

Security Dashboard Console User's Manual

Version 1.0, May 2020

www.moxa.com/product



© 2020 Moxa Inc. All rights reserved.

Security Dashboard Console User's 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

© 2020 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

Moxa Americas

Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa Europe

Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa India

Tel: +91-80-4172-9088
Fax: +91-80-4132-1045

Moxa China (Shanghai office)

Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

Moxa Asia-Pacific

Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Table of Contents

1. Introduction	1-1
Key Features	1-3
Extensive Support for Industrial Protocols	1-3
Policy Enforcement for Mission-critical Machines	1-3
Intrusion Prevention and Intrusion Detection	1-3
Asset Management of Mission-Critical Machines	1-3
Centralized Management	1-3
System Requirements	1-4
2. Installation	2-1
Setting Up the Virtual Machine	2-2
Installing SDC on a VMware Workstation	2-2
Security Dashboard Console Onboard to VMware ESXi	2-5
Configuring the SDC system	2-11
3. Getting Started	3-1
Getting Started Task List	3-2
Opening the Management Console	3-2
Syncing IEC-G102-BP Series Devices to SDC	3-3
4. Dashboard and Widgets	4-1
Dashboard Widgets Overview	4-2
Assets Type	4-2
Environment Summary (Group Summary)	4-3
Device List	4-3
Device Status Count	4-3
Node License Usage	4-3
CPU Usage	4-4
Memory Usage	4-4
Disk Usage	4-4
Load Average	4-4
Top N Cyber Security Events by Source IP	4-5
Top N Cyber Security Events by Destination IP	4-5
Top N IPS Attack Events Categories	4-5
Top N Cyber Security Events	4-6
Top N Cyber Security Severity	4-6
Trends of Top N Cyber Security Events Categories	4-6
Trends of Top N Cyber Security Severity	4-7
Top N Cyber Security Events by Device	4-7
Top N Protocol Filter Events by Source IP	4-7
Top N Protocol Filter Events by Destination IP	4-8
Top N L7 Protocols	4-8
Trend of Top 5 L7 Protocols	4-8
Top N L7 Protocol Filter Events by Device	4-9
Top N Policy Enforcement Events by Source IP	4-9
Top N Policy Enforcement Events by Destination IP	4-9
Top N Policy Enforcement Events by Device	4-10
Tab and Widget Management	4-10
Adding a Tab to the Dashboard	4-10
Deleting a Tab on the Dashboard	4-10
Adding a Widget to the Dashboard	4-10
Removing a Widget from the Dashboard	4-11
Resizing a Widget	4-11
Pausing and Resuming Widget Refreshing	4-11
Configuring Widget Settings	4-11
5. The Visibility Tab	5-1
Common Tasks	5-2
Displaying Asset Information	5-2
Basic Asset Information	5-2
Real-time Network Application Traffic	5-4
6. Node Management	6-1
Common Tasks	6-2
Group Management	6-3
Creating a New Device Group	6-3
Renaming or Deleting a Device Group	6-3
Moving a Node into a Group	6-4
Managing IEC-G102-BP Series Devices	6-4
Accessing the Management Tab	6-4
Updating the Firmware	6-4

Switching Firmware	6-5
Editing the Name or Location of a Node.....	6-5
Rebooting a Node.....	6-5
Configuring Security Operation Mode	6-5
Configuring Cyber Security	6-7
Configuring Policy Enforcement	6-10
Configuring Pattern Setting	6-13
Sharing Management Permissions to Other User Accounts	6-14
7. Object Profiles	7-1
Configuring IP Object Profiles	7-2
Configuring Service Object Profiles.....	7-3
Configuring Protocol Filter Profiles.....	7-4
8. Logs	8-1
Viewing Cyber Security Logs	8-2
Viewing Protocol Filter Logs.....	8-5
Viewing System Logs	8-7
Viewing Audit Logs.....	8-9
Viewing Asset Detection Logs	8-11
Viewing Policy Enforcement Logs	8-13
9. Administration	9-1
Account Management	9-2
User Roles	9-2
Account Input Format	9-4
Adding a User Account	9-5
Changing Your Password	9-5
Configuring the Password Policy	9-5
ID/Password Reset	9-6
Configuring System Time.....	9-7
Configuring Syslog Settings	9-8
Syslog Severity Levels	9-9
Syslog Severity Level Mapping Table	9-9
Updates.....	9-9
Updating Components Manually	9-10
Importing a Component File	9-10
Scheduling Component Updates.....	9-11
Managing the Component Repository	9-11
Managing SSL Certificates.....	9-11
Replacing an SSL certificate.....	9-11
Verifying an SSL certificate	9-12
Removing the Built-in Certificate	9-12
Log Purge	9-12
Viewing Database Storage Usage	9-12
Configuring Automatic Log Purge.....	9-13
Manually Purging Logs	9-13
Back Up/Restore.....	9-14
Restoring a Configuration	9-14
License.....	9-15
Introduction to the Licenses.....	9-15
Viewing Your Product License Information	9-15
Alert Messages.....	9-16
Activating or Renewing Your Product License	9-16
Manually Refresh the License.....	9-17
Proxy	9-17
Configuring Proxy Settings	9-17
A. Setting SDC's Connection	A-1
Setting up a Connection to SDC Via the IEC-G102-BP Series Web Console	A-1
B. Introduction to the vShell	B-1
First Time Using vShell	B-2
Accessing vShell.....	B-2
Change the Default Password to Activate	B-2
How to Set Up a Network.....	B-3
Displaying the Network Settings.....	B-3
Update the Interface Settings	B-4
How to Set Up the ACL	B-6
Querying the Status	B-6
Adding Clients to the Whitelist	B-6
Deleting Clients from the Whitelist.....	B-6
Enable/Disable the ACL of Modules	B-7
Shortcut Table	B-7
List of Command Prompt Commands.....	B-7

Summary	B-7
access-list	B-8
env.....	B-8
exit	B-8
help.....	B-9
iface	B-9
ping.....	B-11
poweroff	B-11
reboot.....	B-11
resolv	B-11
scp	B-12
service.....	B-12
sftp	B-12

Terms and Acronyms

Term/Acronym	Definition
CEF	Common Event Format
EWS	Engineering Workstation
HMI	Human-Machine Interface
ICS	Industrial Control System
IT	Information Technology
SDC	Security Dashboard Console
OT	Operational Technology
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition

The following topics are covered in this chapter:

❑ **Key Features**

- Extensive Support for Industrial Protocols
- Policy Enforcement for Mission-critical Machines
- Intrusion Prevention and Intrusion Detection
- Asset Management of Mission-Critical Machines
- Centralized Management

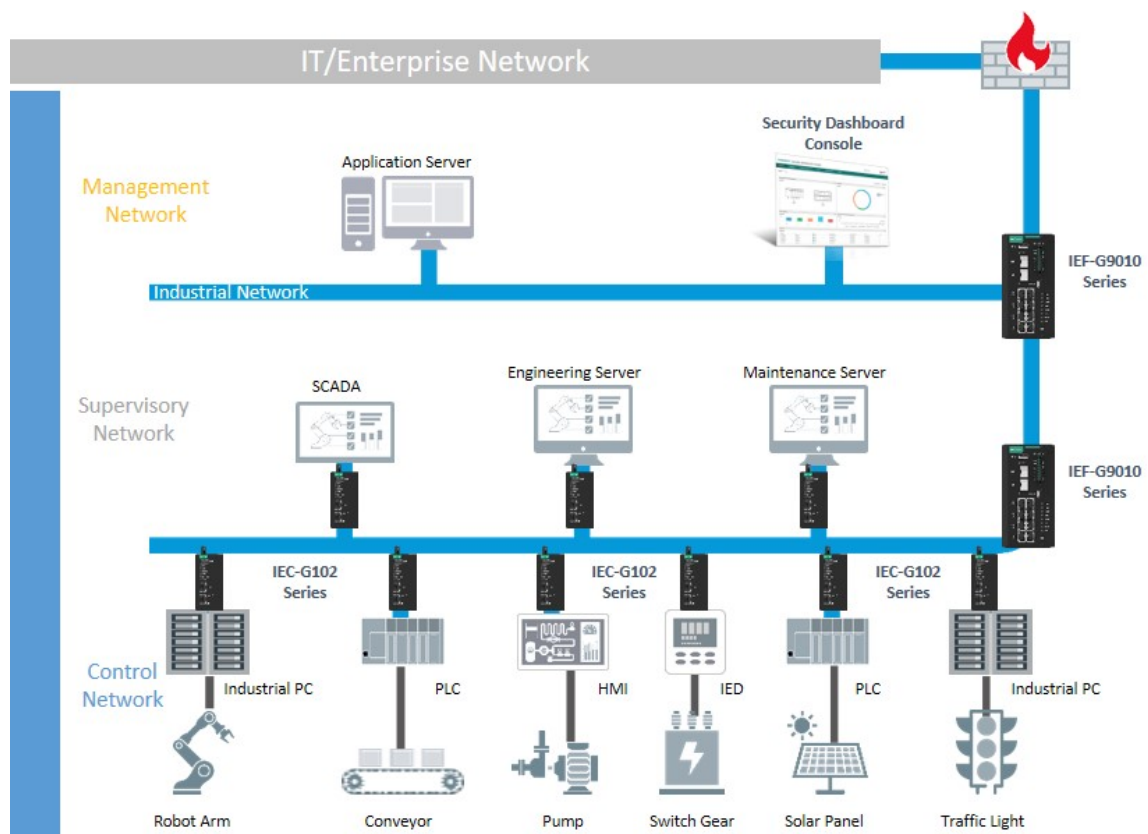
❑ **System Requirements**

Security Dashboard Console (or SDC) is a web-based management console that provides a graphical user interface for device configuration and security policy settings. The management process is designed to comply with the manufacturing SOP of the industry. SDC centrally monitors operational information, edits network protection policies, sets patterns of attack behaviors, and generates reports of security events. All IEC-G102-BP series and IEF-G9010 series are deployed throughout the entire information technology (IT) and operational technology (OT) infrastructure.

IT and OT traditionally are operated separately, each with its own network, transportation team, goals, and needs. In addition, each industrial environment is equipped with tools and devices that were not designed to connect to a corporate network, thus making provisioning timely security updates or patches difficult. Therefore, the need for security products that provide proper security protection and visibility is on the rise.

MOXA provides a wide range of security products that cover both IT and OT layers. These easy-to-build solutions provide active and immediate protection to Industrial Control System (ICS) environments with the following features:

- Certified industrial-grade hardware with size, power consumption, and durability tailored for OT environments and the ability to tolerate a wide range of temperature variations
- Threat detection and interception against the spread of worms
- Protection against Advanced Persistent Threats (APTs) and Denial of Service (DoS) attacks that target vulnerable legacy devices
- Virtual patch protection against OT device exploits



Key Features

The Moxa IEC-G102-BP and IEF-G9010 Series are a lineup of security devices managed by the Security Dashboard Console. The following describes the main functions of the product suite:

Extensive Support for Industrial Protocols

The IEC-G102-BP and IEF-G9010 Series support the identification of a wide range of industrial control protocols, including Modbus and other protocols used by well-known international companies such as Siemens, Mitsubishi, Schneider Electric, ABB, Rockwell, Omron, and Emerson. In addition to allowing OT and IT security system administrators to work together, this feature provides the flexibility to deploy defense measures in appropriate network segments and seamlessly connects them to existing factory networks.

Policy Enforcement for Mission-critical Machines

The IEC-G102-BP Series and IEF-G9010 series allow administrators to maintain a policy enforcement database. By analyzing Layer 3 to Layer 7 network traffic between mission-critical machines, policy enforcement executes filtering of control commands within the protocols and blocks traffic that is not defined in the policy rules. This feature can help prevent unexpected operational traffic, block unknown network attacks, and block other activity that matches a defined policy.

Intrusion Prevention and Intrusion Detection

IPS/IDS provides a powerful, up-to-date first line of defense against known threats. Vulnerability filtering rules provide effective protection against exploits at the network level. Manufacturing personnel manage patching and updating, providing pre-emptive protection against critical production failures and additional protection for old or terminated software.

Asset Management of Mission-Critical Machines

The IEC-G102-BP Series and IEF-G9010 series, when deployed at the forefront of critical production equipment, can be viewed as security sensors. Each IEC-G102-BP Series and IEF-G9010 series node grants network traffic control without interfering with production line performance. The deployed security devices also analyze network traffic and visualize network topology, as well as key devices, on the Security Dashboard Console. In addition to providing detailed analysis of events, the Security Dashboard Console also helps operators to control and monitor legacy devices.

Centralized Management

Security Dashboard Console (SDC) provides administrators with a graphical user interface for policy management in accordance with the manufacturing SOP and regulations. With SDC, administrators can centrally monitor operations information, edit network protection policies, and set patterns for attack behaviors.

All protections are deployed throughout the entire information technology (IT) and operational technology (OT) infrastructure. These include:

- A centralized policy deployment and reporting system
- Full visibility into assets, operations, and security threats
- IPS and policy enforcement configuration can be assigned per device group, allowing all devices in the same device group to share the same policy configuration
- Management permissions for device groups can be assigned per user account

System Requirements

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

	System Requirements				
Managed Nodes	50	100	200	300	500
CPU (virtual cores)	4	4	8	12	16
RAM	8 GB	16 GB	16 GB	32 GB	32 GB
Hard Disk Space	256 GB or above (recommended)				
Supported Virtual Machines	VMWare ESXi 6.x or above, VM Workstation 14 or above, KVM 2.x or above, XEN 4.4. (available in 2020), Hyper V (available in 2020)				

The following topics are covered in this chapter:

▣ **Setting Up the Virtual Machine**

- Installing SDC on a VMware Workstation
- Security Dashboard Console Onboard to VMware ESXi
- Configuring the SDC system

Setting Up the Virtual Machine

Installing SDC on a VMware Workstation

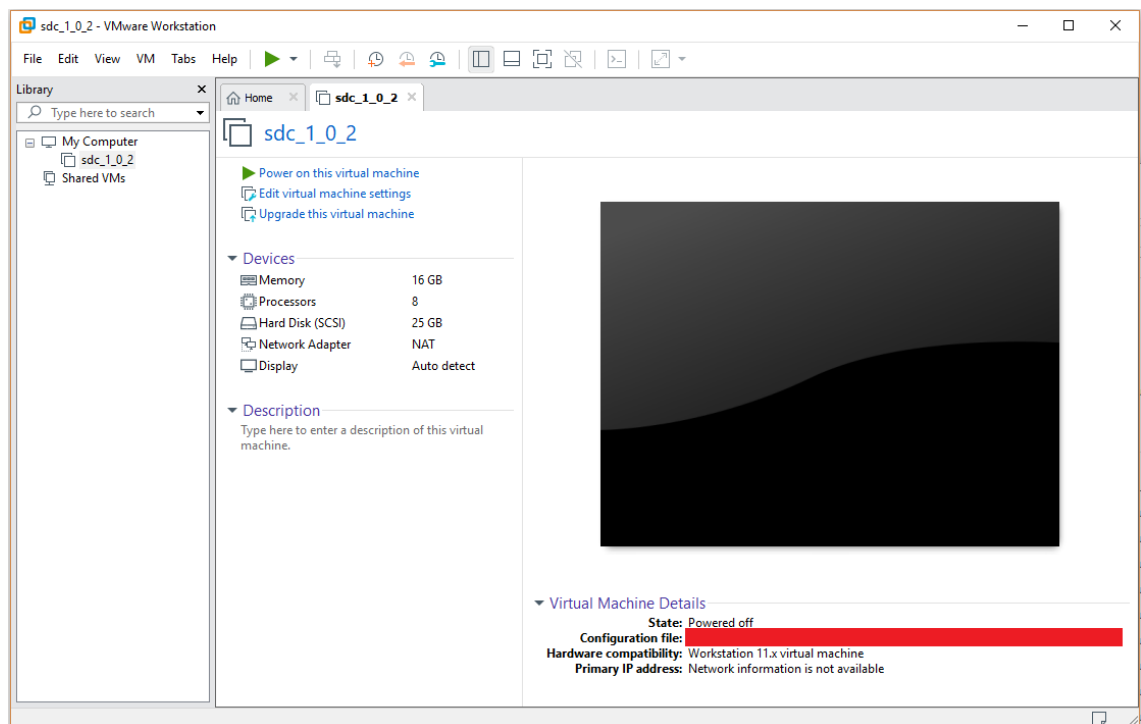
This section describes how to deploy Security Dashboard Console to a VMware Workstation system.

Prerequisites

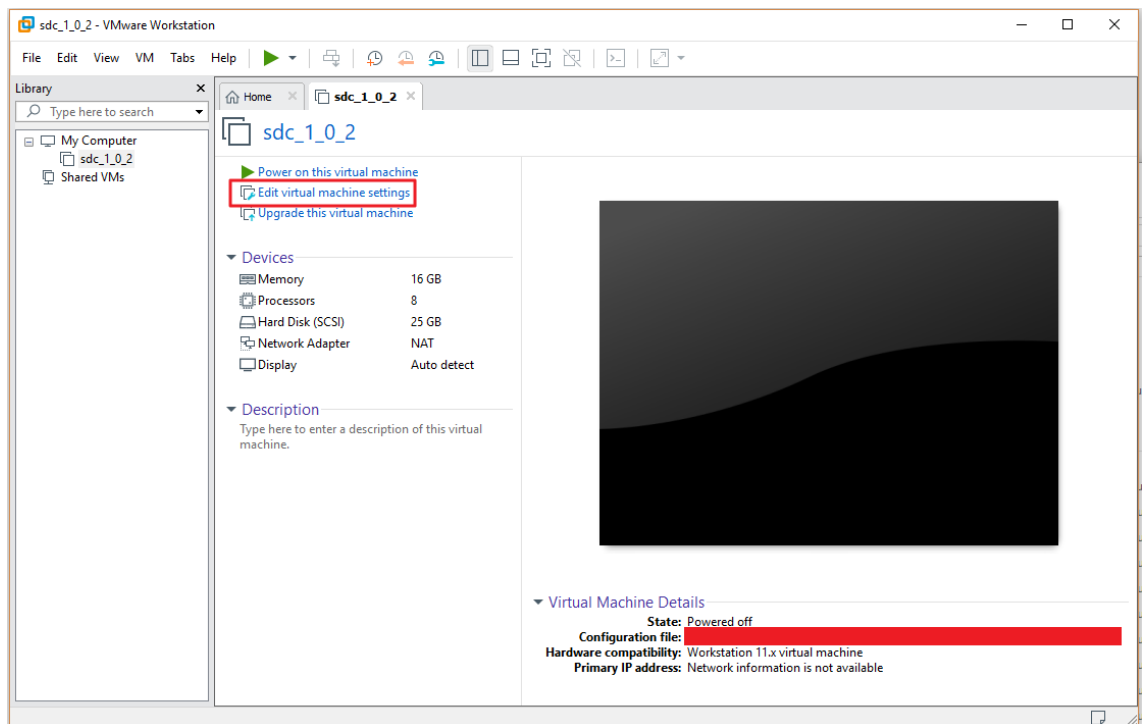
- The OVA packages provided by Moxa must be available and accessible to the VMware Workstation.
- VMware workstation 14 or later is required.

Deploying Security Dashboard Console

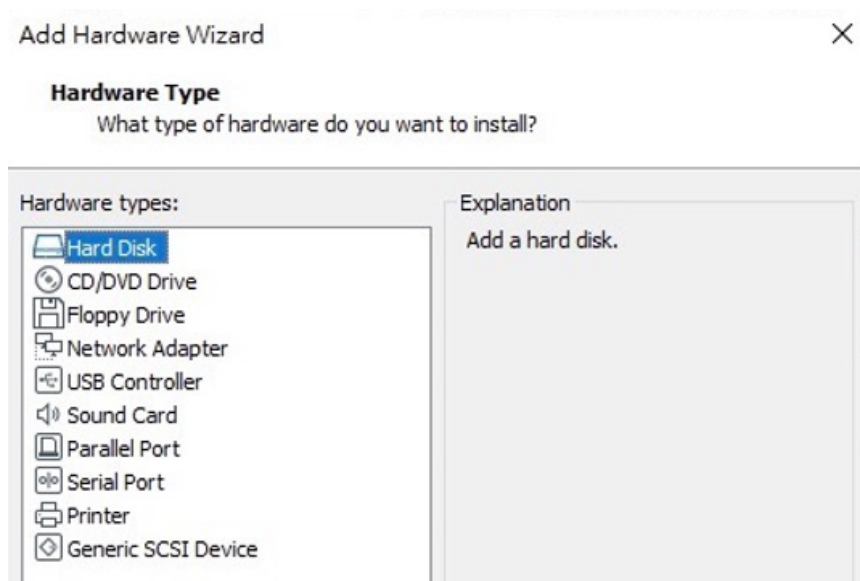
1. Start the VMware Workstation and click **File** in the menu bar.
2. Select **Open** to import the SDC VM image file (*.ova).
3. Select the SDC VM image file from your localhost file path and click **Open**.
4. Specify the name and the storage path for the new virtual machine, and then click **Import**.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



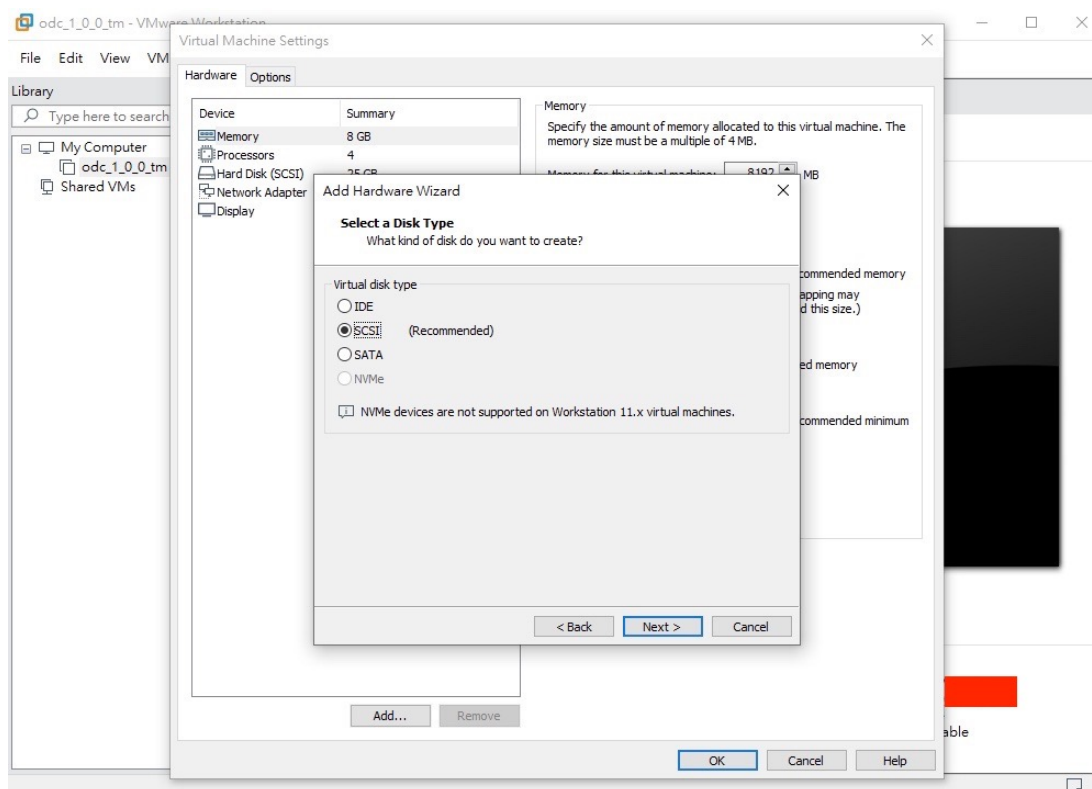
6. Add an external disk.
 - a. Click **Edit virtual machine settings**.



