
2023-07-15 – 2023-10-13

CANCEL

APPLY

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

Schedule Settings

1 item(s) selected

Scheduling Mode *
Weekly

Weekly Day *
Mon. Wed. Fri.

Time *
05:00

Period *
2023-07-15 – 2023-10-13

CANCEL

APPLY

6. Click **APPLY**.

Deleting a Configuration Deployment Schedule

Steps:

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

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

Delete Scheduling

2 item(s) selected

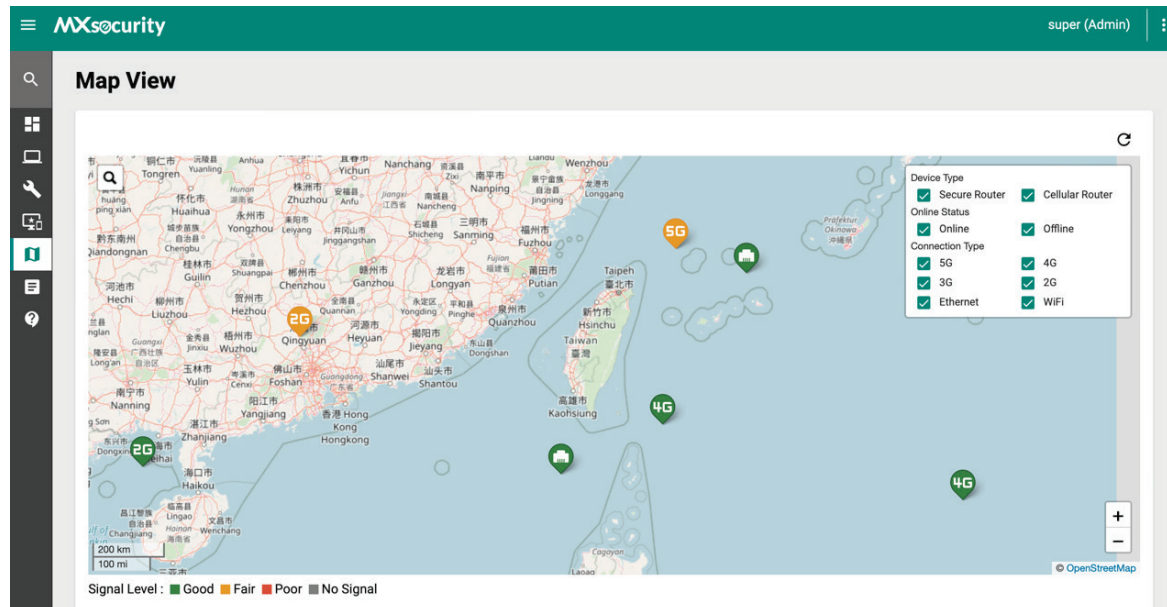
Are you sure you want to delete the selected scheduling?

CANCEL

DELETE

8. Map View

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



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

Basic Functions

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

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

Signal Level

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

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

Icon	Description
	No cellular signal or the Ethernet interface link is down.

Interface in Use

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

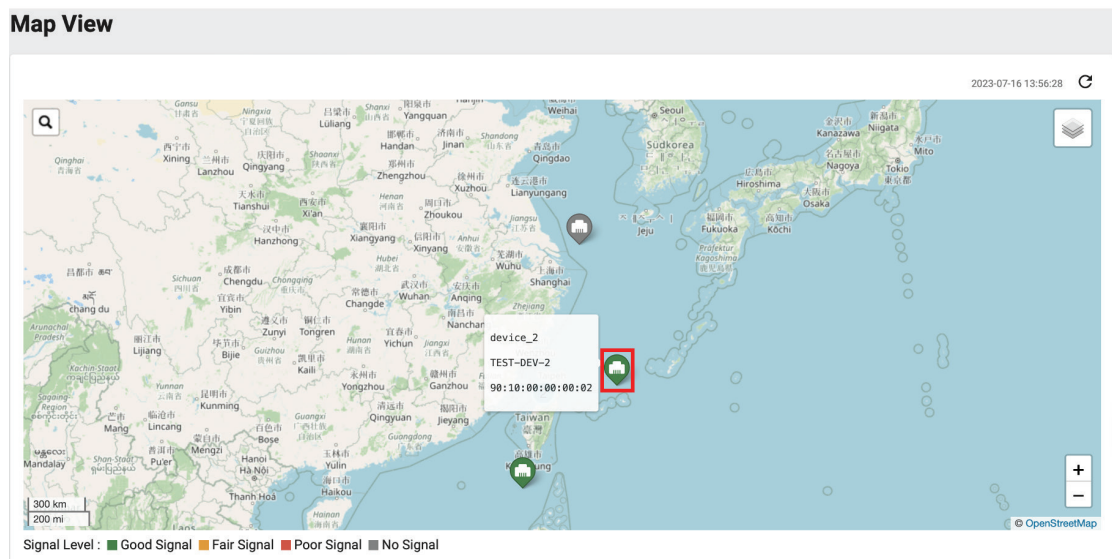
Icon	Description
	The device is using Ethernet WAN to connect to the internet.
	The device is using cellular 5G to connect to the internet.
	The device is using cellular 4G to connect to the internet.
	The device is using cellular 3G to connect to the internet.
	The device is using cellular 2G to connect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

Viewing Detailed Device Information

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

Steps:

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



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

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

Device device_2 Information



● Online

System Uptime
1d23h21m55s

Basic Information

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

CLOSE

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

Device device_4 Information



● Online

System Uptime
1d23h20m17s

Basic Information

Cellular Information

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

CLOSE

Editing the Location of a Device

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

Steps:

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

3. Click  the icon in the Location field.

Device Firewall/VPN Router 77777 Information



● Online

System Uptime
2d21h1m5s

Basic Information

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

Edit Location

CLOSE

4. Enter the longitude and latitude coordinates.

Location ⓘ

122.51, 31.2  

12 / 80

5. Click  .

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

9. Report

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

This section will provide information for the following reports:

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

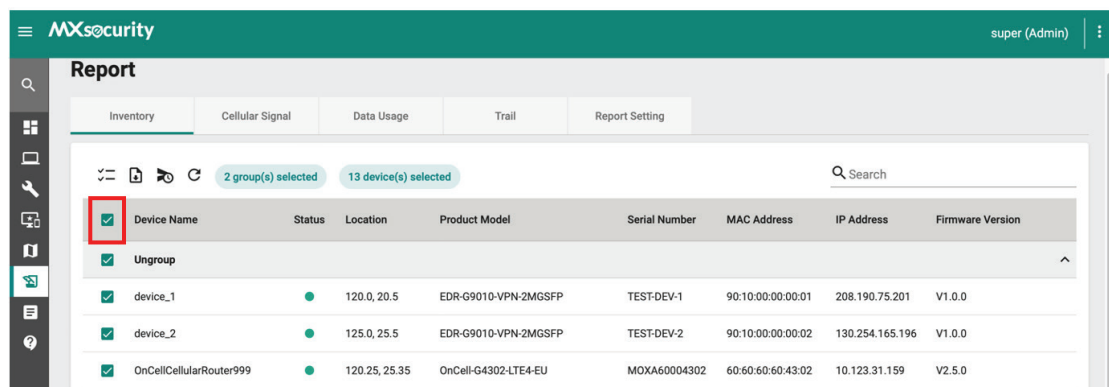
Inventory Reports

Generating a Current Inventory Report

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

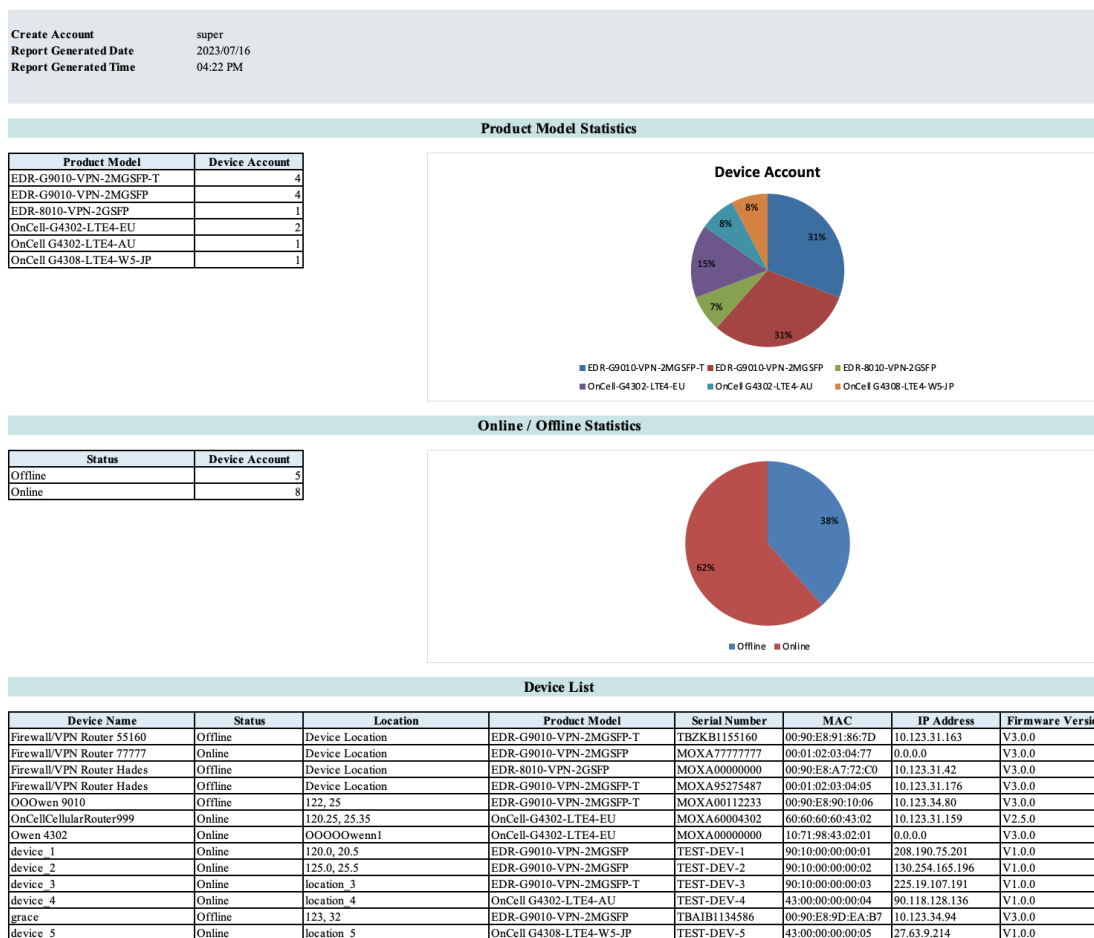
Steps:

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



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

The inventory report includes the following information:



The following table describes the report's fields.

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

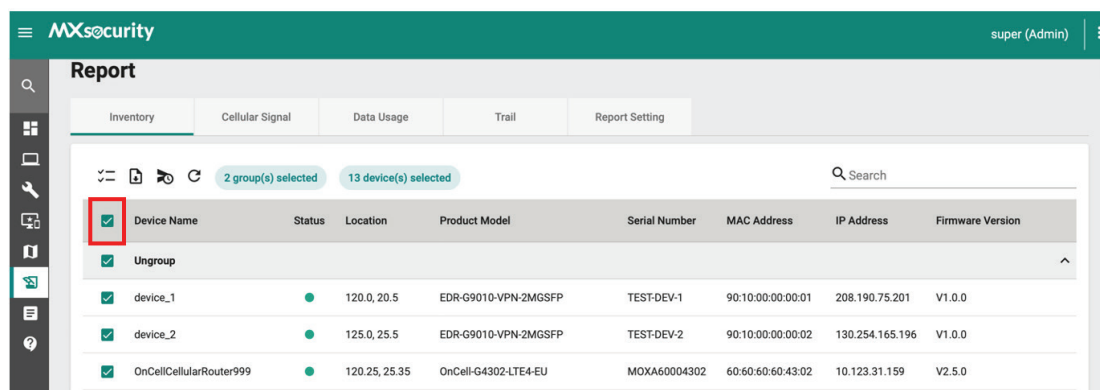
Scheduling an Inventory Report

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

Steps:

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

2. Select all devices.



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

Schedule an Email to Send Inventory Report

13 item(s) selected

Receiver Email *

test1@moxa.com × Test2@moxa.com × 

Test3@moxa.com ×

3 / 5

Subject *

Inventory report of Tapei Site 

30 / 50

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

Scheduling 

Scheduling Mode *

☒ One Time ☐ Monthly

Report sending date

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

Date *

2023-07-17 

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

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

Schedule Settings

1 item(s) selected

Scheduling Mode *

Daily

Time *

05:00 

Period *

2023-07-15 – 2023-10-13 

CANCEL APPLY

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

Cellular Signal Reports

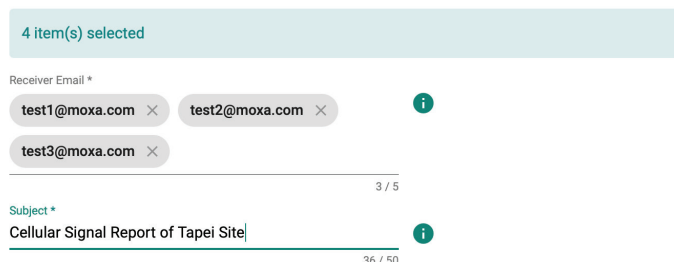
Scheduling a Cellular Signal Report

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

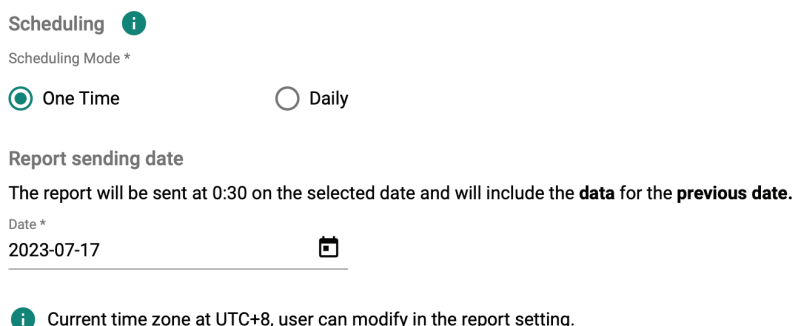
Steps:

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

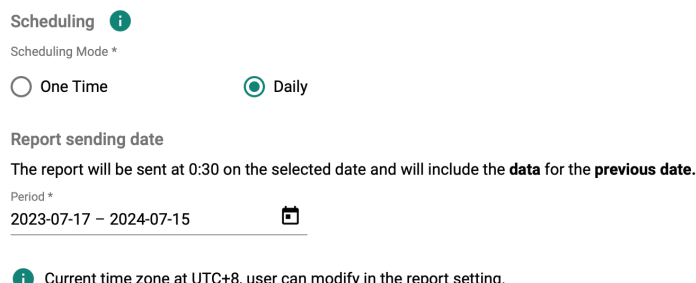
Schedule an Email to Send Cellular Signal Report



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



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



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

Data Usage Reports

Generating a Cellular Data Usage Report

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

Steps:

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

Report

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

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

Search

Device Name	Status	Location	Product Model	Serial Number	MAC Address	IP Address	Firmware Version
Ungroup							
OnCellCellularRouter999		120.25, 25.35	OnCell-G4302-LTE4-EU	MOXA60004302	60:60:60:60:43:02	10.123.31.159	V2.5.0
device_4		location_4	OnCell G4302-LTE4-AU	TEST-DEV-4	43:00:00:00:00:04	221.120.40.156	V1.0.0
Owen 4302		0000Owenn1	OnCell-G4302-LTE4-EU	MOXA00000000	10:71:98:43:02:01	0.0.0.0	V3.0.0
test2							
device_5		location_5	OnCell G4308-LTE4-W5-JP	TEST-DEV-5	43:00:00:00:00:05	27.63.9.214	V1.0.0