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

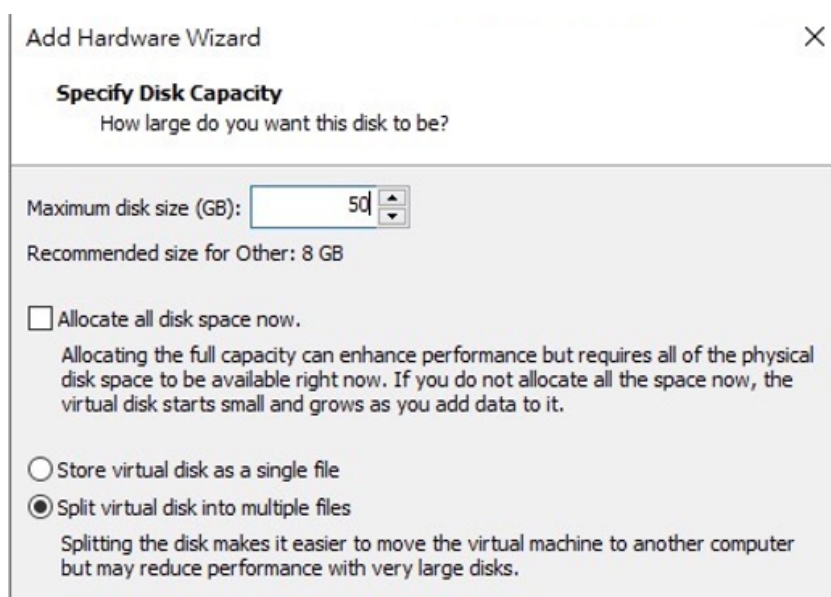


- c. Select a disk type.



- d. Set the disk space of the new hard disk to at least 50 GB. You can configure the external disk size depending on the number of logs to be stored, as shown in the suggestion table below.

Number of Logs	Required Disk Size
10,000,000	50 GB
50,000,000	150 GB
100,000,000	300 GB



- e. Select the path to store the disk.
 f. Click **OK**.
 g. **(Optional)** If necessary, you can increase the disk size to hold a larger number of SDC logs. To increase the disk size, power off the SDC, increase the external disk size based on your

requirements, then power the SDC back on. SDC will enlarge the storage available for storing log files.

7. **(Optional)** Adjust your SDC instance to use proper resource configurations based on the following sizing table or using default settings (8 CPU cores, 16 GB of memory). Click **Edit virtual machine settings**.

Sizing Table

Nodes	CPU	Memory
50	4 cores	8 GB
100	4 cores	16 GB
200	8 cores	16 GB
300	12 cores	32 GB
500	16 cores	32 GB

- a. Click **Edit virtual machine settings**.
 - b. Configure the amount of memory.
 - c. Configure the number of CPU cores.
8. **(Optional)** Depending on your network environment, change the network adapter setting from 'NAT' to 'Bridged' if necessary.
 - a. Right-click the SDC VM icon and select **Settings**.
 - b. Select **Network Adapter** and change the default setting from **NAT** to **Bridged** if necessary.
 9. Boot the SDC VM, and the SDC instance will start.

Migrating to a Newer Version of SDC

When a new version of SDC is released, you can migrate the settings of the old SDC by attaching the external disk of the old SDC to the new SDC VM. Settings that are migrated include:

- The UUID of the old SDC.
 - The pattern and firmware downloaded by the old SDC.
 - The system configuration set from the old SDC including its license, account information, security policies, etc.
 - The security event logs stored by old SDC.
1. Launch the new instance of SDC (refer to section **Deploying Security Dashboard Console**)
 2. Power off the old SDC.
 3. Attach the external disk of the old SDC to the new SDC.
 4. A window will appear where you can select which settings and data to migrate to the new SDC. After confirming, the selected information of the old SDC will be migrated over to the new SDC.

Security Dashboard Console Onboard to VMware ESXi

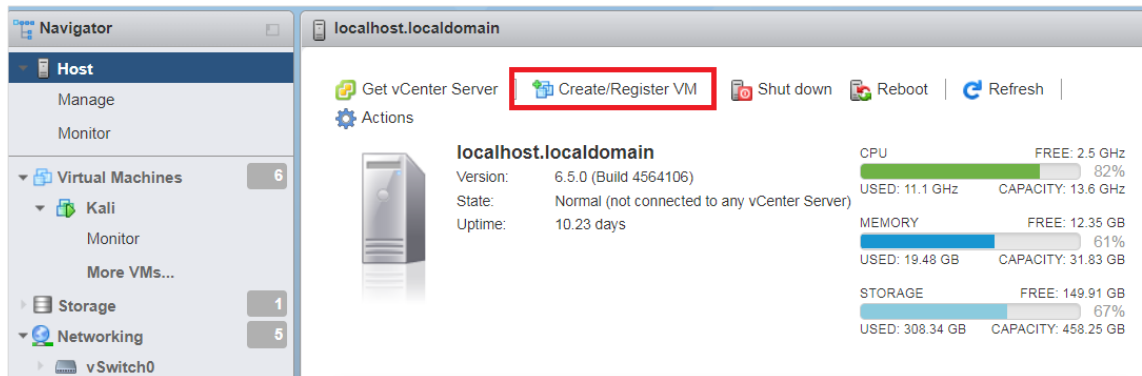
This section describes how to deploy Security Dashboard Console to a VMware ESXi system.

Prerequisites

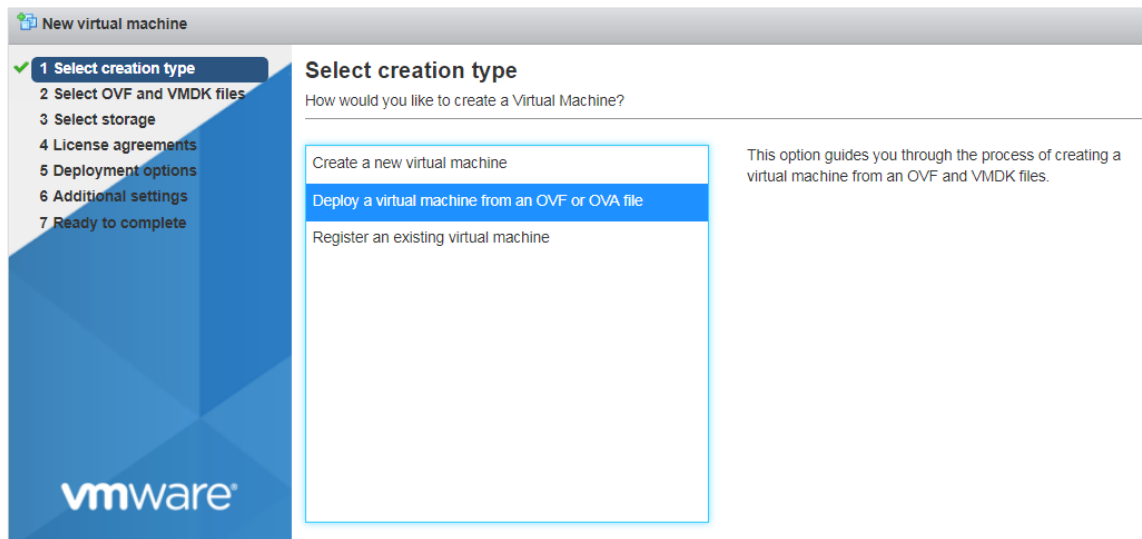
- The OVA packages provided by Moxa must be available and accessible to VMware ESXi.
- ESXi version 6 or above with the required specifications.
- The necessary networks have been properly created in ESXi.

Deploying Security Dashboard Console

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 SDC and then select an SDC image to upload.

5. Choose a storage location for the SDC virtual machine.

The screenshot shows the 'New virtual machine - odc' wizard at the 'Select storage' step. On the left, a progress bar indicates the following 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'.

6. Select **Deployment options**.

The screenshot shows the 'New virtual machine - odc' wizard at the 'Deployment options' step. On the left, the progress bar indicates: 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 'test' in the adjacent text field. 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.

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 SDC image is being uploaded. Wait until the upload has finished.
8. Add an external disk with at least 50 GB of space to the SDC instance.
 - a. Power off the SDC 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

Size: 8 Unit: MB Capacity: 20480

Hard disk 1: 25 GB

SCSI Controller 0: LSI Logic Parallel

Network Adapter 1: test ☒ Connect

Video Card: Specify custom settings

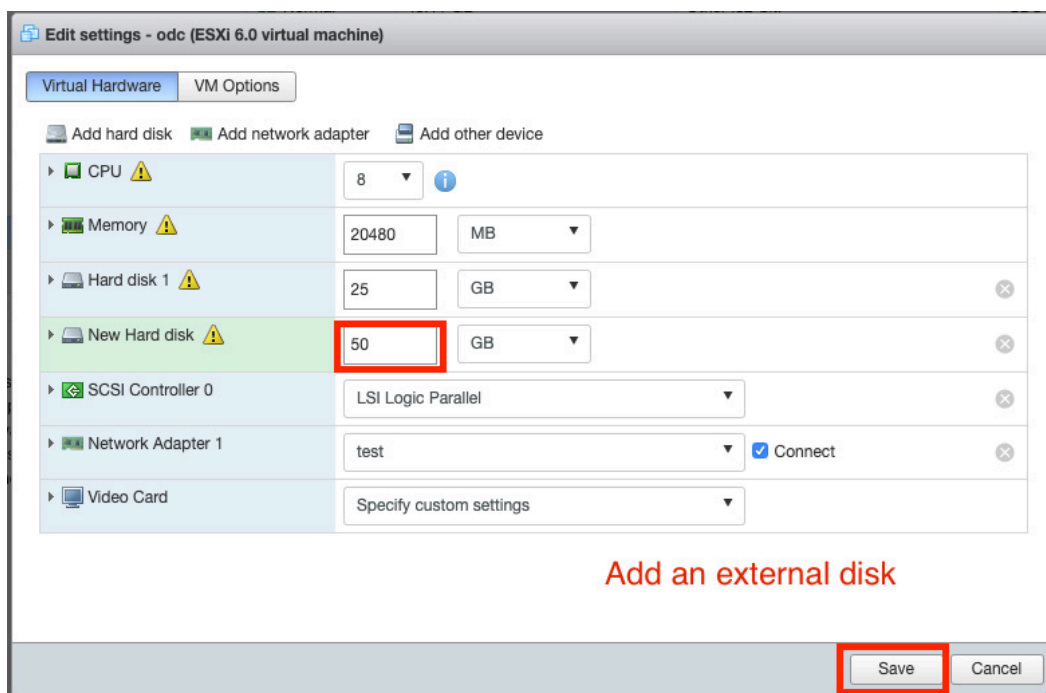
Save Cancel

- c. Set the disk space of the new hard disk to at least 50 GB and click **Save**. You can configure the external disk size depending on the number of logs to be stored, as shown in the suggestion table below.

Number of Logs	Required Disk Size
10,000,000	50 GB
50,000,000	150 GB

100,000,000

300 GB



- d. **(Optional)** If necessary, you can increase the disk size to hold a larger number of SDC logs. To increase the disk size, power off the SDC, increase the external disk size based on your requirements, then power the SDC back on. SDC will enlarge the storage available for storing log files.
- . If you want to migrate the existing SDC settings to the newly launched VM, please refer to **System Migration**.

NOTE The SDC requires one external disk with at least 50 GB of free disk space, otherwise the SDC will not be able finish initialization and complete the boot up process.

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

9. Power on the VM.

(Optional) Adjust your SDC instance to use proper resource configurations based on the following sizing table or using the default settings (8 core CPU, 16 GB memory).

Sizing Table

Nodes	CPU	Memory
50	4 cores	8 GB
100	4 cores	16 GB
200	8 cores	16 GB
300	12 cores	32 GB
500	16 cores	32 GB

- a. Shut down the instance of SDC and click **Edit**.
The **Edit settings** window appears.

- b. Configure the number of CPU cores.

Virtual Hardware VM Options

Add hard disk Add network adapter Add other device

CPU	8	
Memory	16384	MB
Hard disk 1	100	GB
SCSI Controller 0	LSI Logic Parallel	
Network Adapter 1	VM Network	<input checked="" type="checkbox"/> Connect
Video Card	Specify custom settings	

Save Cancel

- c. Configure the amount of memory.

Edit settings - 0.8.1-Neo-ODC (ESXi 6.0 virtual machine)

Virtual Hardware VM Options

Add hard disk Add network adapter Add other device

CPU	8	
Memory	16384	MB
Hard disk 1	100	GB
SCSI Controller 0	LSI Logic Parallel	
Network Adapter 1	VM Network	<input checked="" type="checkbox"/> Connect
Video Card	Specify custom settings	

Save Cancel

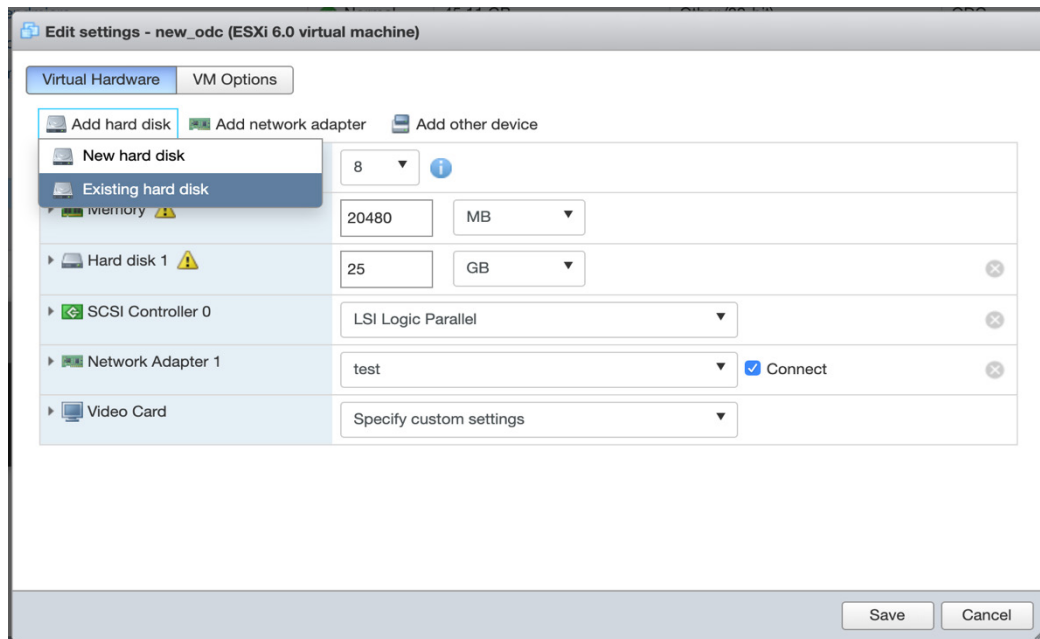
- d. Click **Save**.
- e. Boot the SDC instance.

Migrating to a Newer Version of SDC

When a new version of SDC is released, you can migrate the settings of the old SDC by attaching the external disk of the old SDC to the new SDC VM. Settings that are migrated include:

- The UUID of the old SDC. To ensure all virtual machines are identified properly, each virtual machine is automatically assigned a universal unique identifier (UUID).
- The pattern and firmware downloaded by the old SDC.

- The system configuration set from the old SDC including its license, account information, security policies, etc.
 - The security event logs stored by old SDC.
1. Launch the new instance of SDC. Refer to the **Deploying Security Dashboard Console** section for instructions on how set up a new SDC instance.
 2. Power off the old SDC.
 3. Attach the external disk of the old SDC to the new SDC.
 4. The old SDC's information will be migrated into the new SDC.



Configuring the SDC system

Accessing the SDC CLI

1. Open the SDC VM console.
2. Log in with username **root** and password **moxa**.

```
Debian GNU/Linux 9 SDC tty1

SDC login: root
Password:
Linux SDC 4.9.0-11-amd64 #1 SMP Debian 4.9.189-3+deb9u2 (2019-11-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
vShell, version v1.1.0

If you want to exit this shell, please type `exit` or `Ctrl-D`.

Caution: please type the command ``oobe`` to activate the vShell.
Caution: please type the command ``oobe`` to activate the vShell.
Caution: please type the command ``oobe`` to activate the vShell.
Caution: please type the command ``oobe`` to activate the vShell.
Caution: please type the command ``oobe`` to activate the vShell.
$
```

3. Change the default password
 - a. Enter the **oobe** command.
 - b. Change the default password.
 - c. Log in to the SDC again with your new password.

```
Debian GNU/Linux 9 SDC tty1

SDC login: root
Password:
Last login: Thu Mar 12 15:58:01 GMT 2020 on tty1
Linux SDC 4.9.0-11-amd64 #1 SMP Debian 4.9.189-3+deb9u2 (2019-11-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
vShell, version v1.1.0

If you want to exit this shell, please type `exit` or `Ctrl-D`.
$ _
```

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

```
vShell, version v1.1.0
The commands provided in:
access-list  Manage the IP whitelists
env          Manage system environment variables
exit        Exit this shell
help        List all command usage
iface       Manage the network interfaces
ping        Test the reachability of a host
poweroff    Shut down the machine immediately
pwd         Change the root user password
reboot      Restart the machine immediately
resolv      Manage the domain name server
scp         Send files via scp
service     Manage the dashboard service
sftp        Send files via sftp

Shortcut table:
Tab         Auto-complete or choose the next suggestion on the list
Ctrl + A   Go to the head of the line (Home)
Ctrl + E   Go to the tail of the line (End)
Ctrl + D   Delete the character located at the cursor
Ctrl + L   Clear the screen
$ _
```

Getting the IP Address of the SDC Instance

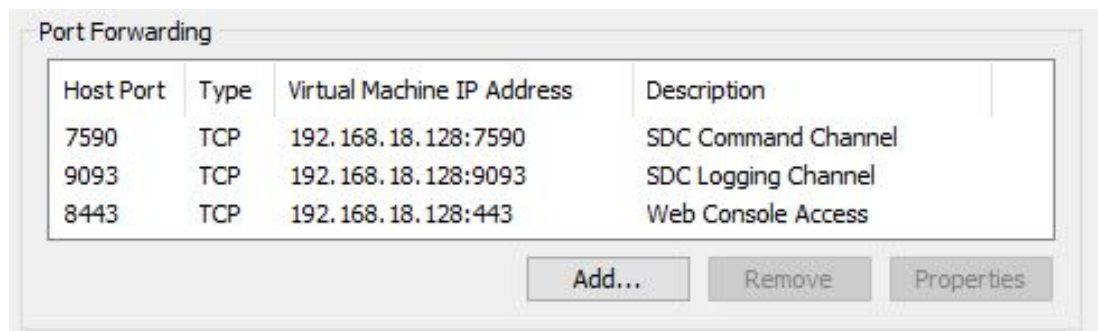
1. Enter the **iface ls** command to get the IP address of the SDC instance.

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
vShell, version v1.1.0

If you want to exit this shell, please type `exit` or `Ctrl-D`.
$ iface ls
[
  {
    "Name": "lo",
    "Family": "inet",
    "Method": "loopback"
  },
  {
    "Name": "eth0",
    "Family": "inet",
    "Method": "dhcp"
  }
]
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:5b:39:06 brd ff:ff:ff:ff:ff:ff
    inet 192.168.18.128/24 brd 192.168.18.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe5b:3906/64 scope link
        valid_lft forever preferred_lft forever
$
```

2. If your VMware network adapter setting is using NAT, you will need to create port forwarding rules to allow traffic to pass from the IEC-G102-BP Series to the SDC.
 - a. Navigate to **Edit → Virtual Network Editor**, select the right network subnet and click **NAT Settings**.
 - i. To allow users to configure the IEC-G102-BP Series through the SDC including all configuration settings and commands, forward packets from the host TCP port 7590 to the SDC server IP TCP port 7590.
 - ii. To allow IEC-G102-BP Series to upload logs to the SDC, forward packets from the host TCP port 9093 to the SDC server IP TCP port 9093.
 - iii. To access a web management console, forward packets from host TCP port 8443 to the SDC server IP TCP port 443.



- a. Set up the NAT outbound IP address for the SDC environment parameters.
 - i. Find the NAT outbound IP address on the VM host PC. If the host PC uses Windows, you can find the IP address of the wireless or Ethernet interface using the **ipconfig** command.
 - ii. Type the following command in the SDC CLI to set the IP environment parameters of the SDC instance:

```
$ env exip [the NAT outbound IP address]
$ service reload
```


[Optional] Configuring the IP Address Settings

You can manually configure the IP address if necessary.

1. Use the **iface update** command to update the settings of an existing network interface. For example, the following command sets the interface "eth0" to a static IP address 10.7.19.157/24 with the gateway IP address 10.7.19.254

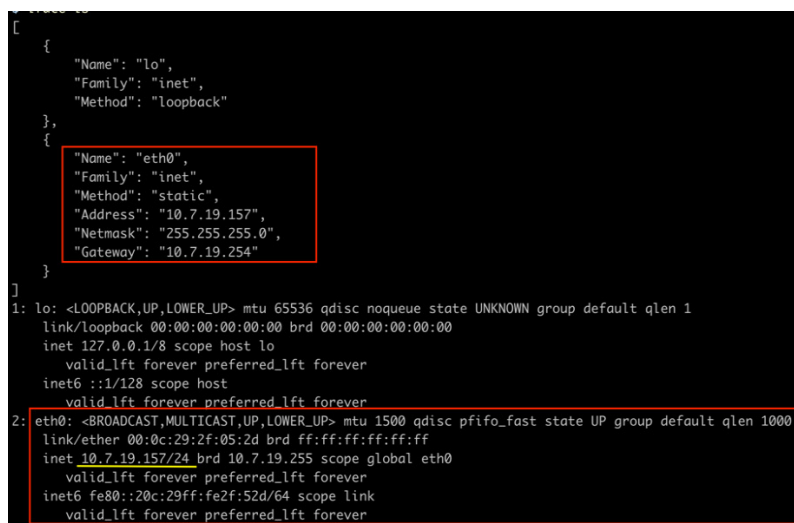
```
$ iface update eth0 --method static --address 10.7.19.157 --netmask 255.255.255.0 --gateway 10.7.19.254
```

2. Confirm the network interface settings are correct and execute the interface restart command to bring the new settings into effect.

```
$ iface restart eth0
```

3. Execute the following command to view the network interface settings.

```
$ iface ls
```



```
[
  {
    "Name": "lo",
    "Family": "inet",
    "Method": "loopback"
  },
  {
    "Name": "eth0",
    "Family": "inet",
    "Method": "static",
    "Address": "10.7.19.157",
    "Netmask": "255.255.255.0",
    "Gateway": "10.7.19.254"
  }
]
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:2f:05:2d brd ff:ff:ff:ff:ff:ff
    inet 10.7.19.157/24 brd 10.7.19.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe2f:52d/64 scope link
        valid_lft forever preferred_lft forever
```

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

```
$ resolv add 8.8.8.8
```

5. Type the following command to view the DNS server settings.

```
$ resolv ls
```



```
vShell
File Edit Tabs Help
$ resolv ls
$ resolv add 8.8.8.8
8.8.8.8 is added.
$ resolv ls
nameserver 8.8.8.8
```

6. Execute the following command to reboot the VM.