4. Select the report period.

Download Data Usage Report

4 item(s) selected

Period *

2023-06-01 – 2023-06-30

2023

S M T W T F S

JUN

1 2 3

4 5 6 7 8 9 10

11 12 13 14 15 16 17

18 19 20 21 22 23 24

25 26 27 28 29 30

CANCEL DOWNLOAD

5-JP TEST-DEV-5 43:00:00:00:00:05



NOTE

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



NOTE

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

5. Click **DOWNLOAD**.

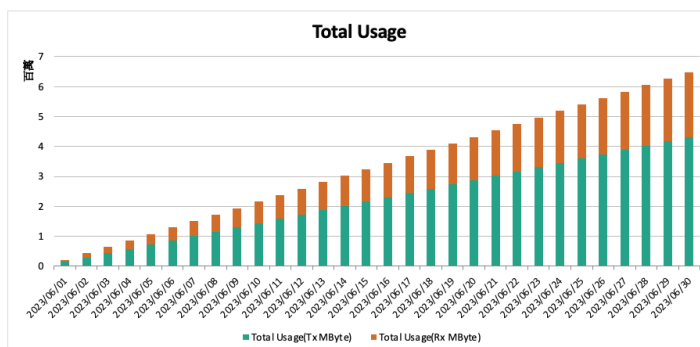
The cellular data usage report includes the following information:

Data Usage Report

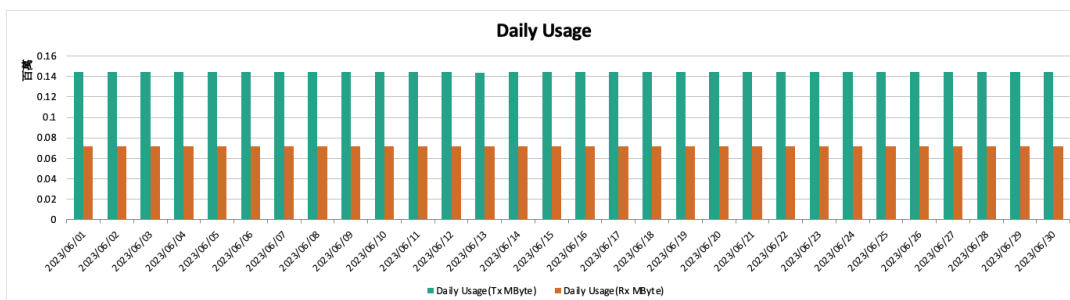
Create Account	super
Report Generated Date	2023/07/16
Report Generated Time	06:01 PM
Data Period	2023/06/01 - 2023/06/30
Device Name	device_4
Device MAC Address	43:00:00:00:00:04
Device Serial Number	TEST-DEV-4

Data Usage(Total Usage)

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



Data Usage(Daily Usage)



The following table describes the report's fields.

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

Scheduling a Cellular Data Usage Report

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

Steps:

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

Schedule an Email to Send Data Usage Report

4 item(s) selected

Receiver Email *

test1@moxa.com × Test2@moxa.com × 

Test3@moxa.com ×

3 / 5

Subject *

Data Usage report of Tapei Site 

31 / 50

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

Scheduling

Scheduling Mode *

☒ One Time ☐ Monthly

Report sending date

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

Date *

2023-07-17 

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

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

Scheduling

Scheduling Mode *

☐ One Time ☒ Monthly

Report sending date

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

Generate Report Date * Period *

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

1 ~ 31

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

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

Trail Reports

Generating a Trail Report

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

Steps:

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

Report

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

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

Search

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

4. Select the report period.

Download Trail Report

4 item(s) selected

Date *
2023-07-10

2023 < >

S M T W T F S

JUL

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

CANCEL DOWNLOAD

TEST-DEV-5 43:00:00:00:00:05



NOTE

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



NOTE

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

5. Click **DOWNLOAD**.

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

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

Scheduling a Trail Report

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

Steps:

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

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

Schedule an Email to Send Trail Report

4 item(s) selected

Receiver Email *

test1@moxa.com × test2@moxa.com × test3@moxa.com ×

3 / 5

Subject *

Trail Report of OnCell Devices

30 / 50

6. Select a scheduling mode:

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

Scheduling

Scheduling Mode *

☒ One Time ☐ Daily

Report sending date

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

Date *

2023-07-18

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

Scheduling

Scheduling Mode *

☐ One Time ☒ Daily

Report sending date

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

Period *

2023-07-18 – 2024-07-16

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

7. Click **APPLY**.

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

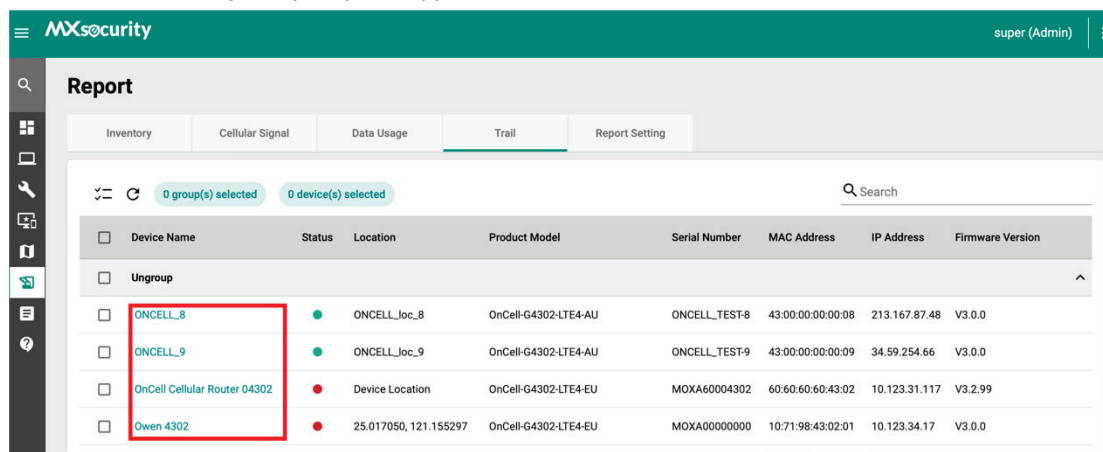
Viewing GPS Trajectories

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

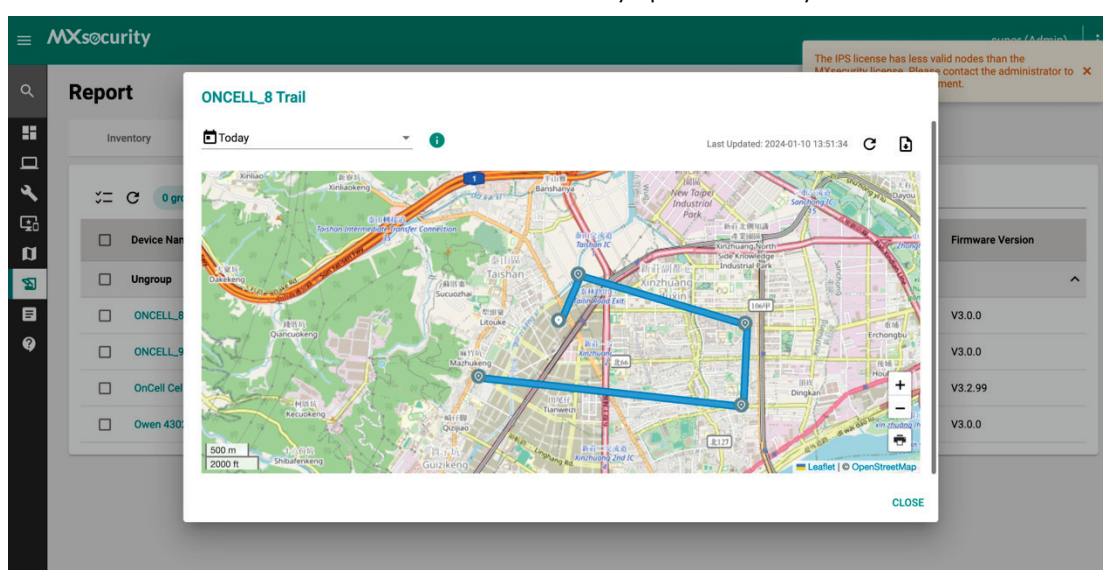
Steps:

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

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



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



Report Settings

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

Configure Report Time Zone Settings

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

Steps:

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

Editing a Report Schedule

Steps:

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

10. Logging

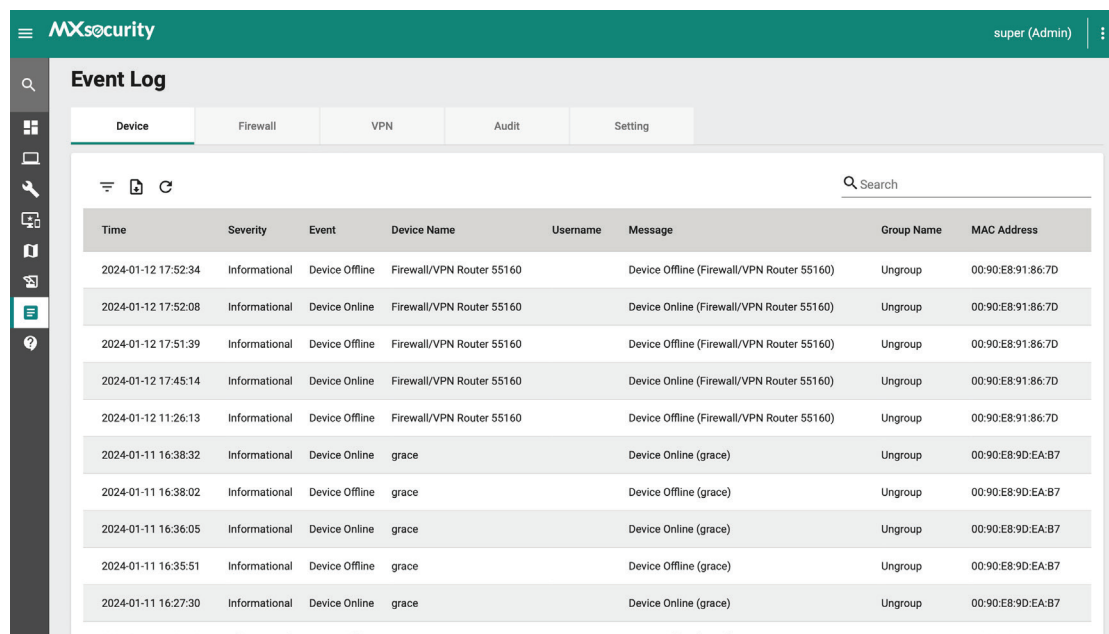
This chapter covers the event log and notification functions. Users can view logs related to the device, firewall, VPN, and audits. The notification function enables users to receive notifications for particular event logs. Users can send these notifications to designated email recipients or a syslog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

Event Log

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

Device Log

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



The screenshot shows the MXsecurity Event Log interface. The top bar is green with the MXsecurity logo and a user profile 'super (Admin)'. Below the bar, there's a search icon and the title 'Event Log'. A horizontal tab bar contains 'Device', 'Firewall', 'VPN', 'Audit', and 'Setting', with 'Device' selected. Below the tabs is a table with columns: Time, Severity, Event, Device Name, Username, Message, Group Name, and MAC Address. The table contains 12 rows of log entries. A search bar is located on the right side of the table.

Time	Severity	Event	Device Name	Username	Message	Group Name	MAC Address
2024-01-12 17:52:34	Informational	Device Offline	Firewall/VPN Router 55160		Device Offline (Firewall/VPN Router 55160)	Ungroup	00:90:E8:91:86:7D
2024-01-12 17:52:08	Informational	Device Online	Firewall/VPN Router 55160		Device Online (Firewall/VPN Router 55160)	Ungroup	00:90:E8:91:86:7D
2024-01-12 17:51:39	Informational	Device Offline	Firewall/VPN Router 55160		Device Offline (Firewall/VPN Router 55160)	Ungroup	00:90:E8:91:86:7D
2024-01-12 17:45:14	Informational	Device Online	Firewall/VPN Router 55160		Device Online (Firewall/VPN Router 55160)	Ungroup	00:90:E8:91:86:7D
2024-01-12 11:26:13	Informational	Device Offline	Firewall/VPN Router 55160		Device Offline (Firewall/VPN Router 55160)	Ungroup	00:90:E8:91:86:7D
2024-01-11 16:38:32	Informational	Device Online	grace		Device Online (grace)	Ungroup	00:90:E8:9D:EA:B7
2024-01-11 16:38:02	Informational	Device Offline	grace		Device Offline (grace)	Ungroup	00:90:E8:9D:EA:B7
2024-01-11 16:36:05	Informational	Device Online	grace		Device Online (grace)	Ungroup	00:90:E8:9D:EA:B7
2024-01-11 16:35:51	Informational	Device Offline	grace		Device Offline (grace)	Ungroup	00:90:E8:9D:EA:B7
2024-01-11 16:27:30	Informational	Device Online	grace		Device Online (grace)	Ungroup	00:90:E8:9D:EA:B7
2024-01-11 16:26:59	Informational	Device Offline	grace		Device Offline (grace)	Ungroup	00:90:E8:9D:EA:B7

Viewing Device Logs

Steps:

1. Navigate to **Logging > Event Log > Device**.
2. You can perform the following actions:
 - a. Click the  icon to open the filter menu. Select a start/end day and time or log severity from the respective drop-menu.



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

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



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



The following table describes the log's fields.

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

Firewall Log

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

<

Viewing Firewall Logs

Steps:

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

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

Event Log

Device

Firewall

Trusted Access ▾

Trusted Access

Malformed Packets

DoS Policy

Layer 3-7 Policy

Protocol Filter Policy

ADP

IPS

Session Control

Layer 2 Policy

Severity	Group Name
Error	Ungrou
Notice	Ungrou
Alert	Ungrou
Notice	Ungrou
Emergency	Ungrou
Alert	Ungrou
Alert	Ungrou

3. You can perform the following actions:

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



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

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



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



The following table describes the log's fields.

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

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

VPN Log

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

MXsecurity

super (Admin)

Event Log

DeviceFirewallVPNAuditSetting

≡

📄

🔍

Search

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

Viewing VPN Logs

Steps:

- 1. Navigate to **Logging > Event Log > Audit**.
- 2. You can perform the following actions:
 - a. Click the  icon to open the filter menu. Select a start/end day and time or log severity from the respective drop-menu.



Filters

Start Date

Start Time

End Date

End Time

Event

Severity

CLEAR

APPLY

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

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



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



The following table describes the log's fields.

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

Audit Log

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

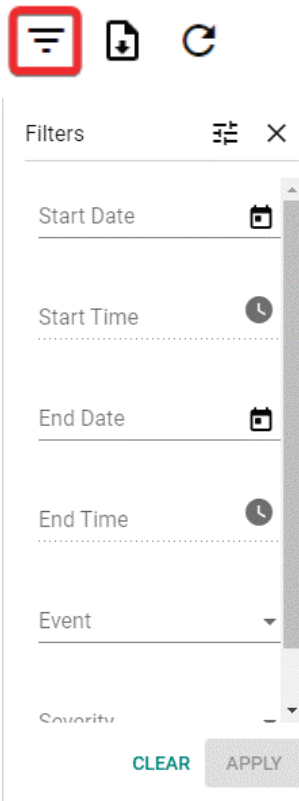
 A screenshot of the MXsecurity web interface showing the 'Event Log' section. The interface has a dark green header with the MXsecurity logo and a user profile 'super (Admin)'. A sidebar on the left contains various navigation icons. The main content area has tabs for 'Device', 'Firewall', 'VPN', 'Audit' (selected), and 'Setting'. Below the tabs is a search bar and a table of log entries. The table has columns for Time, Severity, Event, Username, and Message. The log entries show a series of 'Login Success' events for the 'super' user, followed by one 'Login Failure' event.

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

Viewing Audit Logs

Steps:

1. Navigate to **Logging > Event Log > Audit**.
2. You can perform the following actions:
 - a. Click the  icon to open the filter menu. Select a start/end day and time or log severity from the respective drop-menu.



The filter menu is a vertical panel with a title bar containing the word 'Filters', a filter icon, and a close 'X' button. It contains several filterable fields: 'Start Date' with a calendar icon, 'Start Time' with a clock icon, 'End Date' with a calendar icon, 'End Time' with a clock icon, 'Event' with a dropdown arrow, and 'Severity' with a dropdown arrow. At the bottom of the panel are two buttons: 'CLEAR' in green and 'APPLY' in grey.