```
$ reboot
```

Getting Started

This chapter describes how to get started with Security Dashboard Console and perform the initial configuration.

The following topics are covered in this chapter:

- ❑ **Getting Started Task List**
- ❑ **Opening the Management Console**
- ❑ **Syncing IEC-G102-BP Series Devices to SDC**

Getting Started Task List

Getting Started Tasks provides a high-level overview of all procedures required to get Security Dashboard Console 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.
3. Activate the license.

For more information, see ***Activating or Renewing Your Product License***.

4. Configure the system time.

For more information, see ***Configuring System Time***.

5. **(Optional)** Configure the Syslog settings.

For more information, see ***Configuring Syslog Settings***.

6. Update the components.

For more information, see ***Updates***.

7. Create the device groups for IEC-G102-BP Series devices.

For more information, see ***Group Management***.

8. Assigning policies to the device groups.

For more information, see ***Node Management*** and ***Object Profiles***.

9. Creating user accounts and sharing device group management permissions to the user accounts.

For more information, see ***Account Management*** and ***Sharing Management Permissions to Other User Accounts***.

Opening the Management Console

Security Dashboard Console 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 63 or later; Firefox version 53 or later; Safari version 10.1 or later; or Edge version 15 or later.
-------------	--

1. In a web browser, type the address of the Security Dashboard Console in the following format:

`https://<target server IP address or FQDN>`

The login screen appears.

2. Enter your user name and password.

Use the default administrator credentials when logging in for the first time:

- User name: admin
- Password: moxa

3. Click **Log On**.

If this is your first time logging in, the Login Information Setup frame will appear.

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

NOTE The new login name cannot be "root", "admin", "administrator", or "auditor" (case-insensitive).

a. Enter your new log in details.

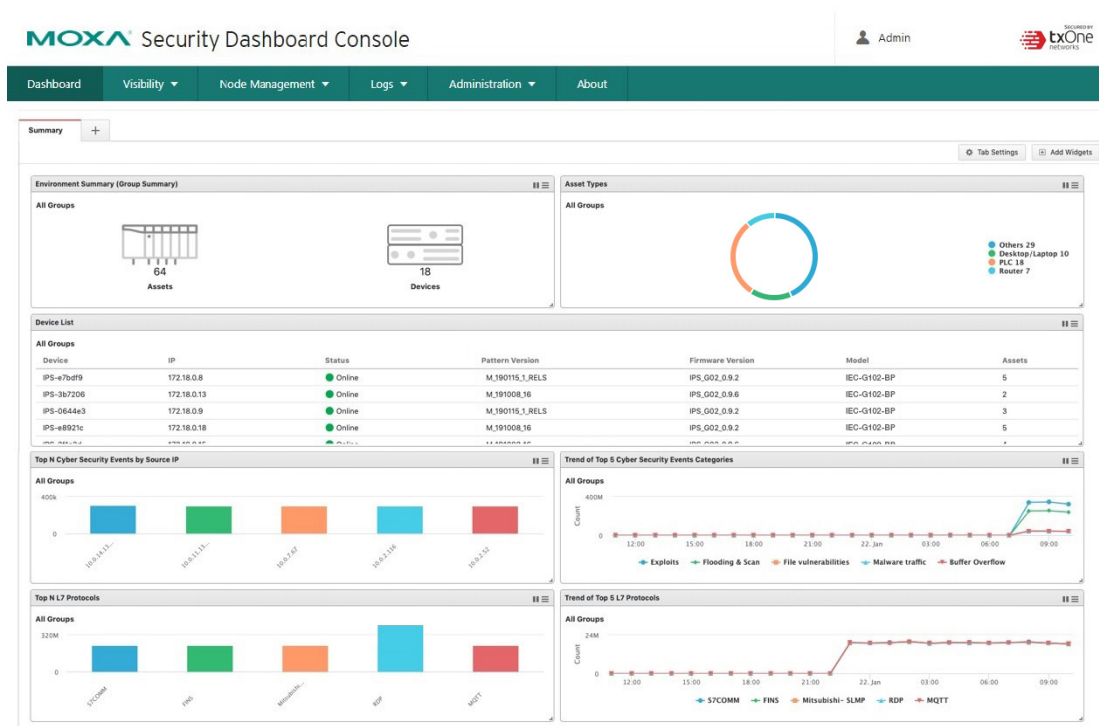
- New Login Name
- New Password
- Retype Password

b. Click **Confirm**.

You will be automatically logged out of the system. The Log On screen will appear again.

c. Log in again using your new credentials.

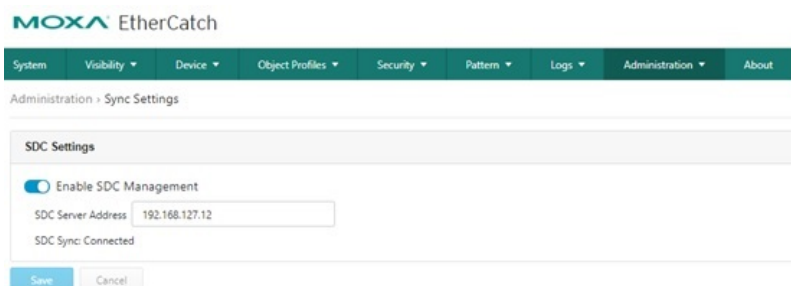
The dashboard screen appears.



Syncing IEC-G102-BP Series Devices to SDC

To manage IEC-G102-BP Series devices through SDC, the device needs to be synced to the SDC.

1. Open a web browser and navigate to the IEC-G102-BP device's web management interface by entering its IP address into the address bar.
2. Navigate to **Administration** → **Sync Settings**.
3. Click the **Enable SDC Management** toggle button.
4. Enter the SDC IP address field in the **SDC Server Address** field.



5. Click **Save**.

Dashboard and Widgets

The following topics are covered in this chapter:

❑ Dashboard Widgets Overview

- Assets Type
- Environment Summary (Group Summary)
- Device List
- Device Status Count
- Node License Usage
- CPU Usage
- Memory Usage
- Disk Usage
- Load Average
- Top N Cyber Security Events by Source IP
- Top N Cyber Security Events by Destination IP
- Top N IPS Attack Events Categories
- Top N Cyber Security Events
- Top N Cyber Security Severity
- Trends of Top N Cyber Security Events Categories
- Trends of Top N Cyber Security Severity
- Top N Cyber Security Events by Device
- Top N Protocol Filter Events by Source IP
- Top N Protocol Filter Events by Destination IP
- Top N L7 Protocols
- Trend of Top 5 L7 Protocols
- Top N L7 Protocol Filter Events by Device
- Top N Policy Enforcement Events by Source IP
- Top N Policy Enforcement Events by Destination IP
- Top N Policy Enforcement Events by Device

❑ Tab and Widget Management

- Adding a Tab to the Dashboard
- Deleting a Tab on the Dashboard
- Adding a Widget to the Dashboard
- Removing a Widget from the Dashboard
- Resizing a Widget
- Pausing and Resuming Widget Refreshing
- Configuring Widget Settings

Monitor your assets, devices, network status, and threat detection on the Summary tab. The Summary tab is automatically added to the Dashboard by default when there are no user-defined tabs. By default, the Summary includes widgets for Environment Summary, Asset Types, Device List, Top N Cyber Security Events by Source IP, Top N L7 Protocols, Trends of Top 5 Cyber Security Events Categories, and Trends of Top 5 L7 Protocols.



NOTE The amount of statistical information shown depends on your user account role and whether permission to manage each particular device group has been shared with you. For more information, see **Sharing Management Permissions to Other User Accounts** and **User Roles**.

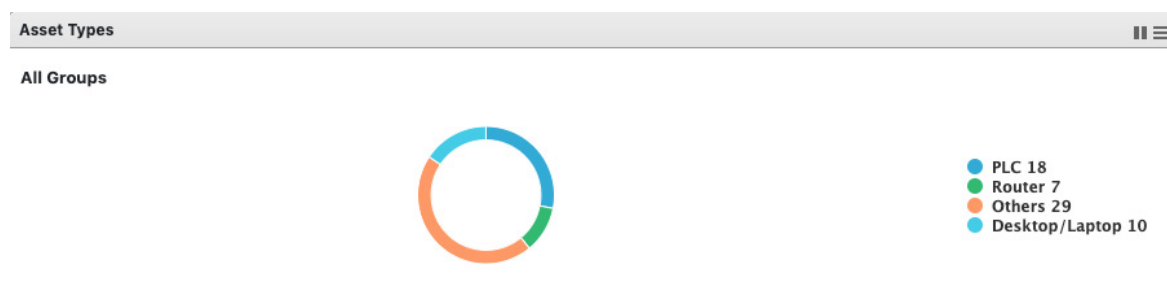
NOTE The six widgets Top N Cyber Security Events by Source IP, Top N Cyber Security Events by Destination IP, Top N Protocol Filter Events by Source IP, Top N Protocol Filter Events by Destination IP, Top N Policy Enforcement Events by Source IP and Top N Policy Enforcement Events by Destination IP may cause a performance issue when the event log has recorded too many events during the last 24 hours. We suggest setting the auto refresh interval to **5 minutes** if these widgets are unable to show the most-recent information.

Dashboard Widgets Overview

This section describes available widgets on the dashboard.

Assets Type

This widget displays the number of assets in the selected device group(s) categorized by type.



Environment Summary (Group Summary)

The Environment Summary widget displays a quick summary of your network environment, including the IEC-G102-BP and IEF-G9010 Series products (Devices) managed by the SDC, the machines protected by these devices (Assets), and the protocol types identified in your network environment.



Item	Description
Assets	Click this item to view a summary of all the machines protected by IEC-G102-BP Series and IEF-G9010 Series devices.
Devices	Click this item to view a summary of all IEC-G102-BP Series and IEF-G9010 Series devices managed by the Security Dashboard Console.

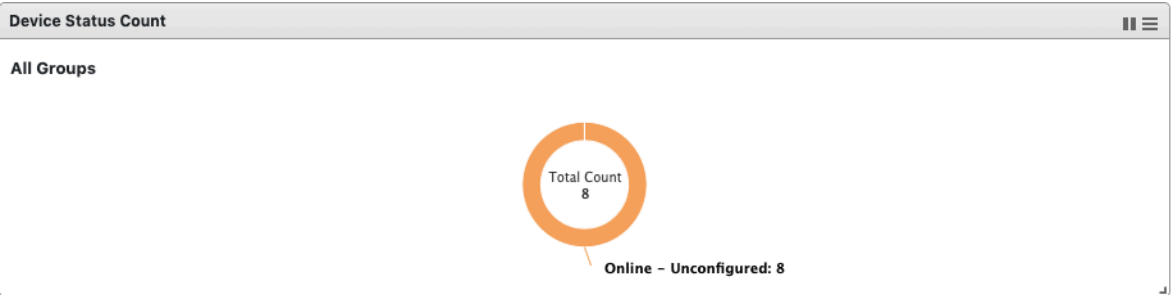
Device List

This widget lists the information for all devices in the selected device group(s), including the device name, IP, and device status.

Item	Description
Device	The name of the device.
IP	The IP address of the device.
Status	The real-time status of the device (online or offline).
Pattern Version	The pattern version of the device.
Firmware Version	The firmware version of the device.
Model	The model name of the device.
Assets	The number of assets that are managed by the device.

Device Status Count

This widget lists the information for all devices in the selected device group(s), including the device model name, host name, IP, status, and so on.

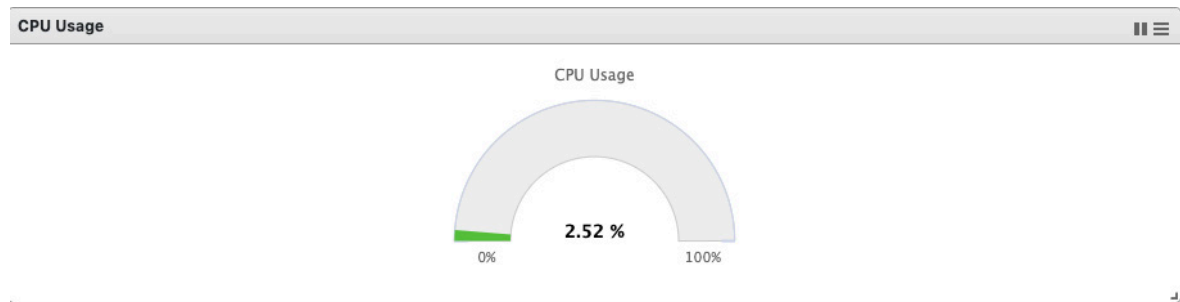


Node License Usage

This widget displays the numbers of registered IEC-G102-BP Series and IEF-G9010 Series devices and the amount of unused node licenses.

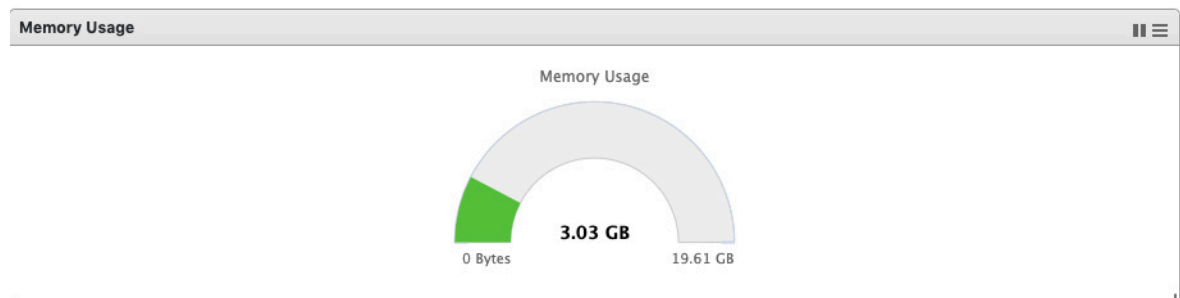
CPU Usage

Shows the CPU usage of the system running the instance of SDC.



Memory Usage

Shows the memory usage of the system running the instance of SDC.



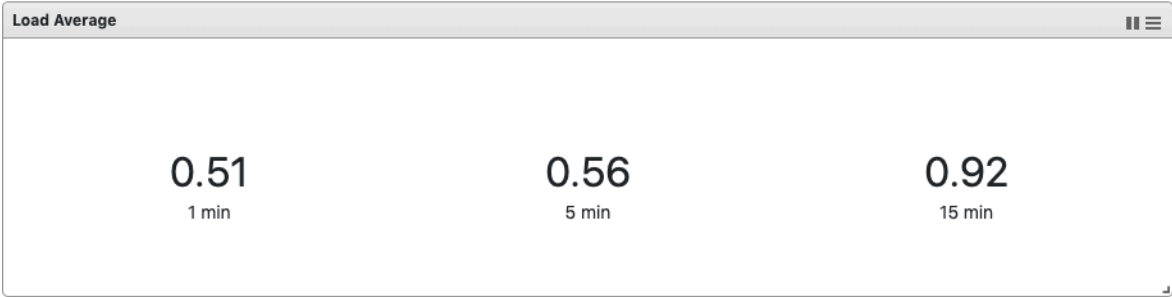
Disk Usage

Shows the currently used disk space on the system running the instance of SDC.



Load Average

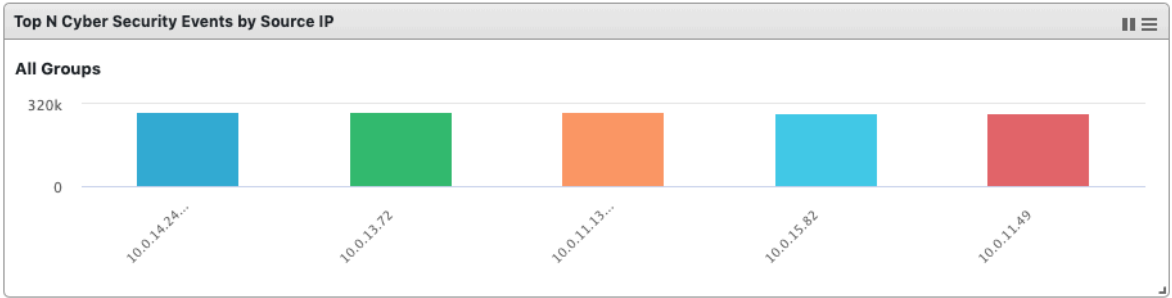
Shows the SDC load average. This refers to the average amount of work the system is doing, based on how many processes are using or are waiting for the CPU, over the course of 1 minute, 5 minutes, and 15 minutes.



Top N Cyber Security Events by Source IP

This widget displays the top N (5 or 10) source IP addresses in the selected device group(s) where the most cyber security events where detected within the last 24 hours.

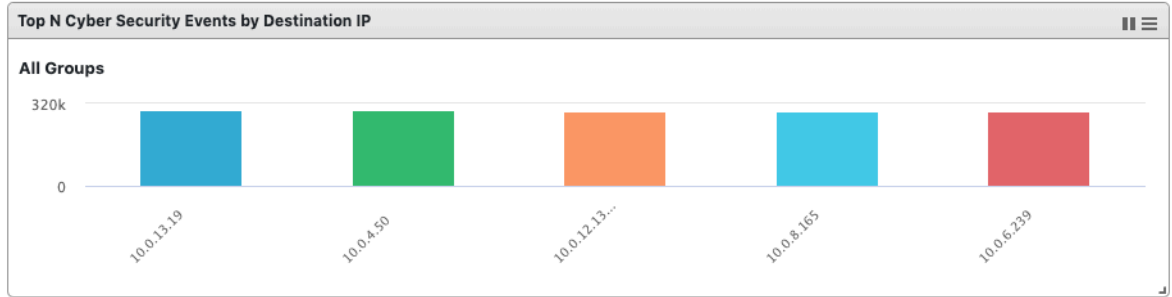
NOTE This widget may cause a performance issue when the event log has recorded too many events during the last 24 hours. We suggest setting the auto refresh interval to **5 minutes** if the widget is unable to show the most-recent information.



Top N Cyber Security Events by Destination IP

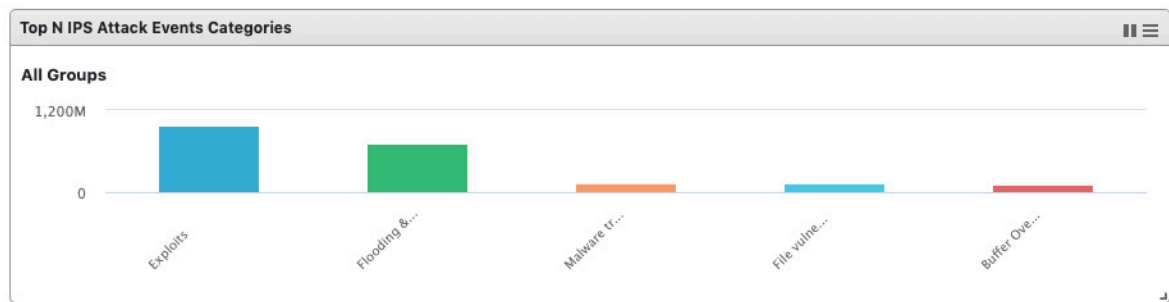
This widget displays the top N (5 or 10) destination IP addresses in the selected device group(s) where the most cyber security events where detected within the last 24 hours.

NOTE This widget may cause a performance issue when the event log has recorded too many events during the last 24 hours. We suggest setting the auto refresh interval to **5 minutes** if the widget is unable to show the most-recent information.



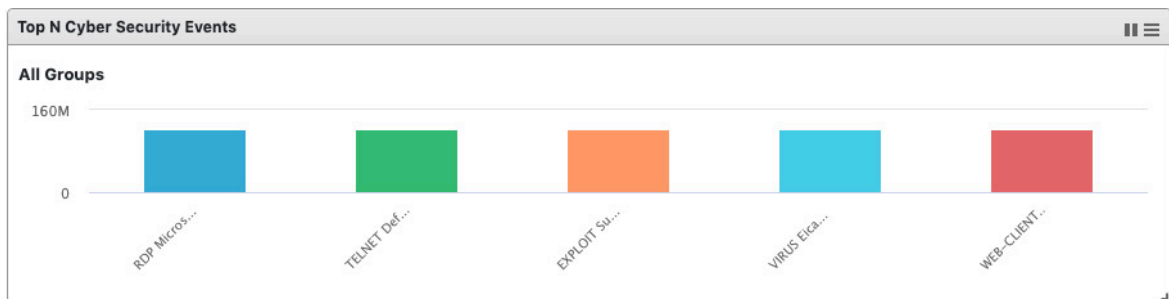
Top N IPS Attack Events Categories

This widget displays the top N (5 or 10) categories of IPS cyber security attacks detected in the selected device group(s) within the last 24 hours.



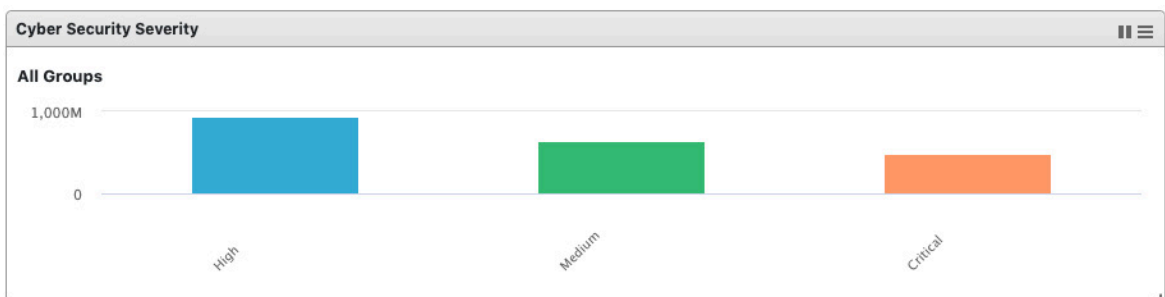
Top N Cyber Security Events

This widget displays the top N (5 or 10) cyber security events found in the selected device group(s), within the last 24 hours.



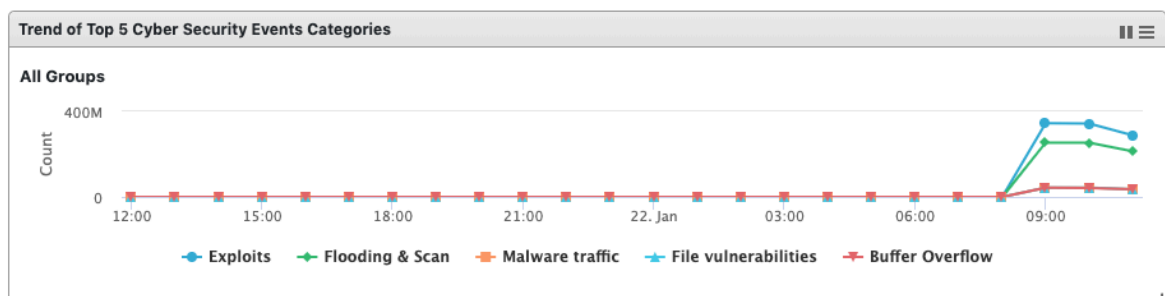
Top N Cyber Security Severity

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



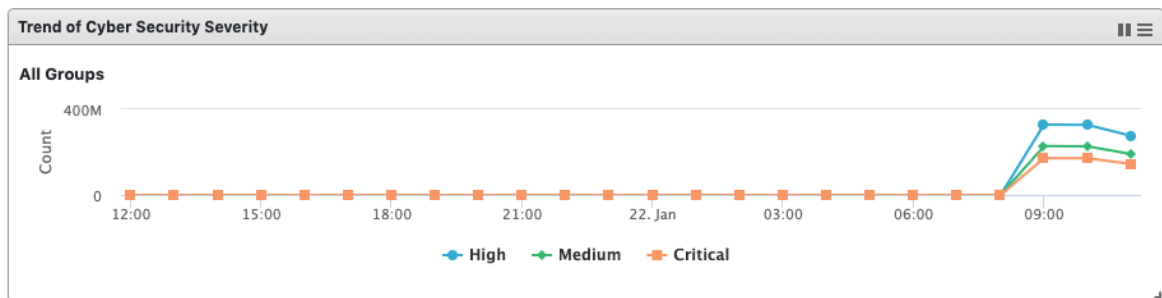
Trends of Top N Cyber Security Events Categories

This widget displays event occurrence trends for the top five cyber security categories in the selected device group(s) within the last 24 hours.



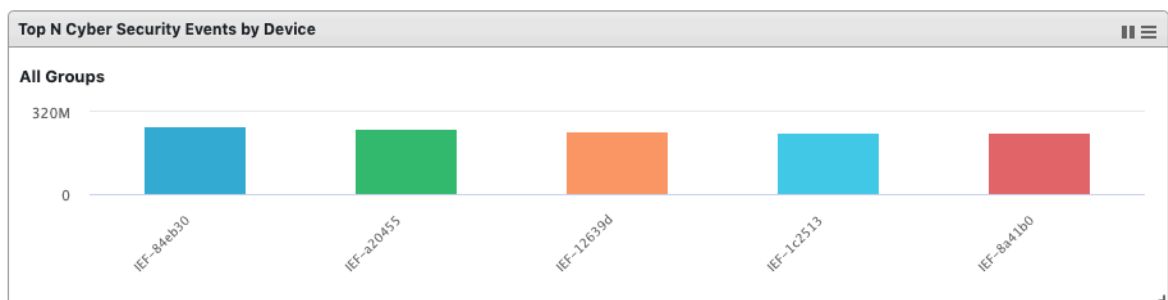
Trends of Top N Cyber Security Severity

This widget displays event occurrence trends in the selected device group(s) in the last 24 hours categorized by severity level.



Top N Cyber Security Events by Device

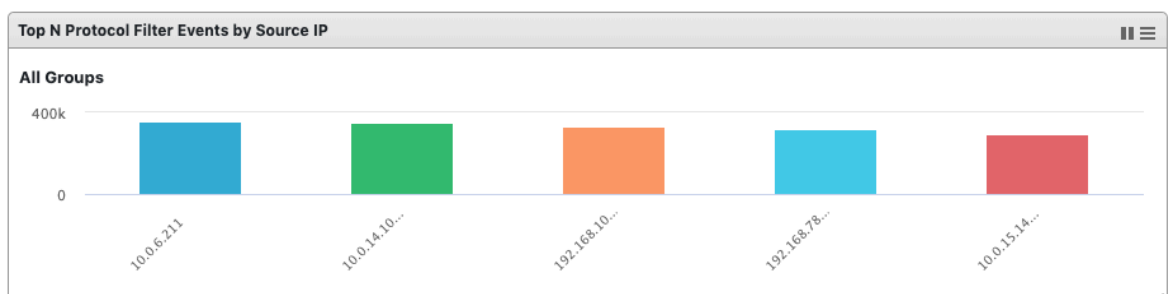
This widget displays the top N (5 or 10) devices in the selected device group(s) that have detected the most cyber security events within the last 24 hours.



Top N Protocol Filter Events by Source IP

This widget displays the top N (5 or 10) source IP addresses in the selected device group(s) that detected the most protocol filter events within the last 24 hours.

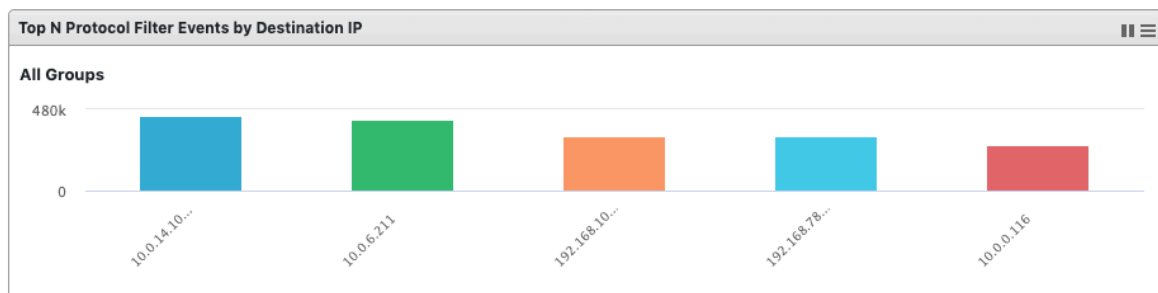
NOTE This widget may cause a performance issue when the event log has recorded too many events during the last 24 hours. We suggest setting the auto refresh interval to **5 minutes** if the widget is unable to show the most-recent information.



Top N Protocol Filter Events by Destination IP

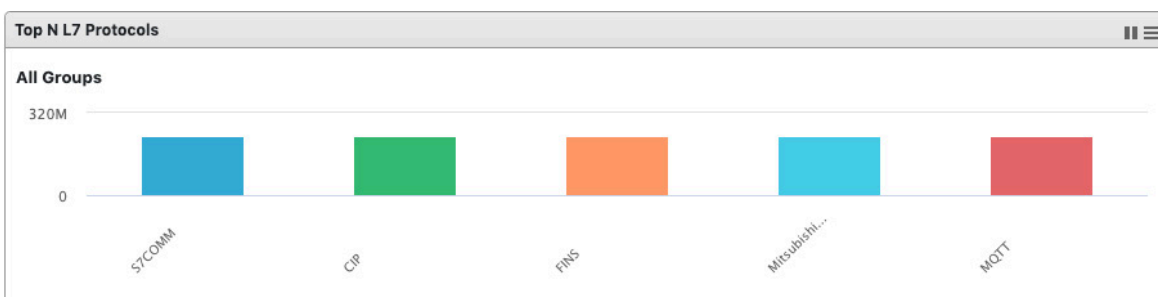
This widget displays the top N (5 or 10) destination IP addresses in the selected device group(s) that detected the most protocol filter events within the last 24 hours.

NOTE This widget may cause a performance issue when the event log has recorded too many events during the last 24 hours. We suggest setting the auto refresh interval to **5 minutes** if the widget is unable to show the most-recent information.



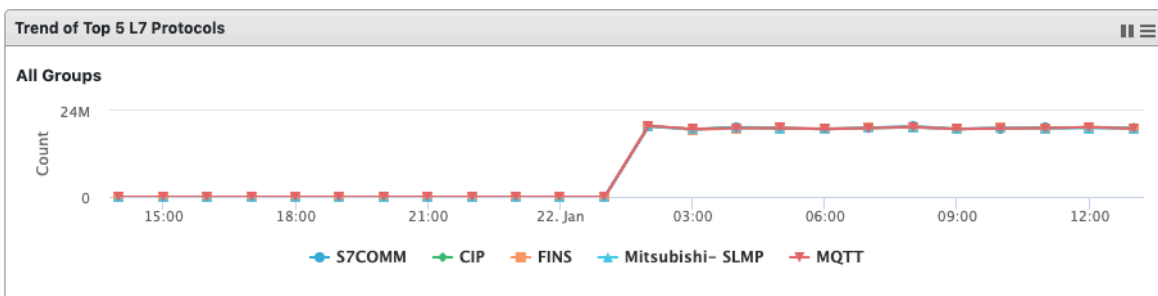
Top N L7 Protocols

This widget displays the top N (5 or 10) L7 protocol names of the protocol filter events detected in the selected device group(s) within the last 24 hours.



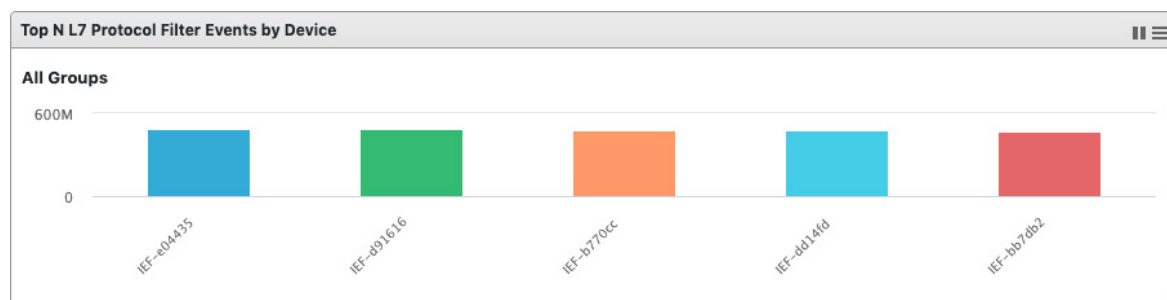
Trend of Top 5 L7 Protocols

This widget displays the event trends of the top five L7 protocol names found in the selected device group(s) within the last 24 hours.



Top N L7 Protocol Filter Events by Device

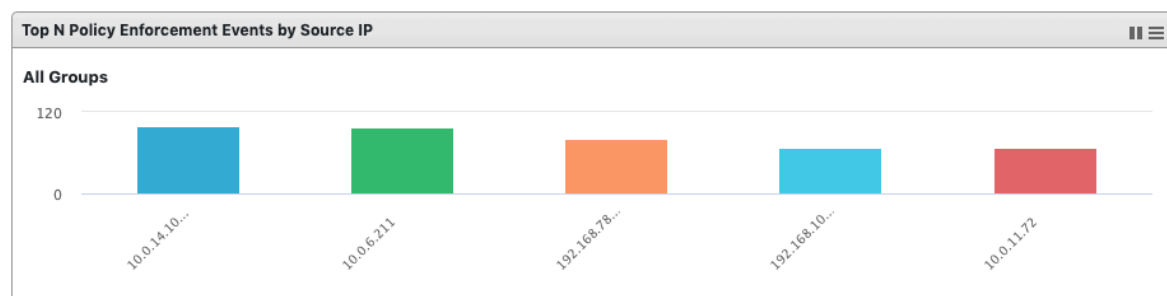
This widget displays the top N (5 or 10) devices in the selected device group(s) that have detected the most protocol filter events within the last 24 hours.



Top N Policy Enforcement Events by Source IP

This widget displays the top N (5 or 10) source IP addresses in the device group(s) that detected the most policy enforcement events within the last 24 hours.

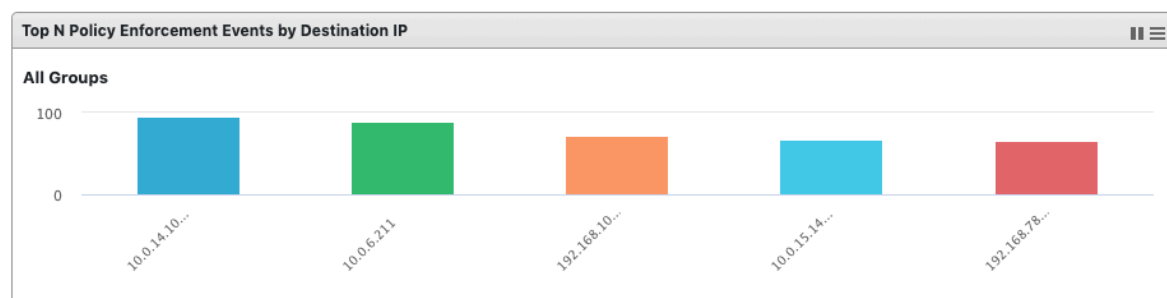
NOTE This widget may cause a performance issue when the event log has recorded too many events during the last 24 hours. We suggest setting the auto refresh interval to **5 minutes** if the widget is unable to show the most-recent information.



Top N Policy Enforcement Events by Destination IP

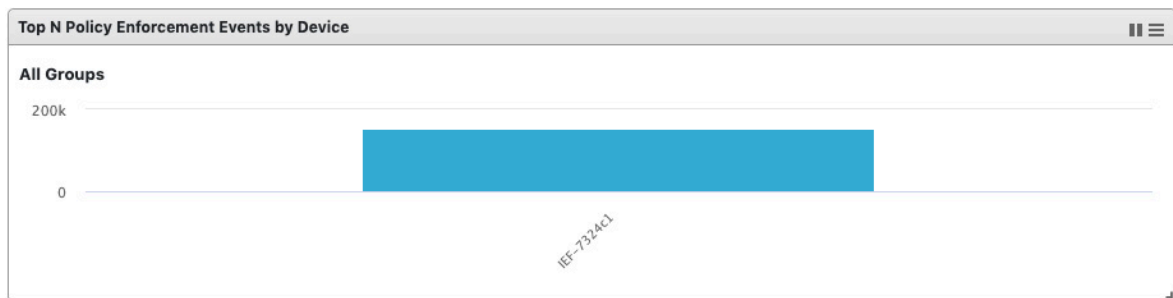
This widget displays the top N (5 or 10) destination IP addresses in the device group(s) that detected the most policy enforcement events within the last 24 hours.

NOTE This widget may cause a performance issue when the event log has recorded too many events during the last 24 hours. We suggest setting the auto refresh interval to **5 minutes** if the widget is unable to show the most-recent information.



Top N Policy Enforcement Events by Device

This widget displays the top N (5 or 10) devices in the selected device group(s) that detected the most policy enforcement events within the last 24 hours.



Tab and Widget Management

This section describes how to manage the tabs and widgets on the SDC Dashboard.

Adding a Tab to the Dashboard

1. Click the **Add Tab** () icon.



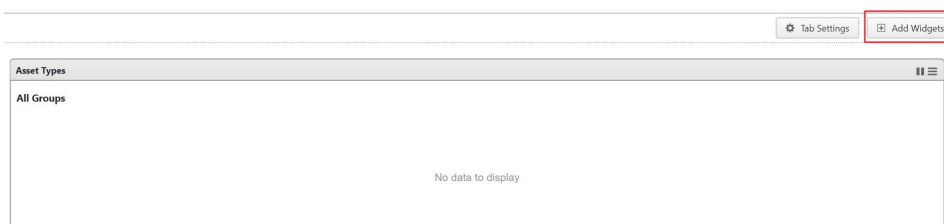
2. Enter a name for the new tab.
3. Click **Ok**.

Deleting a Tab on the Dashboard

1. Hover the mouse cursor over the name of the tab to delete.
The **Delete** (X) icon will appear.
2. Click the **X** to delete the tab.

Adding a Widget to the Dashboard

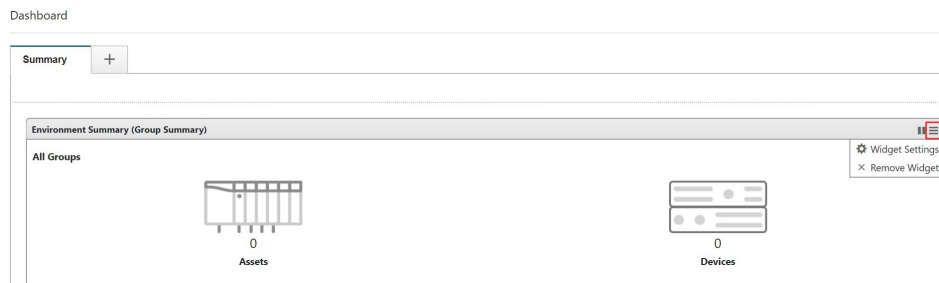
1. Click **Add Widgets**.



2. Check the checkbox next to the widget(s) you want to add. You can browse different categories of widgets by clicking the different category names. A total of 10 widgets can be added to a tab.
3. Click **Add** to add the selected widget(s) to the tab

Removing a Widget from the Dashboard

1. Hover the mouse cursor over the **Menu** (☰) icon in the top-right corner of the widget.



2. Click **Remove Widget**.
3. Click **Ok** to confirm.

Resizing a Widget

1. Hover the mouse cursor over the **Resize** (↘) icon in the bottom-right corner of the widget.
2. Click and drag the corner of the widget to the desired size, then release the mouse.

Pausing and Resuming Widget Refreshing

1. To pause automatic widget refreshing, click the **Pause** (⏸) button in the widget title bar.
2. To resume automatic widget refreshing, click the **Resume** (▶) button in the widget title bar.

Configuring Widget Settings

1. Hover the mouse cursor over the **Menu** (☰) icon in the top-right corner of the widget
2. Click **Widget Settings**.

The widget settings popup window appears

3. Configure the widget settings. Refer to table below for a description of each setting.

Setting	Description
Widget Name	Edit the widget name. The widget name will display on the title bar of the widget in the Dashboard.
Auto Refresh Settings	Select the automatic widget refresh interval from the drop-down menu. This interval determines when the information in the widget is renewed. Select Manual Refresh if you don't want the widget to refresh automatically.
Top Statistics (For selected widgets only)	Select the amount of items for top statistics (top 5 or top 10) from the drop-down menu.
Chart Type (For selected widgets only)	Click on the different chart icons to select the chart type such as a bar or pie chart, shown on the widget.

Device Type (For selected widgets only)	Click on the device type, (IEC-G102-BP, IEF-G9010) to see the corresponding group list. Select the group by clicking the group name in the Groups panel. Deselect the group by clicking the group name in the Selected Groups panel.
--	---

4. Click **OK** to save your settings.

The Visibility Tab

The **Visibility** tab gives you an overview of all your managed assets. This tab provides you with accurate real-time information about the assets that are managed by IEC-G102-BP Series industrial IPS and IEF-G9010 Series next-general firewall devices.

The IEC and IEF devices register all traffic passing through it and automatically identify the connected devices and machines (assets) that are sending and receiving data. These assets will appear on the Visibility tab.

NOTE	The term asset in this chapter refers to the devices or hosts that are protected by the IEC-G102-BP Series industrial IPS and IEF-G9010 Series next-generation firewall.
-------------	---















NOTE	The statistical information shown depends on your user account role and whether permission to manage the device groups has been shared with you. For more information, see <i>Sharing Management Permissions to Other User Accounts</i> and <i>User Roles</i> .
-------------	---

The following topics are covered in this chapter:

- ❑ **Common Tasks**
- ❑ **Displaying Asset Information**
- ❑ **Basic Asset Information**
- ❑ **Real-time Network Application Traffic**

Common Tasks

The following table lists the common tasks that can be performed from the Visibility tab.



Task	Action																																			
To search for an asset	Select the search criteria, enter the keyword, and click the Search () button. <div><div>Group Name ▾</div><div>Search<div></div></div></div>																																			
To list devices/assets as icons	Click the Grid View () button to view all devices as icons. <div><div><div><div>Device 1 Industrial Controller 192.168.182.95 54:4b:14:d7:df:f8</div></div><div><div>Device 2 Industrial Network ... 192.168.182.96 54:4b:14:d7:df:f9</div></div><div><div>Device 3 Industrial Drives & ... 192.168.182.97 54:4b:14:d7:df:f0</div></div><div><div>Device 4 Industrial Producti... 192.168.182.98 54:4b:14:d7:df:f1</div></div><div><div>Device 5 Industrial Embedd... 192.168.182.99 54:4b:14:d7:df:f2</div></div><div><div>Device 6 Industrial assets 192.168.182.100 54:4b:14:d7:df:f3</div></div></div><div><div><div>Device 7 SCADA 192.168.182.101 54:4b:14:d7:df:f4</div></div><div><div>Device 8 HMI 192.168.182.102 54:4b:14:d7:df:f5</div></div><div><div>Device 9 Industrial Workstat... 192.168.182.103 54:4b:14:d7:df:f6</div></div><div><div>Device 10 PLC 192.168.182.104 54:4b:14:d7:df:f7</div></div></div></div>																																			
To list devices in a table list	Click the Table View () button to view all devices in a table format. <table><tr><th><input type="checkbox"/></th><th>Host Name</th><th>Asset Type</th><th>IP Address</th><th>MAC Address</th></tr><tr><td><input type="checkbox"/></td><td>Device 1</td><td>Industrial Controller</td><td>192.168.182.95</td><td>54:4b:14:d7:df:f8</td></tr><tr><td><input type="checkbox"/></td><td>Device 2</td><td>Industrial Network appliance</td><td>192.168.182.96</td><td>54:4b:14:d7:df:f9</td></tr><tr><td><input type="checkbox"/></td><td>Device 3</td><td>Industrial Drives & I/O Device</td><td>192.168.182.97</td><td>54:4b:14:d7:df:f0</td></tr><tr><td><input type="checkbox"/></td><td>Device 4</td><td>Industrial Production Machines</td><td>192.168.182.98</td><td>54:4b:14:d7:df:f1</td></tr><tr><td><input type="checkbox"/></td><td>Device 5</td><td>Industrial Embedded PC</td><td>192.168.182.99</td><td>54:4b:14:d7:df:f2</td></tr><tr><td><input type="checkbox"/></td><td>Device 6</td><td>Industrial assets</td><td>192.168.182.100</td><td>54:4b:14:d7:df:f3</td></tr></table>	<input type="checkbox"/>	Host Name	Asset Type	IP Address	MAC Address	<input type="checkbox"/>	Device 1	Industrial Controller	192.168.182.95	54:4b:14:d7:df:f8	<input type="checkbox"/>	Device 2	Industrial Network appliance	192.168.182.96	54:4b:14:d7:df:f9	<input type="checkbox"/>	Device 3	Industrial Drives & I/O Device	192.168.182.97	54:4b:14:d7:df:f0	<input type="checkbox"/>	Device 4	Industrial Production Machines	192.168.182.98	54:4b:14:d7:df:f1	<input type="checkbox"/>	Device 5	Industrial Embedded PC	192.168.182.99	54:4b:14:d7:df:f2	<input type="checkbox"/>	Device 6	Industrial assets	192.168.182.100	54:4b:14:d7:df:f3
<input type="checkbox"/>	Host Name	Asset Type	IP Address	MAC Address																																
<input type="checkbox"/>	Device 1	Industrial Controller	192.168.182.95	54:4b:14:d7:df:f8																																
<input type="checkbox"/>	Device 2	Industrial Network appliance	192.168.182.96	54:4b:14:d7:df:f9																																
<input type="checkbox"/>	Device 3	Industrial Drives & I/O Device	192.168.182.97	54:4b:14:d7:df:f0																																
<input type="checkbox"/>	Device 4	Industrial Production Machines	192.168.182.98	54:4b:14:d7:df:f1																																
<input type="checkbox"/>	Device 5	Industrial Embedded PC	192.168.182.99	54:4b:14:d7:df:f2																																
<input type="checkbox"/>	Device 6	Industrial assets	192.168.182.100	54:4b:14:d7:df:f3																																
To collapse the device group column	Click the X button next to the Device Group column name.																																			

Displaying Asset Information

From the Asset Information window, you can view basic and network information for the selected device.

Basic Asset Information

The **Assets Information** panel shows basic information for the asset.

1. Navigate to **Visibility** → **Assets View**.
2. Click the **Information** () button to display asset information
3. In the device information window, click the **Basic Information** () button.

 PLC Example Nr 11

Vendor Name

Rockwell-b

Model Name

LOGIX5058

Asset Type

PLC

Host Name

PLC Example Nr 11

Serial Number

SN 1234.251555

OS

FreeBSD 6.3

MAC Address

14:0f:b1:d1:c8:d2

Field	Description	Example
Vendor Name	The name of asset vendor.	Rockwell Automation/ Allen-Bradley
Model Name	The model name of the asset.	1756-L61/B LOGIX5561
Asset Type	The type of asset.	Industrial Controller
Host Name	The name of the asset.	Rockwell
Serial Number	The serial number of the asset.	7079450
OS	The system OS used by the asset	Linux 2.6
MAC Address	The MAC address of the asset.	00:0c:29:da:14:1c
IP Address	The IP address of the asset.	10.24.254.94
First Seen	The date and time the asset was first seen on the network.	2020-01-22T11:26:39+08:00
Last Seen	The date and time the asset was last seen on the network.	2020-01-22T11:44:28+08:00

NOTE The IEC-G102-BP and IEF-G9010 Series will attempt to automatically collect the above information from connected assets and transfer that information to the Security Dashboard Console.


Real-time Network Application Traffic


The **Real Time Network Application Traffic** panel shows a list of network traffic statistics for the asset.



1.

Navigate to **Visibility** → **Assets View**.
2.

Click the **Information** (ⓘ) button to display asset information
3.

In the device information window, click the **Network Information** () button.

 **PLC Example Nr 11** ✕



Refresh Time

10 Sec ▾

No	Application Name	TX	RX
1	Modbus	2.11 TB	1.90 TB
2	Mitsubishi-SLMP	2.04 TB	2.09 TB
3	DouyuTV	2.27 TB	2.10 TB

Field	Description
Refresh Time	The interval at which the traffic information is renewed.
No.	The ordinal number of the application.
Application Name	The application type.
TX	The amount of data transmitted by this application.
RX	The amount of data received for this application.

NOTE Click **Manual asset info refresh** to manually refresh the information displayed.

Node Management

The **Node Management** window lets you manage the IEC-G102-BP Series devices that have been registered to your Security Dashboard Console. The **Node Management** tab features two levels of operations: device-level and group-level. You can manage each node individually or arrange them in groups to share the same configuration. All nodes are placed in the **Ungroup** group by default.

The following types of nodes can be managed by the Security Dashboard Console:

- IEC-G102-BP Series industrial IPS

NOTE The term **node** here refers to devices that have been registered to the Security Dashboard Console.

NOTE The maximum number of managed nodes is dependent on the resources allocated to the SDC. See the **System Requirements** section for more details.

NOTE The information shown depends on your user account role and whether the permission to manage the device groups has been shared with you. For more information, see **Sharing Management Permissions to Other User Accounts** and **User Roles**.

The following topics are covered in this chapter:

❑ **Common Tasks**

❑ **Group Management**


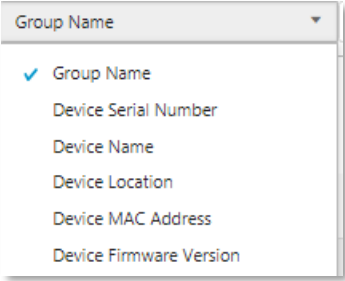




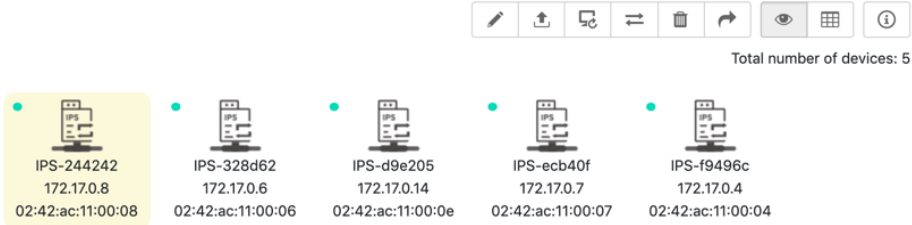




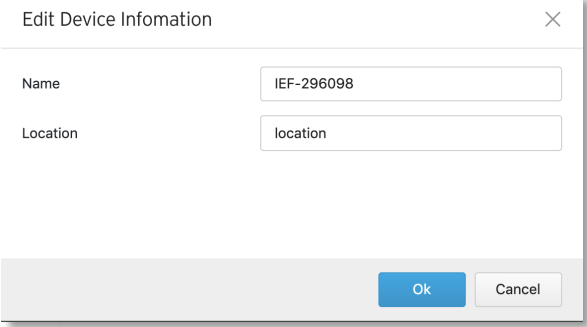
- Creating a New Device Group
- Renaming or Deleting a Device Group
- Moving a Node into a Group

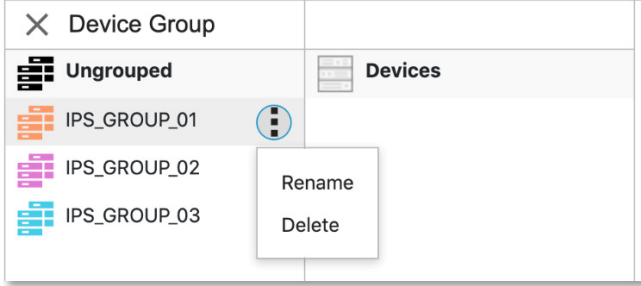
❑ **Managing IEC-G102-BP Series Devices**

- Accessing the Management Tab
- Updating the Firmware
- Switching Firmware
- Editing the Name or Location of a Node
- Rebooting a Node
- Configuring Security Operation Mode
- Configuring Cyber Security
- Configuring Policy Enforcement
- Configuring Pattern Setting
- Sharing Management Permissions to Other User Accounts

Common Tasks

The following table lists the common tasks that can be performed from the Node Management tab.

Task	Action
To search for a device	<p>Select the search criteria, enter the keyword, and click the Search () button.</p> 
To add a new device group	Click the Add () button to add a new device group.
To view ungrouped devices	Click Ungrouped in the Device Group column.
To list devices as icons	Click the Grid View () button to view all nodes as icons.
To list devices in a table list	Click the Table View () button to view all nodes in a table format.
To show the detailed information of a device	Click the Information () button.
To delete/move/reboot a device when in grid view	<p>Select one or more nodes and click the corresponding action button in the top-right.</p>  <p>Delete (): Remove the selected device(s) from the group.</p> <p>Move (): Move the selected device(s) to another group.</p> <p>Reboot (): Reboot the selected device(s).</p>
To edit a device when in table view	<p>Select the device in the table and click the Edit () button in the top-right corner.</p> 

Task	Action
To rename/delete a group	<p>Hover the mouse cursor over the group name, click the Menu (⋮) button of the group, and select the desired action.</p> 

Group Management

To easily manage a large number of devices using SDC, 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 security policy configurations that can be shared are:

- Security operation mode
- Cyber security policies
- Policy enforcement
- Pattern settings

NOTE Security operation mode is only supported by the IEC-G102-BP Series.

Creating a New Device Group


1. Navigate to **Node Management** → **EtherCatch** or **EtherFire**.
2. Under the **Device Group** panel, click the (+) icon.
3. Provide a name for the group.
The group name can be up to 32 characters long and supports a-z, A-Z, 0-9, periods (.), underscore (_), and hyphens (-).
4. Click **Confirm**.

Renaming or Deleting a Device Group

1. Hover the mouse cursor over the group icon and click the **Menu** (⋮) button for the group.
2. Select the desired action.






Moving a Node into a Group

You can easily move devices between different groups. When moving a device, the settings of the new group will be automatically be applied to the moved device(s).

1. Select one or more nodes, click the **Move** () button in the function area located at the top-right
2. Click **Move**.
3. Select the group the node will be moved to.



Total number of devices: 5

 IPS-244242 172.17.0.8 02:42:ac:11:00:08	 IPS-328d62 172.17.0.6 02:42:ac:11:00:06	 IPS-d9e205 172.17.0.14 02:42:ac:11:00:0e	 IPS-ecb40f 172.17.0.7 02:42:ac:11:00:07	 IPS-f9496c 172.17.0.4 02:42:ac:11:00:04
--	--	---	--	--

Managing IEC-G102-BP Series Devices


This section describes how to manage the IEC-G102-BP Series devices that have been registered to the Security Dashboard Console.

Accessing the Management Tab

1. Navigate to **Node Management** → **EtherCatch** or **EtherFire**.
2. Click a node icon to view the details of this node.

Updating the Firmware

Procedure when in Table View

1. Click on one or more nodes.
2. Click the **Upgrade** () button.
3. Select the target firmware version number from the drop-down menu, then click **Confirm**.

Upgrade Firmware

Device List

Name	Running Firmware Version
IPS-244242	IPS_0.9.1

Select the firmware version

3.3.0


The upgraded firmware will be installed on the standby partition, and you can then switch partitions, so the device starts running on the newer firmware version.

Confirm

Cancel


Procedure when in Grid View

1. Click on one or more nodes.


2. Click the **Upgrade** () button.
3. Select the target firmware version number from the drop-down menu, then click **Confirm**.

Switching Firmware

When a new firmware is uploaded to the node, it will be automatically stored on the standby disk partition of the node. You can use the Switch Firmware function to switch between the active and standby disk partition to boot the node with. If the node does not support a standby disk partition, the newly uploaded firmware will be automatically installed over the existing firmware and become the running firmware version.

1. Click on one or more nodes.
2. Click the **Switch Firmware** () button.

Editing the Name or Location of a Node

1. Click the node and click the **Edit** () button.
2. Provide name or location information for the node.
3. Click **Ok**.

Rebooting a Node

1. Select one or more nodes.
2. Click the **Reboot** () button.
3. A confirmation window will appear. Click **Confirm** to reboot the selected node(s).

Configuring Security Operation Mode

IEC-G102-BP Series offers two operation modes:

Inline Mode


IEC-G102-BP sits in the direct communication path between the source and destination, actively analyzing, filtering, and taking actions on all traffic that passes through it.

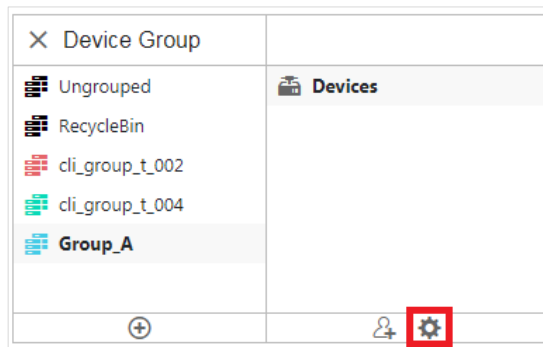
Offline Mode

Data packets are mirrored from a switch to **port 2** of the IEC-G102-BP, which keeps detecting and monitoring, as well as outputting detection logs if threat events are detected, but does not take actions.

NOTE **Port 1** of the IEC-G102-BP functions as the management port, which connects to another switch, allowing the IEC-G102-BP to be managed by SDC.

Enabling Security General Setting

1. Click the device group you want to manage.
2. Click the **Edit Settings** () button.



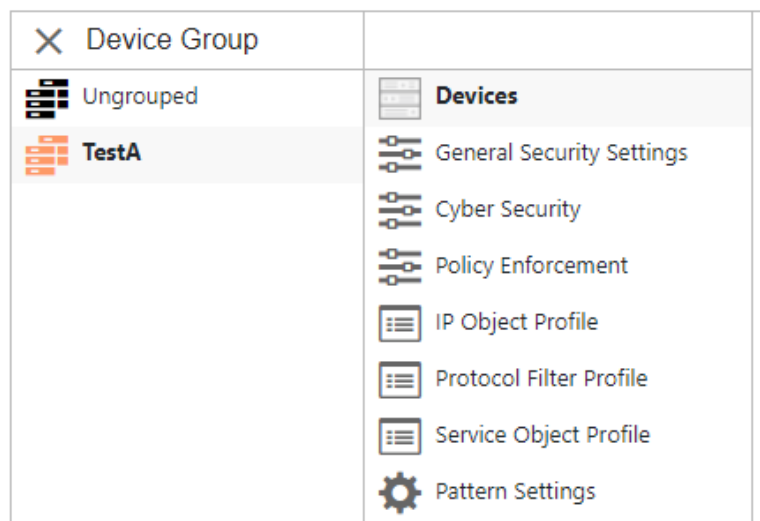
The **Edit Settings** screen appears.

3. Toggle the **Security General Settings** slider to enable the feature and click **Continue**.



Configuring Security Operation Mode

1. Click the group name in the **Device Group** column.
2. Click **Security General Settings**.



The **Security Operation Mode Selection** screen appears.

3. Choose the desired operation mode for this device group.

Security Operation Mode Selection

☒ Inline Mode
☐ Offline Mode

Security Operation Mode Definition


- Inline Mode:** In the direct communication path between source and destination, actively analyzing, filtering and automated actions on all traffic flows that enter the network.
- Offline Mode:** Data packets are mirrored from core switch and EtherGuard keeps detecting, monitoring as well as output detected log if detect threat event.

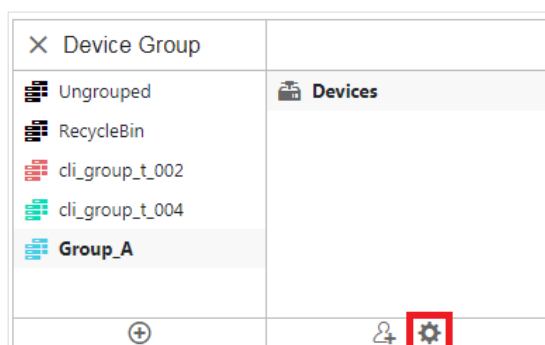
- Click **Save** to apply the settings.

Configuring Cyber Security

IEC-G102-BP series feature cyber security, which covers both intrusion prevention and denial of service attack prevention. The signature rules of intrusion prevention are provided by Moxa and can be regularly updated through SDC.

Enabling Cyber Security

- Click the device group you want to manage.
- Click the **Edit Settings** () button.



The **Edit Settings** screen appears.

- Toggle the **Cyber Security** slider to enable the feature and click **Continue**.

Edit Settings

Security General Setting
☒

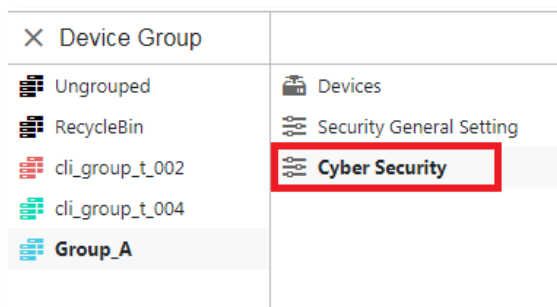
Cyber Security
☒

Policy Enforcement
☐

Pattern Setting
☐

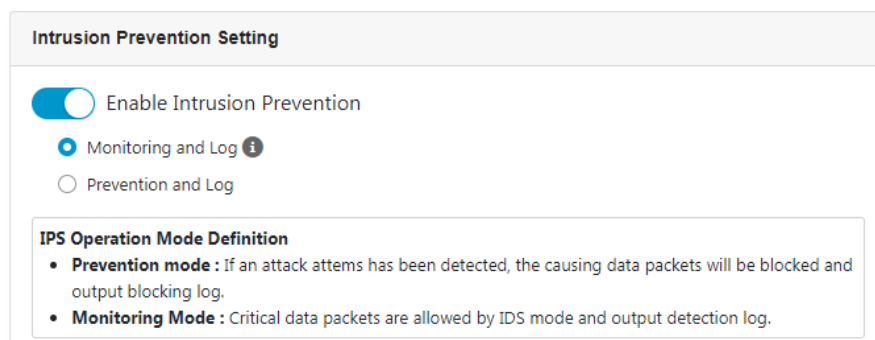
Configuring Intrusion Prevention Settings

- Click the group name in the **Device Group** column.
- Click **Cyber Security**.



The **Cyber Security** screen appears.

3. Toggle the slider to enable or disable the intrusion prevention feature.



4. If enabled, select a prevention mode:

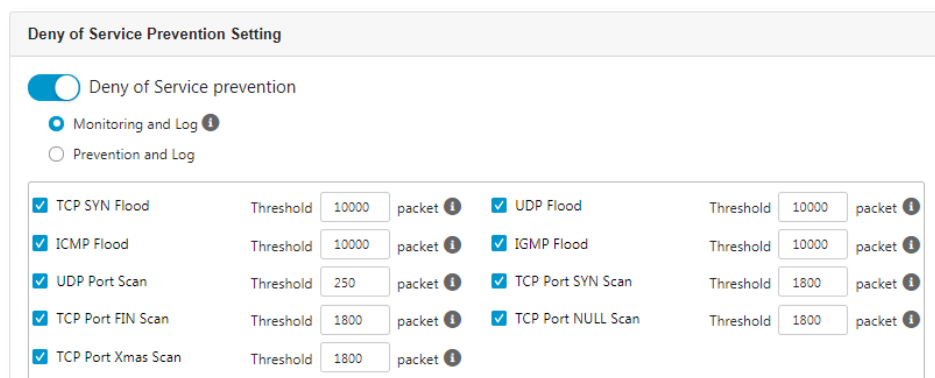
Monitor and Log: IDS allows critical packets and records a detection log.

Prevent and Log: Blocks suspicious packets and records a blocking log.

5. Click **Save** to apply your settings.

Configuring Denial of Service Prevention Settings

1. Click the group name in the **Device Group** column.
2. Click **Cyber Security**.
3. Toggle the slider to enable or disable the denial of service protection feature.



The **Deny of Service Prevention Setting** screen appears.

4. If enabled, select a response action when an intrusion is detected:

Monitor and Log: Detects but allows network attacks and records a detection log.

Prevent and Log: Blocks suspicious packets and records a blocking log. (available in **Offline mode** only)

5. **(Optional)** Enable and configure the packet thresholds of the denial of service rules.
6. Click **Save** to apply your settings.

NOTE Flood/Scan Attack Protection rules use detection period and threshold mechanisms to detect attacks. During a detection period (typically every 5 seconds), if the number of anomalous packets reaches the specified threshold, an attack detection occurs. If the rule action is set to Block, the security node blocks subsequent anomalous packets until the end of the detection period. When the detection period ends, the security node continues to allow anomalous packets to pass through until the threshold is reached again.

The following table summarizes the Inline and Offline mode behaviors:

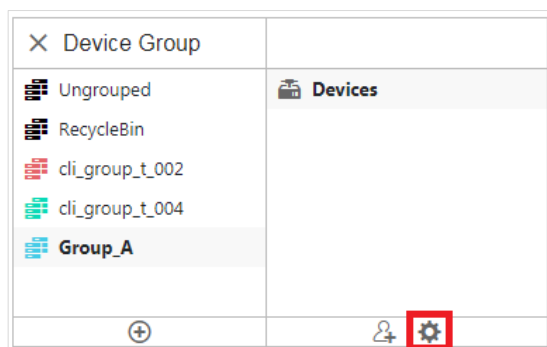
Mode (Security General Setting)	Action Settings	Actions Performed
Inline Mode	Monitor and Log	<ul style="list-style-type: none">• Detects and monitors network attacks, but does not block network attacks.• Generates detection logs.
	Prevent and Log	<ul style="list-style-type: none">• Detects and blocks network attacks.• Generates detection logs.
Offline Mode	Monitor and Log	<ul style="list-style-type: none">• Passively detects and monitors network attacks.• Generates detection logs.

Configuring Policy Enforcement

Policy enforcement allows you to define a custom protocol that matches to an industrial or IT protocol, and then white-list or black-list protocols in your network environment.

Enabling Policy Enforcement

1. Click the device group you want to manage.
2. Click the **Edit Settings** (⚙️) button.



The **Edit Settings** screen will appear.

3. Toggle the **Policy Enforcement** slider to enable the feature and click **Continue**.



4. Click **Save** to apply your settings.

Configuring Policy Enforcement

From the **Policy Enforcement** window, you can configure policy rules to determine how nodes should handle traffic based on the configured parameters. For more granular control, you can use preconfigured profiles for IP Objects, Service Objects, and Protocol Filters to use in policy rules. These profiles must be created separately.

- IP object profiles - for more information, see **Configuring IP Object Profile**.
- Service object profiles - for more information, see **Configuring Service Object Profiles**.
- Protocol filter profiles - for more information, see **Configuring Protocol Filter Profile**.

1. Click the device group you want to manage.
2. Click **Policy Enforcement**.
3. Use the toggle to enable or disable the policy enforcement feature.

Policy Enforcement General Setting

☐ Enable Policy Enforcement

☒ Monitor Mode ⓘ

☐ Prevention Mode

Policy Enforcement Default Rule Action Deny ⓘ

Policy Enforcement Operation Mode