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

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



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



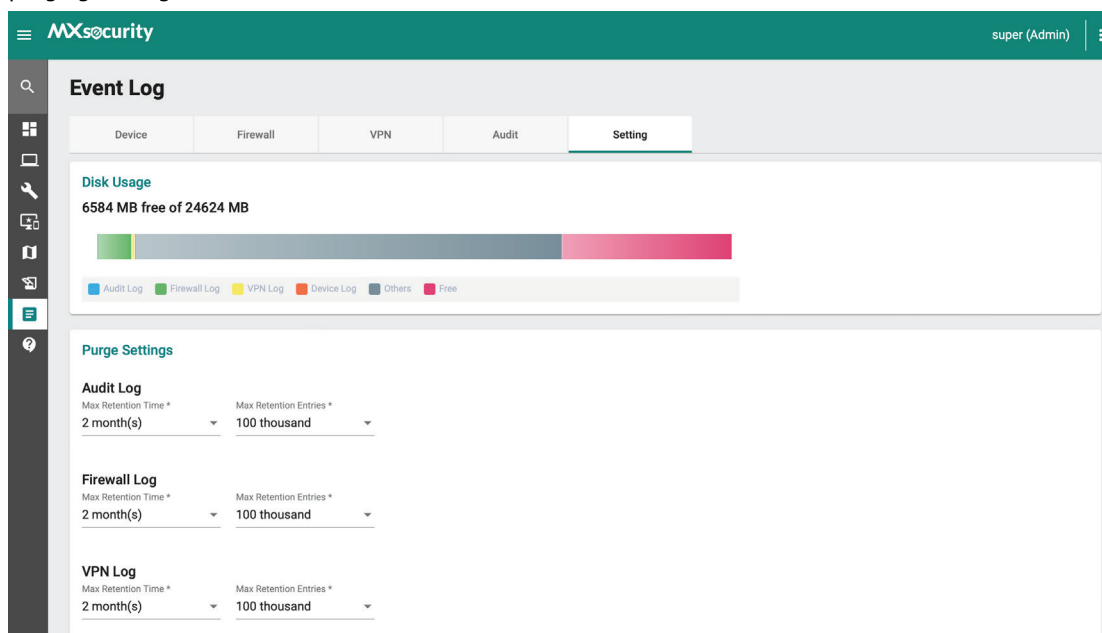
The following table describes the log's fields.

Field	Description
Time	The time the log entry was created.

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

Event Log Settings

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

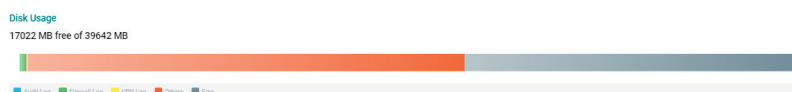


Purging Event Logs

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

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

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



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

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 ▼

Device Log
Max Retention Time * 2 month(s) ▼ Max Retention Entries * 100 thousand ▼

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

Event Log Auto Refresh

Event Log Auto Refresh
☒ Enabled ☐ Disabled

Event Log Auto Refresh Interval *
10 second(s) ▼

APPLY

5. Click **APPLY**.

Notifications

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

Adding a Notification

Steps:

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

3. Enter a name and description for the notification.

Create Notification

1 Notification Information

2 Choose Devices

3 Choose Event and Filter

4 Receiver Settings

Status *

☒ Enabled

☐ Disabled

Notification Name *

Trust Access

12 / 50

Description

0 / 255

CANCEL

NEXT

4. Click **NEXT**.

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

Create Notification

1 Notification Information

2 Choose Devices

3 Choose Event and Filter

4 Receiver Settings

10 of 13 selected

Search

☒	Device Name ↑	Status	Location	Product Model	Serial Number	MAC Address	Firmware Version	Group
☒	Firewall/VPN Router 55160		Device Location	EDR-G9010-VPN-2MGSFP-T	TBZKB1155160	00:90:E8:91:86:7D	V3.0.0	Ungroup
☒	Firewall/VPN Router 77777		Device Location	EDR-G9010-VPN-2MGSFP	MOXA77777777	00:01:02:03:04:77	V3.0.0	Ungroup
☒	Firewall/VPN Router Hades		Device Location	EDR-G9010-VPN-2MGSFP-T	MOXA95275487	00:01:02:03:04:05	V3.0.0	Ungroup
☒	Firewall/VPN Router Hades		Device Location	EDR-8010-VPN-2GSFP	MOXA00000000	00:90:E8:A7:72:C0	V3.0.0	Ungroup
☒	OOOwen 9010		122, 25	EDR-G9010-VPN-2MGSFP-T	MOXA00112233	00:90:E8:90:10:06	V3.0.0	Ungroup
☒	OnCellCellularRouter999		120.25, 25.35	OnCell-G4302-LTE4-EU	MOXA60004302	60:60:60:60:43:02	V2.5.0	Ungroup
☒	Owen 4302		OOOOOwenn1	OnCell-G4302-LTE4-EU	MOXA00000000	10:71:98:43:02:01	V3.0.0	Ungroup

6. Select the event types and configure filter rules:

a. Select the event type.

Create Notification

1 Notification Information

2 Choose Devices

3 Choose Event and Filter

4 Receiver Settings

Firewall

Trusted Access

Malformed Packets

DoS Policy

Layer 3-7 Policy

Protocol Filter Policy

☐ Source IP

☐ Destination IP

Source IP

Destination IP

Severity Mode

BACK

NEXT

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

Create Notification

Notification Information

Choose Devices

3 Choose Event and Filter

4 Receiver Settings

Notification Event *

Trusted Access

Event Filter Rule

☐ Severity

Severity Rule

Lower than or Equal to

☐ Source IP

Source IP

☐ Destination IP

Destination IP

Severity Mode

BACK

NEXT

7. Configure the notification content and recipient settings.

Create Notification

Dear Sir/ Madam,

This notification was automatically sent from MXsecurity.

Email Content *

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

96 / 256

Reset to default

Please check the detailed information on MXsecurity.

Best regards,

MXsecurity

+ Device Name

+ Product Model

+ Mac Address

+ Location

+ Serial Number

+ Event Time

+ Notification Name

+ Event

Receiver Email Address *

0 / 5

- a. Select the notification delivery method. Multiple methods can be selected.
 - b. Edit the notification content using the predefined variables.
 - c. If Email is selected, specify the email recipients. You can add up to 5 recipients separated by a comma.
8. Configure Advanced Settings. To prevent an influx of messages in a short period, users can configure a limit on the number of notifications for a specified interval. When exceeded, all additional notifications will be discarded until the next interval begins.

Advanced Settings *

Notification Limit *

☒ Enabled
 ☐ Disabled

MAX. Notification *

3

1 ~ 5

Period of Time *

10

1 ~ 60 minute(s)

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

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

- c. Specify the interval duration.
9. Click **APPLY**.

11. Administration

This chapter describes the available administrative settings for MXsecurity.

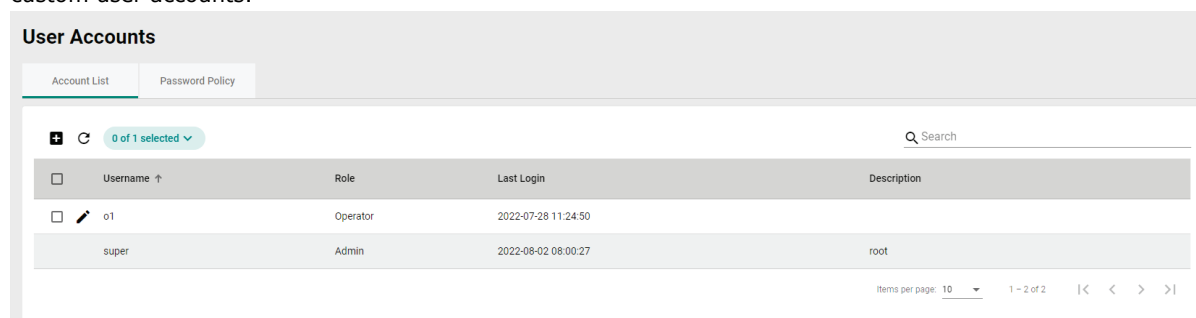
User Accounts



NOTE

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

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



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

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

User Roles

The following table describes the permissions matrix for user roles.