- **Monitoring Mode:** Policy Enforcement rule will be checking without taking action and output detection log
- **Prevention Mode:** Policy Enforcement rule will be checking, any Rule hit and will be taking action and output deny log

6. If enabled, select a prevention mode:

Monitor and Log: The policy enforcement rule will perform checks and records a detection log, but will not take action.

Prevent and Log: The policy enforcement rule will perform checks and will take action when a rule is violated in addition to recording a detection log.

4. From the **Policy Enforcement Default Rule Action** drop-down menu, select a default action for when a policy rule is violated.

The following table summarizes Inline and Offline mode behavior:

Mode (Security General Setting)	Mode (Policy Enforcement)	Action Performed
Inline Mode	Monitor Mode	<ul style="list-style-type: none"> • Detects and monitors packets that violate a policy, but does not take actions. • Generates detection logs.
	Prevention Mode	<ul style="list-style-type: none"> • Take action when a policy is violated. • Generates detection logs.
Offline Mode	Monitor and Log	<ul style="list-style-type: none"> • Not supported.

Adding Policy Enforcement Rules

1. Click the device group you want to manage.
2. Click **Policy Enforcement**.
3. Click **Add** to add a new policy rule.

The **Create Policy Rule** window appears.

Create Policy Rule

☒ Enable Policy Rule

Name* ⓘ

Description ⓘ

Source and Destination Selection

Source IP / IP Object Profile* Any ▼

Destination IP / IP Object Profile* Any ▼

Service Object Selection

Service Object* Any ▼

Action Deny ▼

4. Use the toggle to enable or disable the policy rule.
5. Enter a name for the rule.
6. Enter a description for the rule.
7. From the **Source IP / IP Object Profile** drop-down menu, select one of the following for the source IP address(es):
 - **Any**: Any IP address will qualify.
 - **Single IP**: The rule applies to a designated IP address.
 - **IP Range**: The rule applies to a set range of IP addresses.
 - **IP Subnet**: The rule will apply to all IP addresses within a specific subnet.
 - **Object**: The rule will apply to a previously created IP Object Profile.

NOTE If you select **Object**, you need to select the IP object from the IP object profiles that have been created previously.

8. From the **Destination IP / IP Object Profile** drop-down menu, select one of the following for the destination IP address(es):
 - **Any**: IP address will qualify.
 - **Single IP**: The rule applies to a designated IP address.
 - **IP Range**: The rule applies to a set range of IP addresses.
 - **IP Subnet**: The rule will apply to all IP addresses within a specific subnet.
 - **Object**: The rule will apply to a previously created IP Object Profile.
9. From the **Service Object** drop-down menu, select one of the following for the Layer 4 criteria:
 - **Any**
 - **TCP**: Specify the port range for this protocol.
 - **UDP**: Specify the port range for this protocol.
 - **ICMP**: Specify the protocol number, the ICMP type, and code.
 - **Custom**: Specify the protocol number for this protocol. The term protocol number refers to the one defined in the internet protocol suite.
 - **Service Object**

NOTE You need to select the service object from service object profiles that have been created previously.

10. From the **Action** drop-down menu, select one of the following default actions:
 - a. **Accept**: Select this option to allow network traffic that matches this rule.
 - b. **Deny**: Select this option to block network traffic that matches this rule.
 - c. **Protocol Filter**: The node will take action based on the selected protocol filter.
 - From the **Protocol Filter Profile** drop-down menu, select a previously created protocol filter profile.
 - From the **Protocol Filter Action** drop-down menu, select whether to allow or deny network traffic that matches the protocol filter.
11. Click **Save** to save the configuration.

Managing Policy Enforcement Rules

The following table lists the common tasks that are used manage the policy enforcement rules.

Task	Action
To delete a policy enforcement rule	Check the check box in front of the policy enforcement rule you want to delete and click the Delete button.


To duplicate a policy enforcement rule	Check the check box in front of the policy enforcement rule you want to duplicate and click the Copy button.
To edit a policy enforcement rule	Click the name of the rule you want to edit. The Edit Policy Rule window will appear.
To change the priority of a policy enforcement rule	Check the check box in front of the policy enforcement rule you want to change priority for, click the Change Priority button, and specify a new priority for this rule.

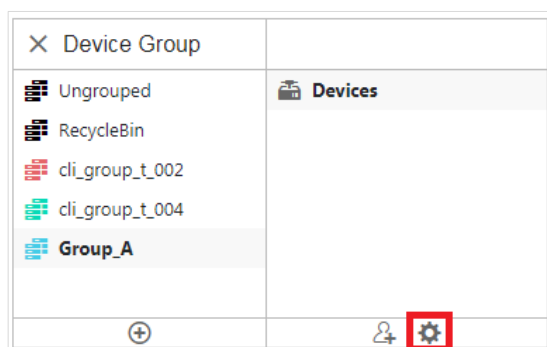
NOTE When more than one policy enforcement rule is matched, the IEC-G102-BP Series device will take the action defined in the rule with the highest priority, and will ignore remaining rules. By default, the rules listed in the rules table are ordered by priority, with the highest priority rule listed in the top row of the table.

Configuring Pattern Setting

From the **Node Management** screen, you can choose to deploy a specified DPI (Deep Packet Inspection) pattern to all IEC-G102-BP Series nodes of the same device group.

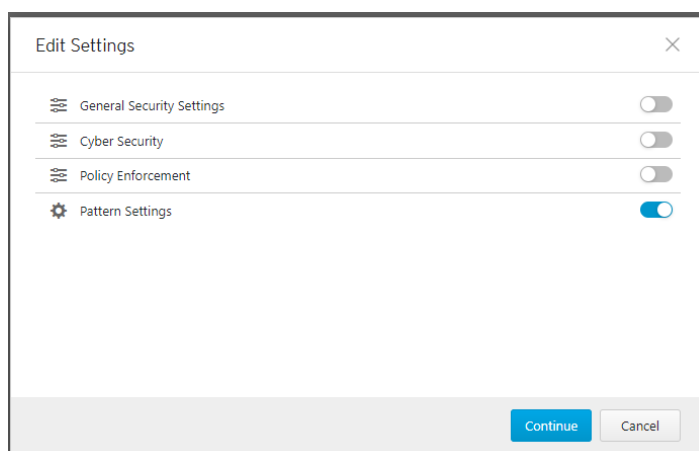
Enabling Pattern Setting

1. Click the device group you want to manage.
2. Click the **Edit Settings** () button.



The **Edit Settings** screen will appear.

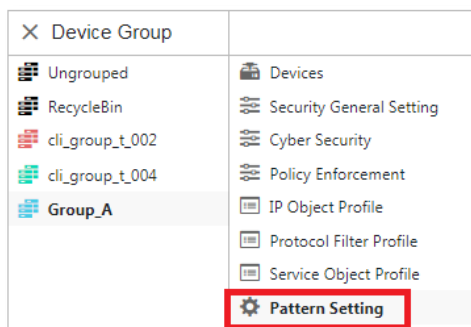
3. Toggle the **Pattern Setting** slider to enable the feature and click **Continue**.



4. Click **Save** to apply your settings.

Configuring Pattern Settings

1. Click the device group you want to manage.
2. Click **Pattern Setting**.




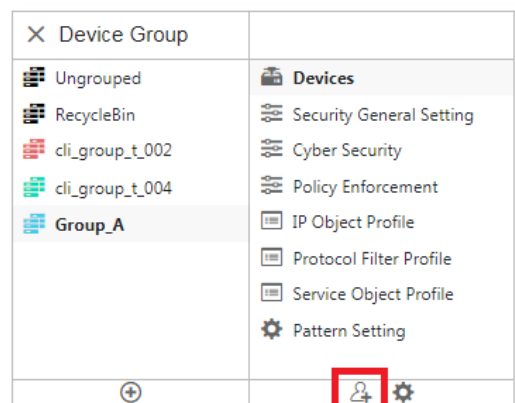
3. Select the DPI pattern to be deployed to the IEC-G102-BP Series nodes:
 - **Latest:** Always deploy the latest DPI pattern available on the SDC.
 - **Fixed version:** Deploy the specified DPI version.
4. Click **Save**.

Sharing Management Permissions to Other User Accounts

By default, the device group can only be created or managed by the admin account. However, the administrator can share access permissions to other users after a device group is created. See the **User Roles** section for more details.

Sharing Management Permissions

1. Click the device group you want to manage.
2. Click the **Share** () button.



The **Share with Others** screen appears

- Click **Add** and select the user accounts to share access to the device group with.

Share with others



Who has access

+ Add		Total Number of Records: 0	
<input type="checkbox"/>	ID	Name	Role
No data to display			

Done

- Click **Done**.

Object Profiles

Object profiles 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 object profiles in Security Dashboard Console:

- **IP Object Profile:** Contains the IP addresses that you can apply to a policy rule.
- **Service Object Profile:** Contains the service definitions that you can apply to a policy rule. TCP port range, UDP port range, ICMP, and custom protocol number are defined here.
- **Protocol Filter Profile:** Contains advanced protocol settings that you can apply to a policy rule. Details of ICS (Industrial Control System) protocols are defined here.

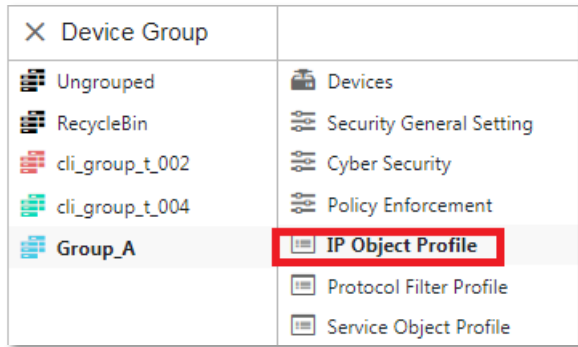
The following topics are covered in this chapter:

- ❑ **Configuring IP Object Profiles**
- ❑ **Configuring Service Object Profiles**
- ❑ **Configuring Protocol Filter Profiles**

Configuring IP Object Profiles

You can configure the IP address in an IP object profile, which can be applied to the device group to which they belong.

1. Navigate to **Node Management** → **EtherCatch**.
2. Select the device group you want to manage.
3. Select **IP Object Profile**. If this option is not visible, you may need to enable **Policy Enforcement** first.



4. Click **Add**.
5. Enter a name for the profile.
6. Enter a description for the profile.
7. Under **IP Profile List**, specify an IP address, an IP address range, or an IP subnet.
8. If you want to add another entry, click the **Add** (+) button.
9. Click **OK**.

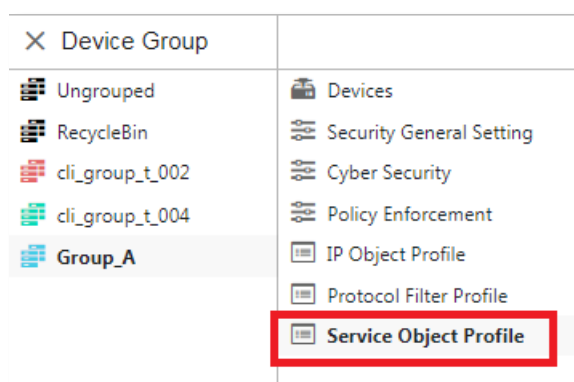
Configuring Service Object Profiles

In a service object profile, you can define the following:

- TCP protocol port range
- UDP protocol port range
- ICMP protocol type and code
- Custom protocol with specified protocol number

NOTE The term **protocol number** refers to the protocol number defined in the Internet protocol suite.

1. Navigate to **Node Management** → **EtherCatch**.
2. Select the device group you want to manage.
3. Select **Service Object Profile**. If this option is not visible, you may need to enable **Policy Enforcement** first.



4. Click **Add**.
5. Enter a name for the profile.
6. Enter a description for the profile.
7. Select a Service Object from the drop-down menu and specify the values based on the selected object:
 - a. **TCP**: Specify the protocol number and the port range.
 - b. **UDP**: Specify the protocol number and the port range.
 - c. **ICMP**: Specify the protocol number, the ICMP type, and code.
 - d. **Custom**: Specify the custom protocol with a specified protocol number.
8. If you want to add another entry, click the **Add** (+) button.
9. Click **OK**.

Configuring Protocol Filter Profiles

A protocol filter profile contains more advanced protocol settings that you can apply to a policy rule.

The following can be configured in a protocol filter profile:

- Details of ICS protocols, including:
 - Modbus
 - CIP
 - S7COMM
 - S7COMM_PLUS
 - PROFINET
 - SLMP
 - FINS
- General Protocol, including:
 - HTTP
 - FTP
 - SMB
 - RDP
 - MQTT

▼ ICS Protocol		
<input type="checkbox"/> Protocol Name	Advanced Settings	Information
<input type="checkbox"/> Modbus	<button>Settings</button>	Any
<input type="checkbox"/> CIP	<button>Settings</button>	Any
<input type="checkbox"/> S7COMM	<button>Settings</button>	Any
<input type="checkbox"/> S7COMM_PLUS	<button>Settings</button>	Any

▼ General Protocol		
<input type="checkbox"/> Protocol Name		
<input type="checkbox"/> HTTP		
<input type="checkbox"/> FTP		

1. Navigate to **Node Management → EtherCatch**.
2. Select the device group you want to manage.
3. Select **Protocol Filter Profile**. If this option is not visible, you may need to enable **Policy Enforcement** first.

X Device Group	
Ungrouped	Devices
RecycleBin	Security General Setting
cli_group_t_002	Cyber Security
cli_group_t_004	Policy Enforcement
Group_A	IP Object Profile
	Protocol Filter Profile
	Service Object Profile

4. Click **Add**.
5. Enter a name for the profile.
6. Enter a description for the profile.

7. In the **ICS Protocol** section, select the protocols you want to include in the protocol filter.
 - a. Click **Settings** next to a protocol, and select one of the following:
 - **Any** - Specify all available commands or function accesses in this protocol.
 - **Basic** - Multiple selections of the following:
 - **Read Only:** Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
 - **Read / Write:** Read and write commands sent from HMI/EWS/SCADA to PLC.
 - **Admin Config:** Firmware update commands sent from EWS to PLC, project update (i.e., PLC code download) commands sent from EWS to PLC, and administration configuration relevant commands sent from EWS to PLC.
 - **Others:** Private commands, undocumented commands, or particular protocols provided by an ICS vendor.
 - b. If you have selected **Modbus**, you can optionally configure advanced settings for this protocol:
 - Click **Settings** next to **Modbus**, and select **Professional Setting**.

Modbus Advanced Setting

Command / Function category access permission ⓘ

☐ Any
 ☐ Basic
 ☐ Read Only
 ☐ Read / Write
 ☐ Admin Config
 ☐ Others

☒ Professional Setting

Function list

0x01: Read Coils

Function Code

0x01 ⓘ

Unit ID

0 ⓘ

Address

Any ⓘ

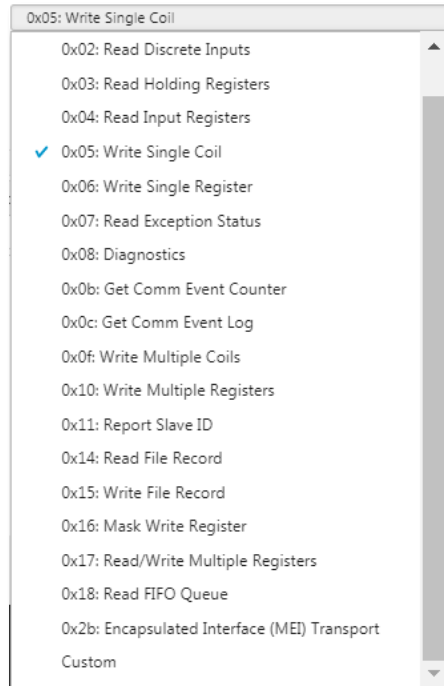
Add

Delete

Max: 8 function code list

<input type="checkbox"/>	No	Function Code	Function Code List	Unit ID	Address
No data to display					

- From the **Function List** drop-down menu, select a function for this protocol.



- If you want to specify a function code by yourself, then select **Custom** and input a function code in the **Function Code** field.
 - Specify the unit ID.
 - Type the address or address range against which the function will operate.
 - Click **Add**.
 - Repeat the above steps if you want to add more protocol definition entries.
 - Click **OK**.
8. In the **General Protocol** section, select the general protocols you want to include in the protocol filter.
9. Click **OK**.

This chapter describes the system event logs and security detection logs you can view on the management console.

The following topics are covered in this chapter:

- ❑ **Viewing Cyber Security Logs**
- ❑ **Viewing Protocol Filter Logs**
- ❑ **Viewing System Logs**
- ❑ **Viewing Audit Logs**
- ❑ **Viewing Asset Detection Logs**
- ❑ **Viewing Policy Enforcement Logs**

Viewing Cyber Security Logs

The cyber security logs cover logs generated by both the intrusion prevention and denial of service prevention features.

Logs > Cyber Security Logs

Device Name		Search
Latest 5000 records	Last 1 hour	
Time	Device Name	Serial Number
2020-01-21T18:44:21+08:00	IPS-e7bdf9	TMG01-e7bdac120008
2020-01-21T18:44:21+08:00	IPS-e7bdf9	TMG01-e7bdac120008
2020-01-21T18:44:21+08:00	IPS-15e695	TMG01-15e6ac12000c
2020-01-21T18:44:21+08:00	IPS-15e695	TMG01-15e6ac12000c
2020-01-21T18:44:21+08:00	IPS-0644e3	TMG01-0644ac120009
2020-01-21T18:44:21+08:00	IPS-0644e3	TMG01-0644ac120009
2020-01-21T18:44:21+08:00	IPS-0644e3	TMG01-0644ac120009
2020-01-21T18:44:21+08:00	IPS-e8921c	TMG01-e892ac120012
2020-01-21T18:44:21+08:00	IPS-e34dd3	TMG01-e34dac120010
2020-01-21T18:44:21+08:00	IPS-e34dd3	TMG01-e34dac120010
2020-01-21T18:44:21+08:00	IPS-2f1e2d	TMG01-2f1eac12000f
Records: 1-100 / 5000 100 per page 1 / 50		

1. Navigate to **Logs → Cyber Security Logs**.
2. You can perform the following actions:
 - Select a time period from the drop-down list. The logs will renew immediately to reflect the time period. The options include **Last 1 hour**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom range**.

Custom range

Last 1 hour

Last 24 hours

Last 7 days

Last 30 days

✓ Custom range

2020-01-21

21:16:15

~

2020-01-21

21:16:15

<

January 2020

>

<

January 2020

>

Su

Mo

Tu

We

Th

Fr

Sa

29

30

31

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

1

Su

Mo

Tu

We

Th

Fr

Sa

29

30

31

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

1

Hour:

Minute:

Second:

Hour:

Minute:

Second:

Save

Cancel

- Select the number of search results from the drop-down list. The logs will renew immediately. The options include **Latest 100 records**, **Latest 1000 records**, and **Latest 5000 records**.

Latest 5000 records

La

Latest 100 records

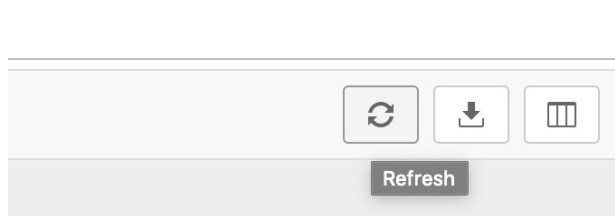
Latest 1000 records


✓ Latest 5000 records

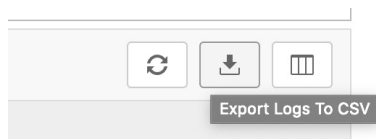
- Select a specific category from the drop-down list, type the value that you want to search for in the input field, then click **Search**.

The screenshot shows a search interface. At the top, there is a dropdown menu labeled 'Device Name' with a list of options: 'Device Name' (selected with a checkmark), 'Serial Number', 'Event ID', 'Security Category', 'Security Severity', and 'Security Rule Name'. To the right of the dropdown is a text input field containing the word 'something'. A blue 'Search' button is located to the right of the input field. Below this, there is a summary bar that says 'Search by: Device Name is "something" x Clear all'. Below the summary bar, there is another dropdown menu labeled 'Device Name' and an empty text input field, with a blue 'Search' button to the right.

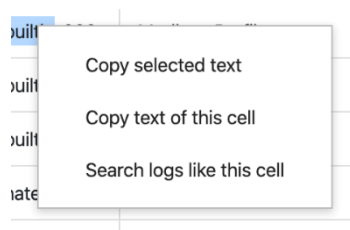
- Click the **Refresh** () button to renew the search results.




- Click the **Export Logs To CSV** () button to export the current search results as a CSV file .



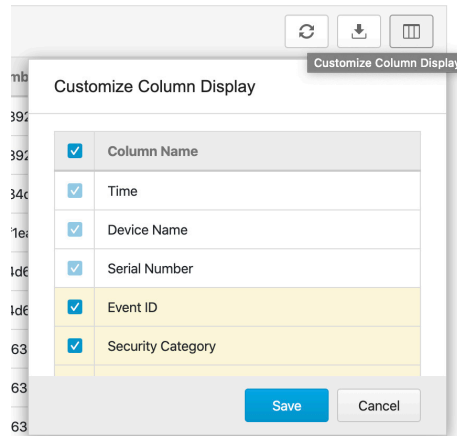
- Right-click on a cell to open the context menu. You can perform one of the following actions:
 - Copy selected text
 - Copy text of this cell
 - Search logs like this cell



- Click the **Customize Column Display** () button to customize the data displayed in each column.

The **Customize Column Display** window appears.

- Select one or more table columns to display.
- Click **Save**.



The following table describes the log's fields.

Field	Description
Time	The time the log entry was created.
Device Name	The host name of the node that generated the log.
Serial Number	The serial number of the node.
Event ID	The ID of the matched signature.
Security Category	The category of the matched signature.
Security Severity	The severity level assigned to the matched signature.
Security Rule Name	The name of the matched signature.
Source MAC Address	The source MAC address of the connection.
Source IP Address	The source IP address of the connection.
Source Port	The source port of the connection.
Destination MAC address	The destination MAC address of the connection.
Destination IP Address	The destination IP address of the connection.
Destination Port	The destination port of the connection.
VLAN ID	The VLAN ID of the connection.
Ethernet Type	The Ethernet type of the connection.
IP Protocol Name	The IP protocol name of the connection.
Action	The action performed based on the policy settings.
Count	The number of detected network packets within the detection period after the detection threshold is reached.

Viewing Protocol Filter Logs

The protocol filter logs cover logs detected by the **Protocol Filter** feature, which is an advanced configuration within the **Policy Enforcement** settings.

Logs > Protocol Filter Logs

Device Name <input type="text"/> <input type="button" value="Search"/>								
Latest 5000 records <input type="button" value="Last 1 hour"/>								
Time	Device Name	Serial Number	Rule Name	Profile Name	Source MAC Address	Source IP Address	Source Port	Destination MAC Address
2020-01-21T21:10:31+08:00	IPS-e34dd3	TMG01-e34dac120010	nate-test	()	79:df:59:a8:fc:c0	192.168.119.254	32651	b8:5c:aa:8e:c0:f7
2020-01-21T21:10:31+08:00	IPS-e34dd3	TMG01-e34dac120010	nate-test	12345678901234567890123456789	08:d3:b8:e0:d2:d4	10.0.15.213	56923	7a:20:60:08:a3:f7
2020-01-21T21:10:31+08:00	IPS-e8921c	TMG01-e892ac120012	nate-test	12345678901234567890123456789(1)	8a:28:dc:27:ef:bd	10.0.2.247	36834	54:3d:4b:0c:49:da
2020-01-21T21:10:31+08:00	IPS-e8921c	TMG01-e892ac120012	nate-test	123(1)	38:bc:29:7d:8f:c2	10.0.0.235	50975	4a:a8:7e:5f:97:ad
2020-01-21T21:10:31+08:00	IPS-e8921c	TMG01-e892ac120012	nate-test	12345678901234567890123456789012	37:85:05:e0:fe:5f	192.168.120.53	62700	54:65:dd:10:08:c4
2020-01-21T21:10:31+08:00	IPS-15e695	TMG01-15e6ac12000c	builtin-001	Modbus-Profiles	61:17:19:c4:75:f3	192.168.118.239	14101	a5:b5:16:8a:3d:86
2020-01-21T21:10:31+08:00	IPS-15e695	TMG01-15e6ac12000c	builtin-001	Modbus-Profiles	0cae:ef:a2:3e:d3	10.0.11.134	50205	c9:08:2e:d4:13:9b
2020-01-21T21:10:31+08:00	IPS-15e695	TMG01-15e6ac12000c	builtin-001	New-Profiles-1	27:af:52:a6:da:0a	192.168.151.162	6283	8e:0f:cb:d0:4d:3d
2020-01-21T21:10:31+08:00	IPS-15e695	TMG01-15e6ac12000c	builtin-000	New-Profiles-1	fa:00:b7:08:83:b6	10.0.4.147	49483	cf:14:a2:89:fe:7f
2020-01-21T21:10:31+08:00	IPS-15e695	TMG01-15e6ac12000c	builtin-000	New-Profiles-1	1e:e9:90:e2:a8:c4	192.168.232.186	19239	c8:18:e7:4b:e7:ee
2020-01-21T21:10:31+08:00	IPS-2f1e2d	TMG01-2f1eac12000f	nate-test	12345678901234567890123456789012	33:15:16:04:95:a3	192.168.222.201	50583	06:4d:79:28:7b:39
Records: 1-100 / 5000 100 per page 1 / 50 < >								

1. Navigate to **Logs → Protocol Filter Logs**.
2. You can perform the following actions:
 - Select a time period from the drop-down list. The logs will renew immediately to reflect the time period. The options include **Last 1 hour**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom range**.

Custom range

~

< January 2020 >

< January 2020 >

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

Hour:

Minute:

Second:

Hour:

Minute:

Second:

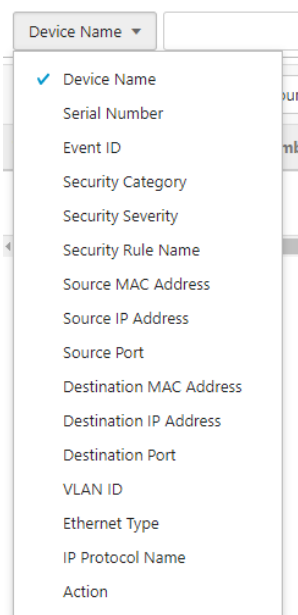
- Select the number of search results from the drop-down list. The logs will renew immediately. The options include **Latest 100 records**, **Latest 1000 records**, and **Latest 5000 records**.


Latest 5000 records

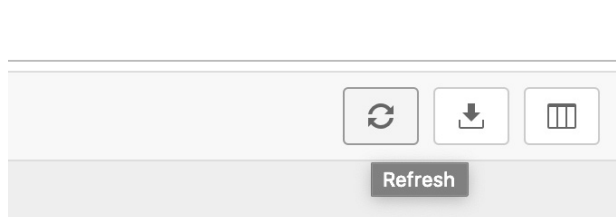
Latest 100 records


Latest 1000 records

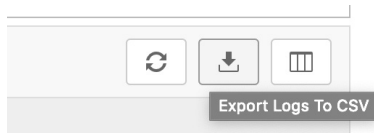
- Select a specific category from the drop-down list, type the value that you want to search for in the input field, then click **Search**.



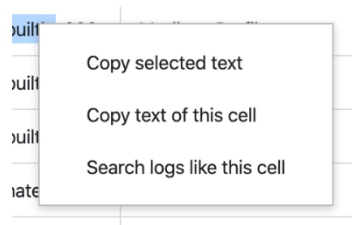
- Click the **Refresh** () button to renew the search results.




- Click the **Export Logs To CSV** () button to export the current search results as a CSV file.



- Right-click on a cell and the menu screen will appear. You can perform the following actions:
 - Copy selected text
 - Copy text of this cell
 - Search logs like this cell



- Click the **Customize Column Display** () button to customize the data displayed in each column.

The **Customize Column Display** window appears.

- Select one or more table columns to display.
- Click **Save**.

The following table describes the log's fields.

Field	Description
Time	The time the log entry was created.
Device Name	The host name of the node that generated the log.
Serial Number	The serial number of the node.
Rule Name	The name of the policy enforcement rule that was used to generate the log.
Profile Name	The name of the protocol filter profile that was used to generate the log.
Source MAC Address	The source MAC address of the connection.
Source IP Address	The source IP address of the connection.
Source Port	The source port, if protocol is selected TCP/UDP. The ICMP type, if protocol is selected ICMP.
Destination MAC address	The destination MAC address of the connection.
Destination IP Address	The destination IP address of the connection.
Destination Port	The destination port, if the selected protocol is TCP/UDP. The ICMP code, if the selected protocol is ICMP.
Ethernet Type	The Ethernet type of the connection.
IP Protocol Name	The IP protocol name of the connection.
L7 Protocol Name	The Layer 7 protocol name of the connection. The term layer 7 refers to the one defined in the OSI (Open Systems Interconnection) model.
Cmd / Fun No	The command or the function number that triggered the log.
Extra Information	Extra information provided with the log.
Action	The action performed based on the policy settings.
Count	The number of detected network packets.

Viewing System Logs

The **System Logs** screen shows all records for system-related events alongside the severity of the event and a descriptive message.

Logs > System Logs

<div>Device Name <input type="text"/></div> <div>Search</div>				
<div>Latest 5000 records <input type="button" value="v"/></div> <div>Last 1 hour <input type="button" value="v"/></div> <div> <input type="button" value="refresh"/> <input type="button" value="download"/> <input type="button" value="print"/> </div>				
Time	Device Name	Serial Number	Severity	Message
2020-01-21T21:02:51+08:00	SDC	45635534-3b97-11ea-9d7d-000c29192a39	Information	DPI pattern metadata updated
2020-01-21T21:02:41+08:00	SDC	45635534-3b97-11ea-9d7d-000c29192a39	Information	Scheduled update for component (Trend Micro DPI Pattern) finished
2020-01-21T21:02:41+08:00	SDC	45635534-3b97-11ea-9d7d-000c29192a39	Information	No new version available for component (Trend Micro DPI Pattern)
2020-01-21T21:02:37+08:00	SDC	45635534-3b97-11ea-9d7d-000c29192a39	Information	Scheduled update for component (Trend Micro DPI Pattern) started
<div>Records: 1-4 / 4</div> <div>100 per page <input type="button" value="v"/></div> <div>1 / 1</div> <div> <input type="button" value="prev"/> <input type="button" value="next"/> </div>				

1. Navigate to **Logs → System Logs**.
2. You can perform the following actions:
 - Select a time period from the drop-down list. The logs will renew immediately to reflect the time period. The options include **Last 1 hour**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom**

range.

Custom range ▾

Last 1 hour
Last 24 hours
Last 7 days
Last 30 days
✓ Custom range

2020-01-21 21:16:15 ~ 2020-01-21 21:16:15

< January 2020 > < January 2020 >

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

Hour: Minute: Second: Hour: Minute: Second:

Save Cancel

- Select the number of search results from the drop-down list. The logs will renew immediately. The options include **Latest 100 records**, **Latest 1000 records**, and **Latest 5000 records**.


Latest 5000 records ▾ La




Latest 100 records
Latest 1000 records
✓ Latest 5000 records

- Select a specific category from the drop-down list, type the value that you want to search for in the input field, then click **Search**.


Device Name ▾




✓ Device Name
Serial Number
Severity

- Click the **Refresh** () button to renew the search results.

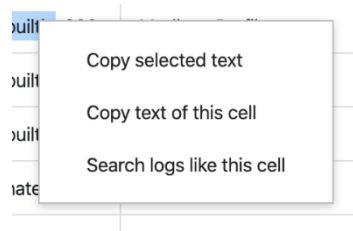
Refresh


- Click the **Export Logs To CSV** () button to export the current search results as a CSV file.

Export Logs To CSV

- Right-click on a cell and the menu screen will appear. You can perform the following actions:
 - Copy selected text
 - Copy text of this cell
 - Search logs like this cell



- Click the **Customize Column Display** () button to customize the data displayed in each column.

The **Customize Column Display** window appears.

- Select one or more table columns to display.
- Click **Save**.




The following table describes the log's fields.

Field	Description
Time	The time the log entry was created.
Device Name	The host name of the node that generated the log.
Serial Number	The serial number of the node.
Severity	The severity level of the log.
Message	The log event description.

Viewing Audit Logs

The **Audit Logs** screen shows details about user access, configuration changes, and other events that occurred when using the Security Dashboard Console.

Logs > Audit Logs

<div>Device Name <input type="text"/></div> <div>Search</div>						
<div>Latest 5000 records <input type="button" value="v"/></div> <div>Last 1 hour <input type="button" value="v"/></div> <div>    </div>						
Time	Device Name	Serial Number	User ID	Client IP	Severity	Message
2020-01-21T21:04:37+08:00	SDC	45635534-3b97-11ea-9d7d-000c29192a39	ali	10.1.230.131	Notice	User (ali) login
2020-01-21T20:57:16+08:00	SDC	45635534-3b97-11ea-9d7d-000c29192a39	ali	10.1.230.131	Notice	User (ali) timeout, force logout
2020-01-21T20:57:15+08:00	SDC	45635534-3b97-11ea-9d7d-000c29192a39	ali	10.1.230.131	Notice	User (ali) timeout, force logout
2020-01-21T20:26:46+08:00	SDC	45635534-3b97-11ea-9d7d-000c29192a39	ali	10.1.230.131	Notice	User (ali) login
<div>Records: 1-4 / 4</div> <div>100 per page <input type="button" value="v"/></div> <div>1 / 1</div> <div> <input type="button" value="v"/> <input type="button" value="v"/> </div>						

- Navigate to **Logs → Audit Logs**.
- You can perform one of the following actions:
 - Select a time period from the drop-down list. The logs will renew immediately to reflect the time period. The options include **Last 1 hour**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom**

range.

- Select the number of search results from the drop-down list. The logs will renew immediately. The options include **Latest 100 records**, **Latest 1000 records**, and **Latest 5000 records**.

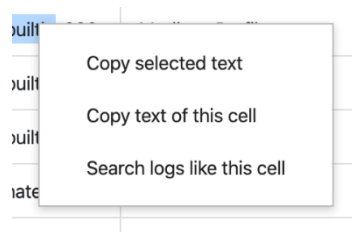
- Select a specific category from the drop-down list, type the value that you want to search for in the input field, then click **Search**.


- Click the **Refresh** () button to renew the search results.

- Click **Export Logs To CSV** to export the current search results as a CSV file.

- Right-click on a cell and the menu screen will appear. You can perform the following actions:
 - Copy selected text
 - Copy text of this cell

- Search logs like this cell



- Click the **Customize Column Display** () button to customize the data displayed in each column.
The **Customize Column Display** window appears.
 - Select one or more table columns to display.
 - Click **Save**.

The following table describes the log's fields.

Field	Description
Time	The time the log entry was created.
Device Name	The host name of the node that generated the log.
Serial Number	The serial number of the node.
User ID	The user account used to execute the task.
Client IP	The IP address of the host used to access the management console.
Severity	The severity level of the log.
Message	The log event description.

Viewing Asset Detection Logs

The asset detection logs cover the system status changes of the managed assets.

Logs > Asset Detection Logs

Device Name

Search

Latest 5000 records

Last 1 hour

Time	Device Name	Serial Number	Event Type	Asset MAC Address	Asset IP Address
2020-01-21T21:18:41+08:00	IEF-bb7db2	TMF01-bb7dac120006	Asset Information Changed	c6:82:cc:3e:45:a9	192.168.52.205
2020-01-21T21:18:41+08:00	IEF-bb7db2	TMF01-bb7dac120006	Timeout	db:d0:c0:2a:c:f:cd	192.168.20.239
2020-01-21T21:18:41+08:00	IEF-bb7db2	TMF01-bb7dac120006	Asset Information Changed	12:ee:4a:bb:d8:06	10.0.12.240
2020-01-21T21:18:41+08:00	IEF-bb7db2	TMF01-bb7dac120006	Asset Information Changed	cc:55:76:aa:bc:e9	10.0.14.238
2020-01-21T21:18:41+08:00	IEF-e04435	TMF01-e044ac120011	Timeout	21:7d:bd:fb:11:53	192.168.88.217
2020-01-21T21:18:41+08:00	IEF-d91616	TMF01-d916ac120004	New Asset	6d:b8:c3:cb:b3:d0	10.0.5.233
2020-01-21T21:18:41+08:00	IEF-d91616	TMF01-d916ac120004	Timeout	38:e6:65:f6:59:15	10.0.5.73
2020-01-21T21:18:41+08:00	IEF-dd14fd	TMF01-dd14ac12000a	Asset Information Changed	42:f3:06:62:16:54	10.0.8.239
2020-01-21T21:18:41+08:00	IEF-dd14fd	TMF01-dd14ac12000a	Asset Information Changed	7e:b7:b4:8d:fd:ca	192.168.204.105
2020-01-21T21:18:41+08:00	IEF-dd14fd	TMF01-dd14ac12000a	Asset Information Changed	cf:7d:b5:d3:bf:9c	192.168.250.255
2020-01-21T21:18:41+08:00	IEF-1c2513	TMF01-1c25ac120007	Asset Information Changed	64:58:0b:92:9f:6b	10.0.7.88

Records: 1-100 / 5000

100 per page


1 / 50

1. Navigate to **Logs → Asset Detection Logs**.
3. You can perform one of the following actions:
 - Select a time period from the drop-down list. The logs will renew immediately to reflect the time period. The options include **Last 1 hour**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom**

range.

- Select the number of search results from the drop-down list. The logs will renew immediately. The options include **Latest 100 records**, **Latest 1000 records**, and **Latest 5000 records**.

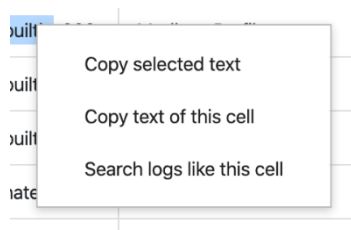
- Select a specific category from the drop-down list, type the value that you want to search for in the input field, then click **Search**.


- Click the **Refresh** () button to renew the search results.

- Click **Export Logs To CSV** to export the current search results as a CSV file.

- Right-click on a cell and the menu screen will appear. You can perform the following actions:
 - Copy selected text

- Copy text of this cell
- Search logs like this cell



- Click the **Customize Column Display** () button to customize the data displayed in each column.

The **Customize Column Display** window appears.

- Select one or more table columns to display.
- Click **Save**.




The following table describes the log's fields.

Field	Description
Time	The time the log entry was created.
Device Name	The host name of the node that generated the log.
Serial Number	The serial number of the node.
Event Type	The log event description.
Asset MAC Address	The MAC address of the asset.
Asset IP Address	The source IP address of the asset.

Viewing Policy Enforcement Logs

The **Policy Enforcement Logs** cover logs generated by the **Policy Enforcement** feature with **Protocol Filter** disabled. This means the policy enforcement action is either to allow or deny traffic, without relying on advancing protocol filtering rules.

Logs > Policy Enforcement Logs

<div>Device Name <input type="text"/></div> <div>Search</div>										
<div>Latest 5000 records ▾ Last 1 hour ▾</div> <div>    </div>										
Time	Device Name	Serial Number	Rule ID	Rule Name	Source MAC Address	Source IP Address	Source Port	Destination MAC Address	Destination IP Address	Destination Port
2020-01-21T21:19:20+08:00	IPS-74d64c	TMG01-74d6ac120005	0	builtin-001	ee:89:57:0f:73:c8	10.0.14.161	13802	7e:08:74:15:cc:5c	192.168.134.216	6371
2020-01-21T21:19:20+08:00	IPS-15e695	TMG01-15e6ac12000c	0	builtin-000	fd:dd:8f:ca:00:62	10.0.5.227	40936	4e:26:2d:26-6c:40	192.168.113.204	2831
2020-01-21T21:19:20+08:00	IPS-15e695	TMG01-15e6ac12000c	0	builtin-000	6f:c6:69:1a:7e:fb	10.0.3.246	387	6b:23:64:51:e7:df	192.168.71.122	4261
2020-01-21T21:19:20+08:00	IEF-bb7db2	TMF01-bb7dac120006	0	builtin-001	ed:b3:aa:ac:8f:c5	10.0.0.254	23307	26:4a:2d:5c:77:b8	192.168.5.51	7165
2020-01-21T21:19:20+08:00	IEF-bb7db2	TMF01-bb7dac120006	0	builtin-001	54:7fee:23:15:98	10.0.13.98	24605	49:6a:5c:03:0fa8	10.0.0.133	3431
2020-01-21T21:19:20+08:00	IEF-bb7db2	TMF01-bb7dac120006	0	builtin-000	18:11:65:28:8f:3a	192.168.190.205	2733	a3:8ef1:8e:a2:db	192.168.188.155	7734
2020-01-21T21:19:20+08:00	IEF-bb7db2	TMF01-bb7dac120006	0	builtin-001	e0:72:78:58:70:5f	10.0.0.211	3341	f3:a2:aca:f7:cf	192.168.126.25	3881
2020-01-21T21:19:20+08:00	IPS-15e695	TMG01-15e6ac12000c	0	builtin-001	72:6c:aa:43:08:8b	192.168.229.147	12651	6e:0d:06:53:bacdb	192.168.219.56	6441
2020-01-21T21:19:20+08:00	IPS-74d64c	TMG01-74d6ac120005	0	builtin-000	14:7c:9f:f3:90:65	192.168.35.94	63207	aa:5a:50:64:01a3	10.0.14.73	3371
2020-01-21T21:19:20+08:00	IPS-e8921c	TMG01-e892ac120012	0	nate-test	66:f8:0b:32:4b:f8	10.0.2.60	51271	17:bc:58:b4:20:27	192.168.112.234	4421
2020-01-21T21:19:20+08:00	IPS-e8921c	TMG01-e892ac120012	0	nate-test	11:bb:e8:fb:3b:61	10.0.6.220	47617	61:69:de:95:b3:ff	192.168.177.221	4351
<div>Records: 1-100 / 5000 100 per page ▾ 1 / 50 < ></div>										

1. Navigate to **Logs → Policy Enforcement Logs**.
4. You can perform one of the following actions:
 - Select a time period from the drop-down list. The logs will renew immediately to reflect the time period. The options include **Last 1 hour**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom**.

range.

Custom range ▾

Last 1 hour
Last 24 hours
Last 7 days
Last 30 days
✓ Custom range

2020-01-21 21:16:15 ~ 2020-01-21 21:16:15

< January 2020 > < January 2020 >

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

Hour: Minute: Second:

Hour: Minute: Second:

Save Cancel

- Select the number of search results from the drop-down list. The logs will renew immediately. The options include **Latest 100 records**, **Latest 1000 records**, and **Latest 5000 records**.

Latest 5000 records ▾ La

Latest 100 records

Latest 1000 records




✓ Latest 5000 records

- Select a specific category from the drop-down list, type the value that you want to search for in the input field, then click **Search**.

Device Name ▾

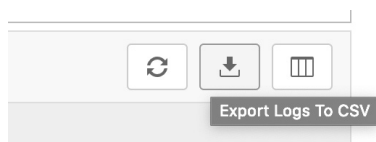
- ✓ Device Name
- Serial Number
- Rule ID
- Rule Name
- Source MAC Address
- Source IP Address
- Source Port
- Destination MAC Address
- Destination IP Address
- Destination Port
- IP Protocol Name
- Action

- Click the **Refresh** () button to renew the search results.

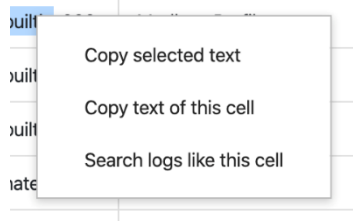
  


Refresh

- Click **Export Logs To CSV** to export the current search results as a CSV file.



- Right-click on a cell and the menu screen will appear. You can perform the following actions:
 - Copy selected text
 - Copy text of this cell