Dashboard

		User Roles		
Dashboard	View	Yes	VG	VG
	All operations	Yes	VG	VG

System Tab

		User Roles		
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		
Device Group	View	Yes	VG	No
	All operations	Yes	No	No
Firmware	View	Yes	Yes	No
	All operations	Yes	No	No
Software Packages	View	Yes	Yes	No
	All operations	Yes	No	No
Objects	View	Yes	Yes	No
	All operations	Yes	No	No
Policy Profiles	View	Yes	Yes	No
	All operations	Yes	No	No
Device Configuration	View	Yes	VG	No
	All operations	Yes	No	No



NOTE

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

Device Deployment

		User Roles		
Device Deployment	View	Yes	VG	No
	All operations	Yes	VG	No



NOTE

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

Map View

		User Roles		
Map View	View	Yes	VG	VG
	All operations	Yes	VG	No

Report

		User Roles		
Reports	View	Yes (All users)	VG (Self)	VG (Self)
	All operations	Write (Self) Delete (All users)	VG (Self)	VG (Self)

Logging

		User Roles		
Event Log	View	Yes	VG	VG
	All operations	Yes	VG	No
Notification	View	Yes	VG (Self)	VG (Self)
	All operations	Write (Self) Delete (All users)	VG (Self)	VG (Self)



NOTE

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

Account Input Format

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

Create User

Username *

0 / 32

i

Password *

0 / 32

i

Confirm Password *

0 / 32

Role *

Description

0 / 255

CANCEL

APPLY

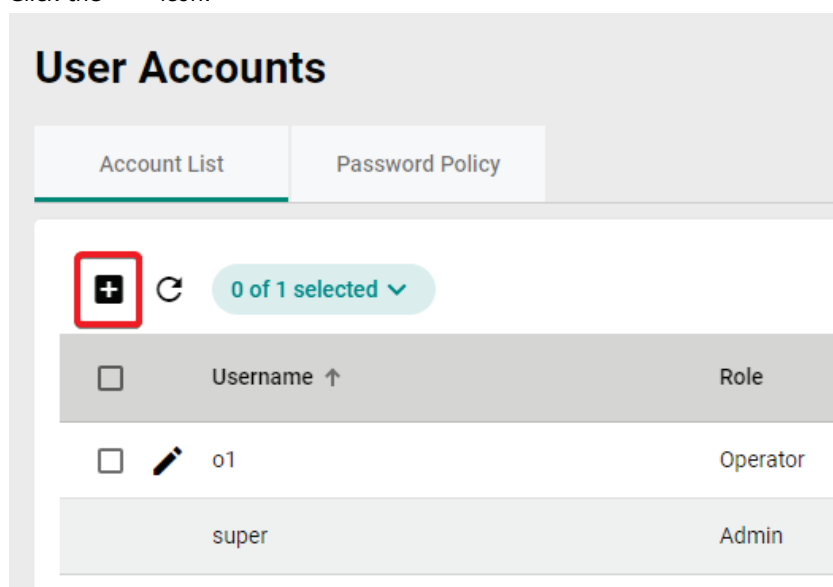
Type	Length	Format	Reserved Name
Username	1 to 32 characters	Letters: a-z, A-Z Numbers: 0-9 Special characters: periods (.), underscores (_)	admin administrator viewer operator root auditor
Description	0 to 255 characters	Letters: a-z, A-Z Numbers: 0-9 Special characters: periods (.), underscores (_),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

Adding a User Account

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

Steps:

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



The **Create User** screen will appear.

Create User

Username *  0 / 32

Password *   0 / 32

Confirm Password *  0 / 32

Role * 

Description 0 / 255

[CANCEL](#) [APPLY](#)

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

Editing an Existing User Account

Steps:

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

User Accounts

Account List Password Policy

  0 of 1 selected

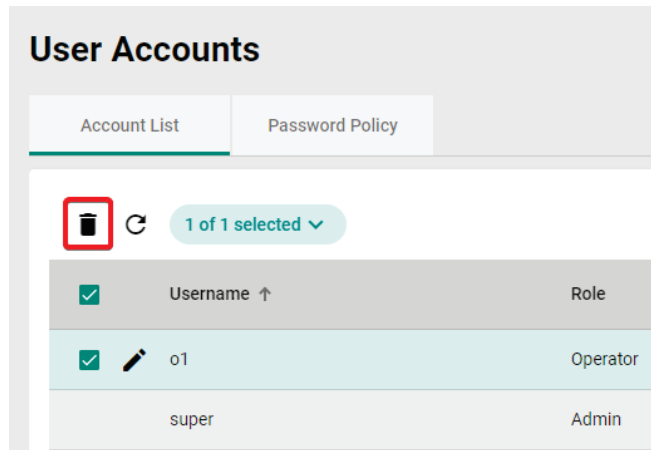
☐	Username ↑	Role
☐	o1	Operator
☐	super	Admin

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).



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

Delete User(s)

1 item(s) selected

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

CANCEL

DELETE

Configuring the Password Policy

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

Steps:

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

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

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.

super (Admin)

Change Password

Troubleshooting

Log Out

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

Change Password

Current Password *

New Password *

Confirm New Password *

CANCEL

APPLY

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

- b. **New Password:** Enter your new password.
- c. **Confirm New Password:** Enter your new password again.
4. Click **APPLY**. This will automatically log you out and return you to the login screen.

Licenses

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



NOTE

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

Introduction to Licenses

MXsecurity supports two types of licenses:

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



NOTE

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

Viewing Your Product License Information

Steps:

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

The **Licenses** screen will appear.

Update Date	Activation Code	License Type	License Duration (days)	License Nodes
2024-01-08 14:07:39		New	Permanent	5
2023-09-07 16:22:20		New	Permanent	50
2023-08-29 16:36:31		New	Permanent	30

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

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

MXsecurity licenses

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

The following table describes the license history.

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

IPS licenses

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

The following table describes the license history.

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

Alert Messages

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

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

Adding a New MXsecurity License

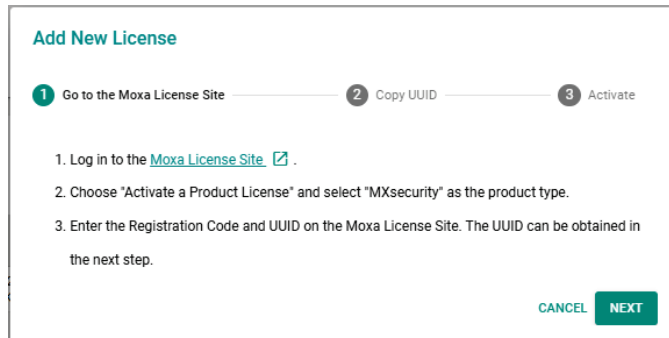
You can activate an MXsecurity license using a valid license activation code.

Steps:

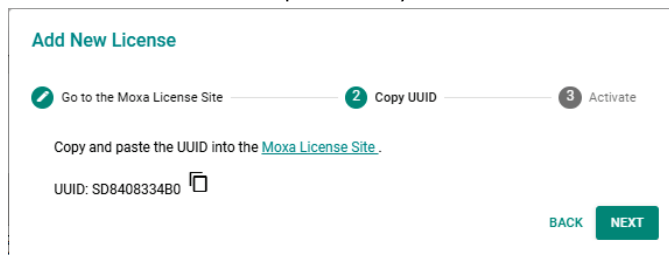
1. Navigate to **System > Licenses > MXsecurity**.

2. Click the **Add New License** button.

The **Add New License** screen will appear.



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



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

Adding a New IPS License

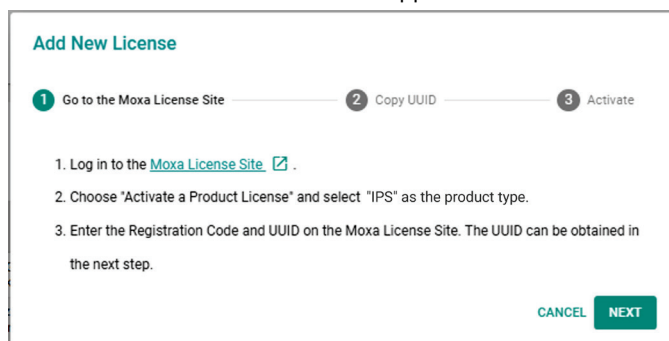
You can activate an IPS license using a valid license activation code.

Steps:

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

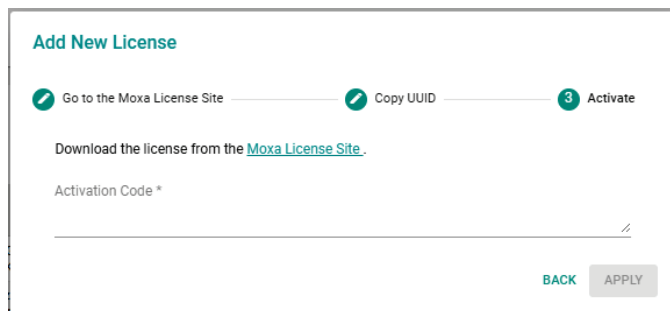
2. Click the **Add New License** button.

The **Add New License** screen will appear.



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

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



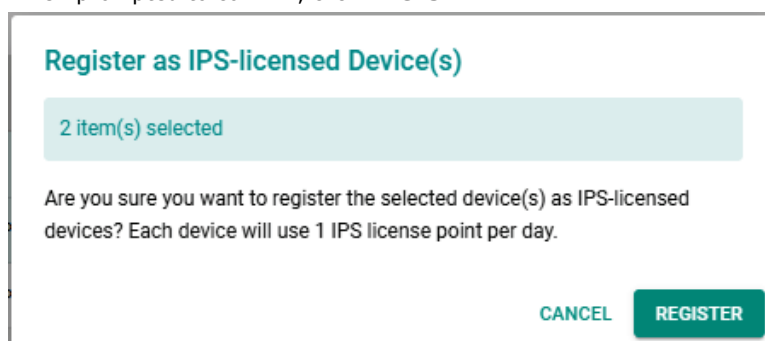
5. Click **APPLY**.
6. Verify the license information is correct.

Registering an IPS-licensed Device

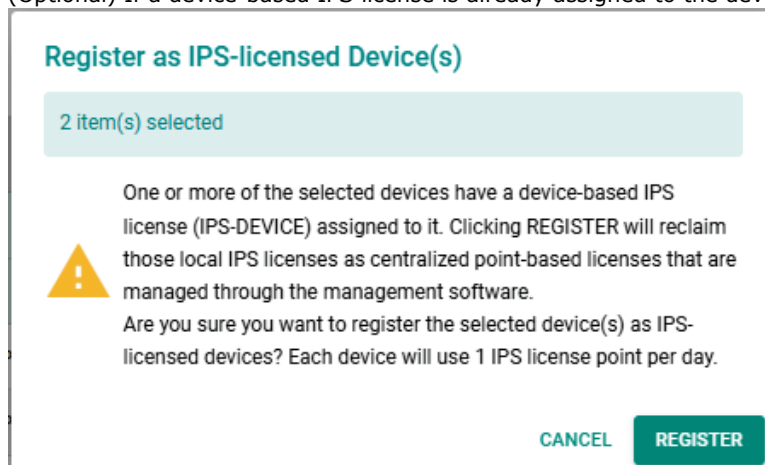
To enable full IPS functionality on a device, you must register the device as an IPS-license device. Once registered, the device will consume one IPS license point per day.

Steps:

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



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



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



NOTE

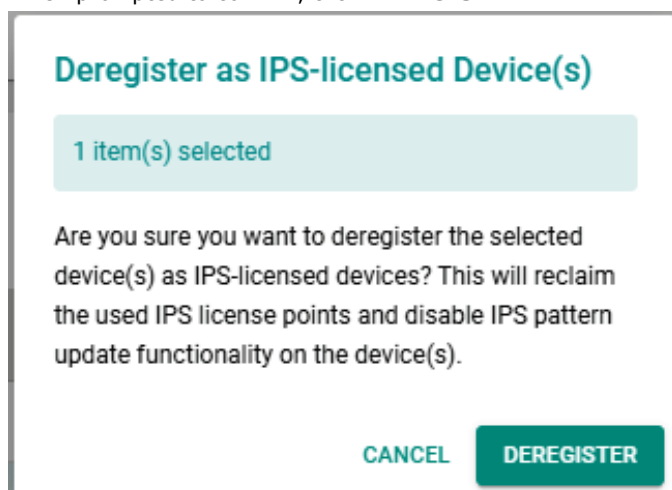
When reclaiming a device-based IPS (IPS-DEVICE) license, the management software will reclaim and reassign the license as a centrally managed IPS license. The original license will be added to the total IPS point balance.

Deregistering an IPS-licensed Device

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

Steps:

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



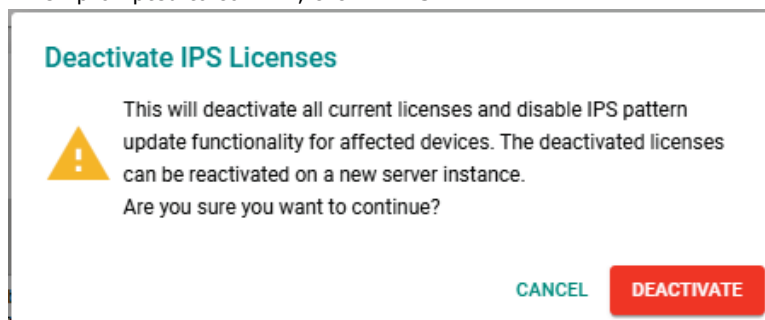
Transferring an IPS License

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

Steps:

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

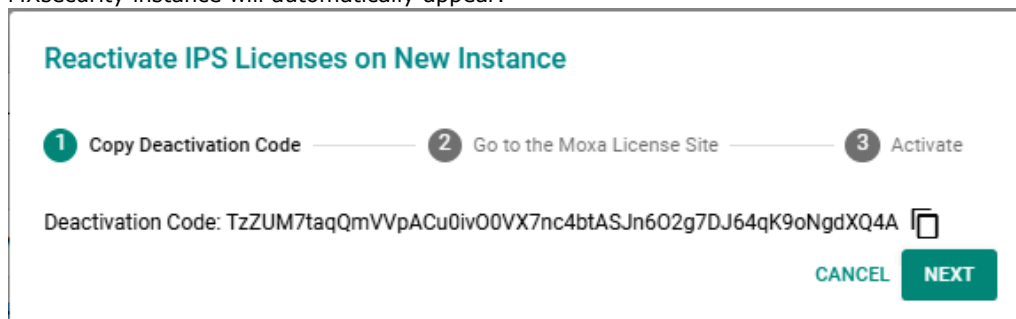
- When prompted to confirm, click **DEACTIVATE**.



NOTE

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

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



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



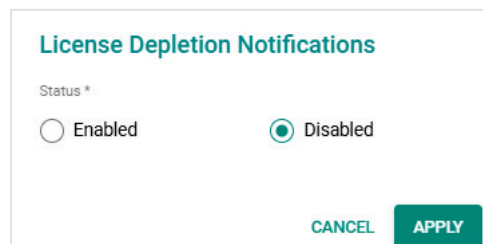
- Follow the steps in the reactivation wizard to complete the license transfer process.

Configuring IPS License Depletion Notifications

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

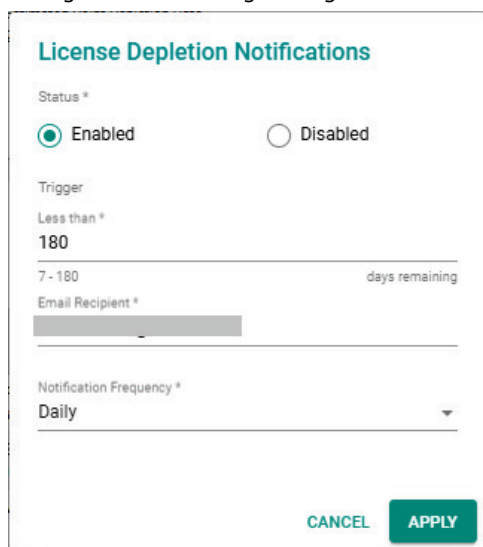
Steps:

- Navigate to **System > Licenses**.
- Click the **IPS** tab.
- Click the **License Depletion Notifications** button. The **License Depletion Notifications** screen will appear.



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

5. Configure the following settings:



The image shows a configuration window titled "License Depletion Notifications". It contains the following fields and controls:

- Status ***: Two radio buttons, "Enabled" (selected) and "Disabled".
- Trigger**: A section with a label "Less than *" and a text input field containing "180". Below the input field, it says "7 - 180" and "days remaining".
- Email Recipient ***: A text input field with a gray placeholder bar.
- Notification Frequency ***: A dropdown menu with "Daily" selected.
- At the bottom right, there are two buttons: "CANCEL" and "APPLY".

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

Settings

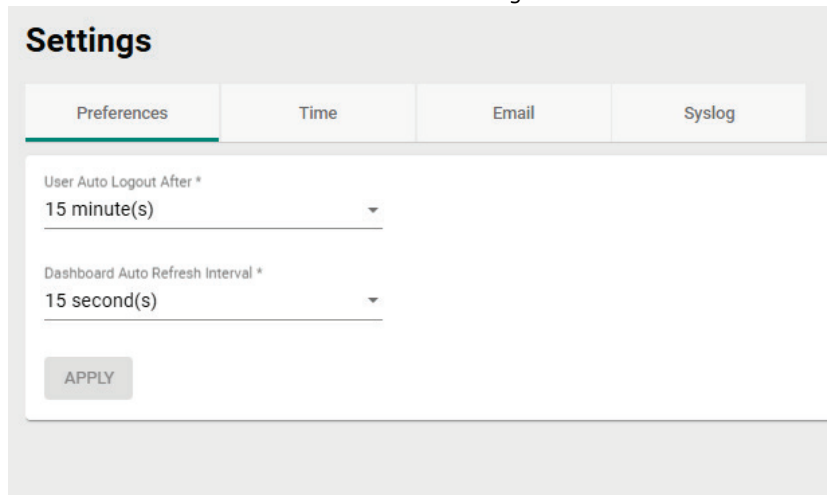
From the **Settings** page, you can configure system preferences, time, email, and syslog settings.

Configuring Preferences

From the **Preferences** screen, you can configure 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.



Settings

Preferences Time Email Syslog

User Auto Logout After *

15 minute(s)

Dashboard Auto Refresh Interval *

15 second(s)

APPLY

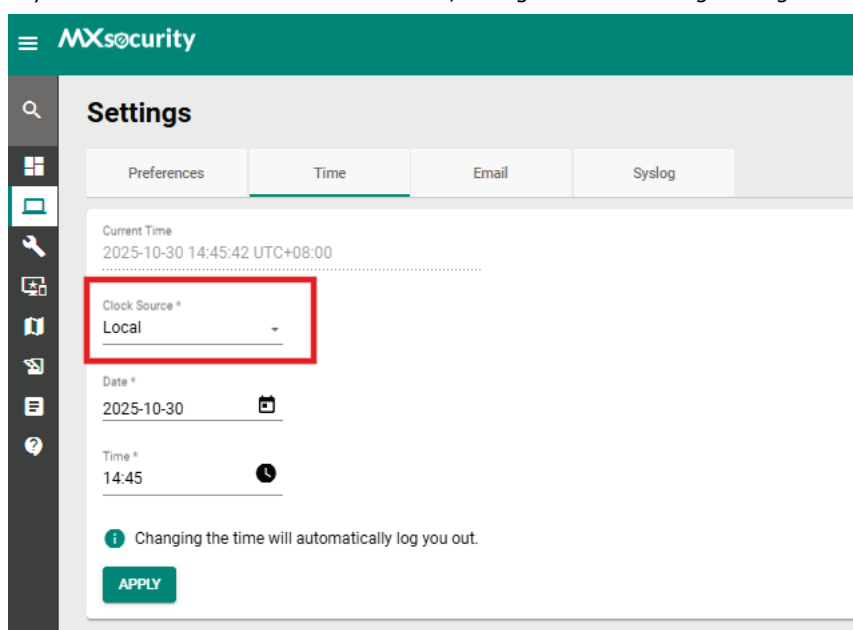
3. Click **APPLY**.

Configuring the System Time

From the **Time** tab, you can manually set the system time.

Steps:

1. Navigate to **System > Settings > Time**.
2. Select the **Clock Source**. Available settings depend on the selected option.
3. If you selected **Local** as the clock source, configure the following settings:



MXsecurity

Settings

Preferences Time Email Syslog

Current Time

2025-10-30 14:45:42 UTC+08:00

Clock Source *

Local

Date *

2025-10-30

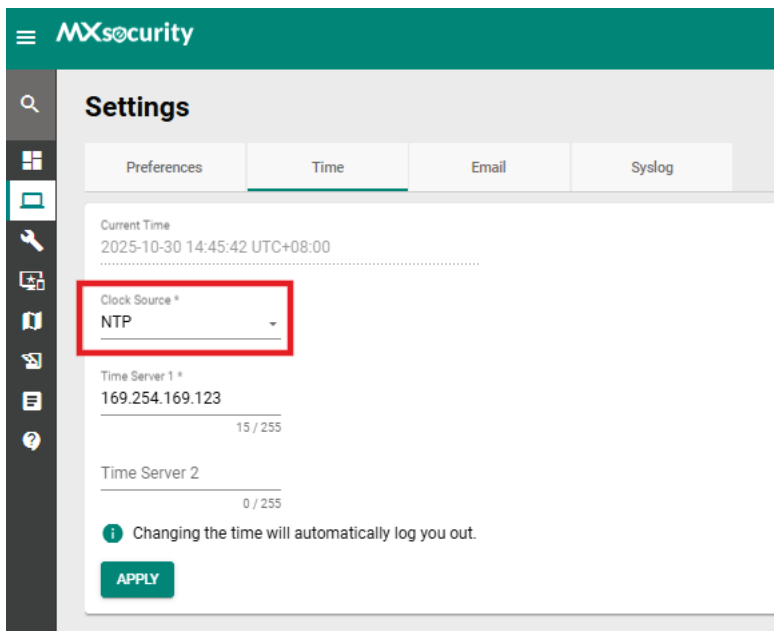
Time *

14:45

Changing the time will automatically log you out.

APPLY

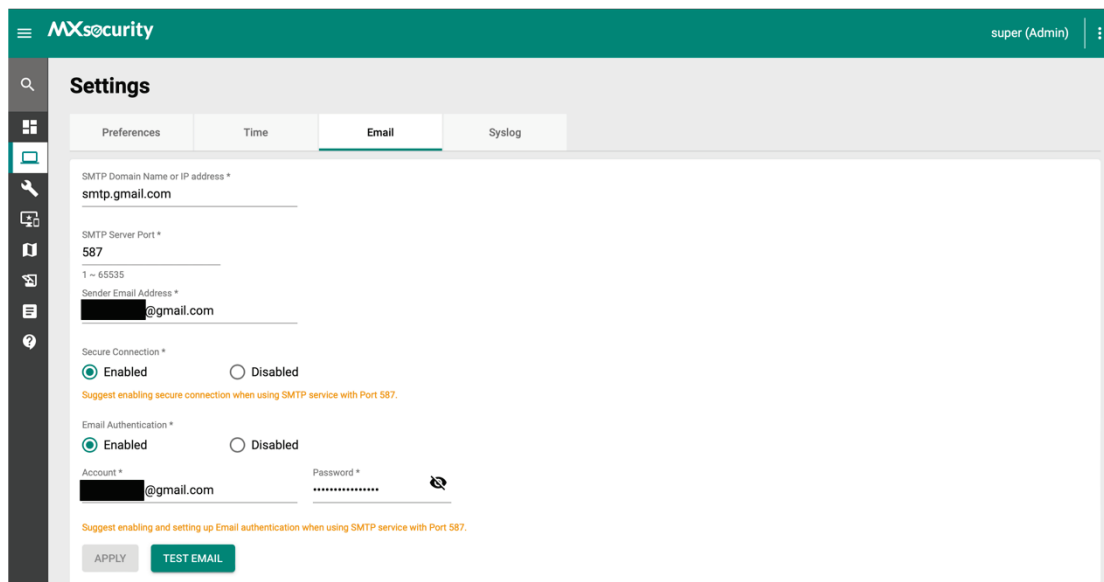
- a. **Date:** Click the  icon to select the date.
- b. **Time:** Click the  icon to select the time.
4. If you selected **NTP** as the clock source, configure the following settings:



- a. **Time Server 1/2:** Specify the time server IP address. You need to configure at least one time server.
5. Click **APPLY**.

Editing Email Settings

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



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

Field	Description
SMTP Domain Name or IP address	The SMTP server domain name or IP address.

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



NOTE

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

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

When finished, click **APPLY**.

Editing Syslog Settings

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

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

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

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

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

When finished, click **APPLY**.