 - Search logs like this cell



- Click the **Customize Column Display** () button to customize the data displayed in each column.
The **Customize Column Display** window appears.
 - Select one or more table columns to display.
 - Click **Save**.

The following table describes the log's fields.

Field	Description
Time	The time the log entry was created.
Device Name	The host name of the node that generated the log.
Serial Number	The serial number of the node.
Rule Name	The name of the policy enforcement rule that was used to generate the log.
Source MAC Address	The source MAC address of the connection.
Source IP Address	The source IP address of the connection.
Source Port	The source port, if protocol is selected TCP/UDP. The ICMP type, if protocol is selected ICMP.
Destination MAC address	The destination MAC address of the connection.
Destination IP Address	The destination IP address of the connection.
Destination Port	The destination port, if the selected protocol is TCP/UDP. The ICMP code, if the selected protocol is ICMP.
IP Protocol Name	The IP protocol name of the connection.
Action	The action performed based on the policy settings.

Administration

This chapter describes the available administrative settings for SDC (Security Dashboard Console).

The following topics are covered in this chapter:

❑ **Account Management**

- User Roles
- Account Input Format
- Adding a User Account
- Changing Your Password
- Configuring the Password Policy
- ID/Password Reset

❑ **Configuring System Time**

❑ **Configuring Syslog Settings**

- Syslog Severity Levels
- Syslog Severity Level Mapping Table

❑ **Updates**

- Updating Components Manually
- Importing a Component File
- Scheduling Component Updates
- Managing the Component Repository

❑ **Managing SSL Certificates**

- Replacing an SSL certificate
- Verifying an SSL certificate
- Removing the Built-in Certificate

❑ **Log Purge**

- Viewing Database Storage Usage
- Configuring Automatic Log Purge
- Manually Purging Logs

❑ **Back Up/Restore**

- Restoring a Configuration

❑ **License**

- Introduction to the Licenses
- Viewing Your Product License Information
- Alert Messages
- Activating or Renewing Your Product License
- Manually Refresh the License

❑ **Proxy**

- Configuring Proxy Settings

Account Management

NOTE Log onto the management console using the administrator account to access the Accounts tab.

SDC system uses role-based administration to grant and control access to the management console. Use the **Account Management** feature to assign specific management privileges to the accounts and configure the 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 log in to the management console using custom user accounts.

The following table outlines the tasks available on the **Account Management** tab.

Task	Description
Add a user account	Click Add to create a new user account. For more information, see Account Input Format .
Delete an existing account	Select the user accounts you want to remove and click Delete .
Edit an existing account	Click the name of an existing user account to view or modify the current account settings.
Configure the Password Policy	Click Password Policy to adjust password restrictions.

User Roles

The following tables describe the permissions matrix for user roles for the different configuration tabs within the SDC.

Administration Tab

		User Roles			
Sub-Tab	Action	Admin	Operator	Viewer	Auditor
Account Management	View	Yes	No	No	No
	All operations	Yes	No	No	No
System Time	View	Yes	No	No	No
	All operations	Yes	No	No	No
Syslog	View	Yes	No	No	No
	All operations	Yes	No	No	No
Updates	View	Yes	No	No	No
	All operations	Yes	No	No	No
SSL Certificate	View	Yes	No	No	No
	All operations	Yes	No	No	No
Log Purge	View	Yes	No	No	No
	All operations	Yes	No	No	No
Backup/Restore	View	Yes	No	No	No
	All operations	Yes	No	No	No
License Control	View	Yes	No	No	No
	All operations	Yes	No	No	No

Dashboard, Visibility, and Log Tabs

		User Roles			
Tab	Action	Admin	Operator	Viewer	Auditor
Dashboard	View	Yes	VG	VG	No
Visibility	View	Yes	VG	VG	No
Log (system, cyber security, policy enforcement, protocol filtering, asset detection)	View	Yes	VG	VG	No
Audit Log	View	Yes	No	No	Yes

NOTE VG denotes that if the administrator has assigned/shared the device group permissions to the user account, then the user can view the information for that device group on the Dashboard/Visibility/Log tabs.

Node Management Tab

		User Roles			
Item	Action	Admin	Operator	Viewer	Auditor
Ungroup	View	Yes	Yes	No	No
	All operations	Yes	No	No	No
Recycle Bin	View	Yes	Yes	No	No
	All operations	Yes	No	No	No
Groups	View	Yes	Yes	No	No
	Device operations (Move/delete)	Yes	No	No	No
	Device operations (Edit/reboot)	Yes	Yes	No	No
	Edit group configuration	Yes	Yes	No	No
	Edit permission settings	Yes	No	No	No
	Group operations (Add/delete/rename)	Yes	No	No	No
	Enable/disable device group configurations	Yes	Yes	No	No

NOTE Device group configurations refers to cyber security, policy enforcement, and pattern settings.

Account Input Format

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

Edit User Account

ID

NewUser_1

Name

first_user

Password

Confirm Password

Role

Operator

Description

Your First User!!

Invalid format. Please verify that the input data is in valid format and try again. (3-0)

Confirm

Cancel

Type	Length	Format	Reserved Name
ID	1 to 32 characters	Letters: a-z, A-Z Numbers: 0-9 Special characters: periods (.), underscores (_) Leading and trailing characters are not special characters Non-successive special characters	admin administrator root auditor
Name	1 to 32 characters	Letters: a-z, A-Z Numbers: 0-9 Special characters: periods (.), underscores (_), spaces The name cannot consist of only spaces	
Description	0 to 64 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 the SDC system.

Procedure

1. Navigate to **Administration** → **Account Management**.
2. Click **Add**.

The **Add User Account** screen appears.

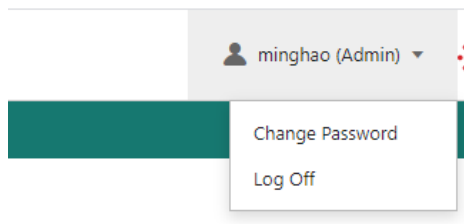
3. Configure the account settings.

Field	Description
ID	Enter the user ID that will be used to log in to the management console.
Name	Enter an alias name for the account. This name is for display purposes only.
Full name	Enter the name of the user for this account.
Password	Enter the account password.
Confirm password	Enter the account password again to confirm.
Role	Select a user role for this account.
Description	Enter a description for this account.

4. Click **Save**.

Changing Your Password

1. On the management console banner in the top-right, click your account name.
2. Click **Change Password**.

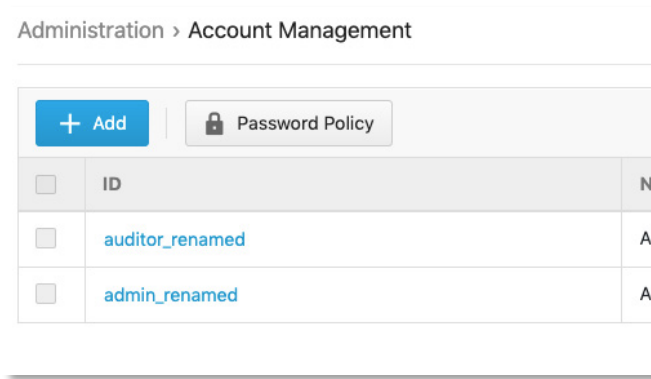


The **Change Password** screen appears.

3. Specify the password settings.
 - Old password
 - New password
 - Confirm password
4. Click **Save**. This will automatically log you out and will bring you back to the login screen.

Configuring the Password Policy

To improve password strength, the administrator can customize the password policy in the **Account Management** screen to enforce a degree of complexity in user account passwords.



1. Navigate to **Administration** → **Account Management**.
2. Click **Password Policy**.

The **Password Policy** screen appears.

✕

Password Policy

Minimum password length:

8

(8 - 32)

☐ Not include user account name

☐ Not include user full name

☐ Include at least one uppercase letter (A - Z)

☐ Include at least one lowercase letter (a - z)

☐ Include at least one number (0 - 9)

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

☐ Not be the same as the last password

Confirm

Cancel

3. Select the password requirements.
4. Click **Confirm**.

ID/Password Reset

In some specific situations, for security reasons, users are required to reset their ID or password in their next login session.

	Scenario	
User Roles	First Time Logging in	Password Change Request By Admin
Admin	Reset ID / Password	
Auditor	Reset ID / Password	
Operator	Reset Password	
Viewer	Reset Password	

Configuring System Time

Network Time Protocol (NTP) synchronizes computer system clocks across the Internet. Configure NTP settings to synchronize the server clock with an NTP server, or manually set the system time.

1. Navigate to **Administration** → **System Time**.

Administration > System Time

Date and Time

Current Time: 2019-10-22T14:54:13+08:00

☒ Synchronize system time with an NTP server

NTP Server: (Default time server: pool.ntp.org)

Time Zone

Time Zone:

2. In the **Date and Time** pane, select one of the following:
 - Synchronize system time with an NTP server.
 - a. Specify the domain name or IP address of the NTP server.
 - b. Click **Synchronize Now**.
 - Set the system time manually.
 - a. Click the calendar to select the date and time.
 - b. Set the hour, minute, and second.
 - c. Click **Apply**.
2. From the **Time Zone** drop-down list, select the time zone.
3. Click **Save**.

NOTE The SDC will automatically synchronize the system time with its managed nodes.

Configuring Syslog Settings

The SDC system maintains Syslog events that provide summaries of security and system events. Common Event Format (CEF) syslog messages are used in SDC.

From the Syslog Settings, you can configure the SDC system to send the Syslog records to a Syslog server.

1. Navigate to **Administration → Syslog**.
2. Select **Send logs to a syslog server** to have the SDC system send logs to a syslog server.
3. Configure the following settings.

Syslog Settings

☒ Send logs to a syslog server

Server address:

Port:

Protocol:
☐ TCP ☒ UDP

Facility Level:

Log Level:

Available logs:

Selected logs:

- CYBER_SECURITY_LOG
- PROTOCOL_FILTER_LOG
- POLICY_ENFORCEMENT_LOG
- ASSET_LOG
- SYSTEM_LOG

Field	Description
Server address	Enter the IP address of the syslog server.
Port	Enter the port number.
Protocol	Select the protocol for the communication.
Facility level	Select a facility level to determine the source and priority of the logs.
Log level	Select a syslog severity level. SDC system only sends logs with the selected severity level or higher to the syslog servers. For more information, see Syslog Severity Level Mapping Table .

4. Select the types of logs to send to the syslog server from the **Available logs** panel and click the **Transfer** (⇄) button.
5. Click **Save**.

Syslog Severity Levels

The syslog severity level specifies the type of messages to be sent to the syslog server.

Level	Severity	Description
0	Emergency	<ul style="list-style-type: none"> Complete system failure Take immediate action.
1	Critical	<ul style="list-style-type: none"> Primary system failure Take immediate action.
2	Alert	<ul style="list-style-type: none"> Urgent failures Take immediate action.
3	Error	<ul style="list-style-type: none"> Non-urgent failures Resolve issues quickly.
4	Warning	<ul style="list-style-type: none"> Error pending Take action to avoid errors.
5	Notice	<ul style="list-style-type: none"> Unusual events Immediate action is not required.
6	Informational	<ul style="list-style-type: none"> Normal operational messages useful for reporting, measuring throughput, and other purposes No action is required.
7	Debug	<ul style="list-style-type: none"> Useful information when debugging the application. NOTE: Setting the debug level can generate a large amount of syslog traffic in a busy network. Use with caution to avoid traffic flooding.

Syslog Severity Level Mapping Table

The following table summarizes the logs of Policy Enforcement/Protocol Filter/Cyber Security and their equivalent Syslog severity levels.

Policy Enforcement / Protocol Filter Action	Cyber Security Severity Level	Syslog Severity Level
		0 - Emergency
	Critical	1 - Alert
	High	2 - Critical
		3 - Error
Deny	Medium	4 - Warning
		5 - Notice
Allow		6 - Information
		7 - Debug

Updates

Download and deploy components for IEC-G102-BP Series. Moxa frequently create new component versions and performs regular updates to address the latest network threats.

Updating components will immediately download the updated versions from the update server. The components will be deployed to security nodes based on the settings configured in the **Node Management** tab. For more information, see **Node Management**.

The following table describes the available components on the **Updates** tab.

Field	Description
DPI Pattern	Contains signatures to enable the following features: <ul style="list-style-type: none">Intrusion prevention Detects and prevents behaviors related to network intrusion attempts and targeted attacks at the network level.
IEC-G102-BP Series Firmware	IEC-G102-BP Series firmware
IEF-G9010 Series Firmware	IEF-G9010 Series firmware

NOTE The SDC system maintains various versions of components in its repository, which allows you to configure which version (a fixed version or the latest) to deploy to the managed nodes.

You can update the components using one of the following methods:

- **Manual updates:** You can manually update components on the SDC system.
- **Manual import of components:** You can manually import components into the SDC system.
- **Scheduled updates:** The SDC system automatically checks and downloads the latest available components from an update source based on a pre-configured schedule.

NOTE The updated components are deployed to managed nodes based on the settings configured in the **Node Management** tab.

NOTE Internet access is needed for the SDC to perform manual updates and/or scheduled updates. Specifically, the SDC system will need to visit odc.cs.txone-networks.com and txone-component-prod.s3.amazonaws.com via HTTPS in order to check the update information and/or to download components.

Updating Components Manually

You can manually update the components on the SDC system. When a component update is complete, SDC system deploys the updated components to managed nodes based on the settings configured in the **Node Management** tab.

1. Navigate to **Administration → Updates**.
2. If a component has a new version available, click **Update Now** in the **Actions** column.

When the component update is complete, the value in the **Latest Version** and **Release Date** columns will be updated to reflect the new component version or will stay the same if it is already up-to-date.


Importing a Component File

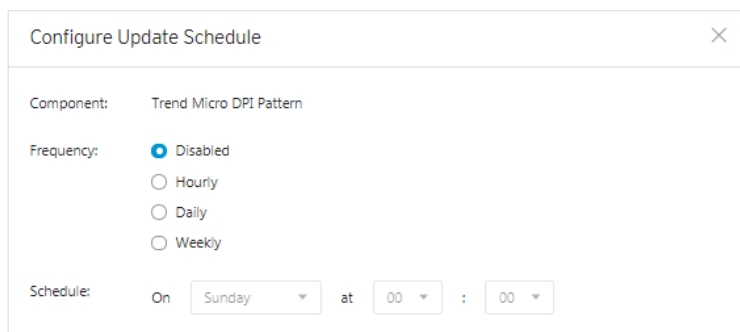
If you are provided a component file, you can manually import the file to the SDC system. The SDC system deploys the updated components to managed nodes based on the settings configured in the **Node Management** tab.

1. Navigate to **Administration → Updates**.
2. Click **Import** for the component.
3. Select the component file.
4. Click **Open** to start the import process.

Scheduling Component Updates

Configure scheduled updates to receive protection from the latest threats or updated firmware of the managed nodes. The SDC system deploys the updated components to managed nodes based on the settings configured in the **Node Management** tab.

1. Navigate to **Administration → Updates**.
2. Click the **Edit** () button in the **Schedule Update** column of the component you want to set the update schedule for.
The **Configure Update Schedule** screen appears.



The dialog box titled "Configure Update Schedule" contains the following fields:

- Component:** Trend Micro DPI Pattern
- Frequency:** ☒ Disabled, ☐ Hourly, ☐ Daily, ☐ Weekly
- Schedule:** On at :

3. Specify the update interval.
4. Click **Save**.

Managing the Component Repository

SDC can store multiple versions of the same component such as firmware or pattern upgrades. All the imported or updated components are maintained in the component repository. You can view and manage the available components on the repository.

1. Navigate to **Administration → Updates**.
2. Click the update component.
The **Component Details** window appears, which allows you to view the available components on the repository.
3. **(Optional)** If you want to delete a component, select the component and click **Delete**.
4. Click **OK**.

Managing SSL Certificates

The SDC system uses the HTTPS protocol to encrypt web traffic between the user's web browser and the web management console. The HTTPS protocol uses an SSL certificate signed by TXOne. This chapter introduces how to change the SSL certificate.

Replacing an SSL certificate

1. Navigate to **Administration → SSL Certificate**.
2. Click **Import Certificate**.
3. Next to the **Certificate** field, click **Select File ...** to import your certificate file.
4. Next to the **Private Key** field, click **Select File ...** to import the private key for the certificate file.
5. Input the passphrase if the certificate requires one.
6. Click **Import and Restart**.

Verifying an SSL certificate

After adding a new certificate to the SDC system, you can verify the certificate is effective.

1. Log in to the SDC system through a web browser.

NOTE The SDC supports Chrome version 63 or later, Firefox version 53 or later, Safari 10.1 or later, Microsoft Edge version 15 or later.

2. In the top-right corner of the browser, navigate to **Three Dots Menu → More Tools → Developer Tools**.
3. Click on the **Security** tab. This will open the **Security Overview** panel. If the tab is not visible, click the **Expand** (») button to see the hidden tabs.
4. In the **Security Overview** panel, click **View certificate**, and you will see the certificate details of the SDC system.

Removing the Built-in Certificate

You can optionally choose to remove the built-in certificate:

1. Navigate to **Administration → SSL Certificate**.
2. Click **Remove Certificate**.
The **Remove Certificate** window appears.
3. Click **Remove and Restart**. A self-signed certificate will be used after the built-in certificate is removed.

Log Purge

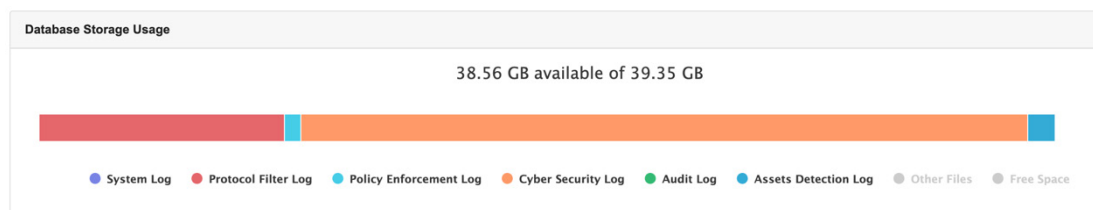
From the **Log Purge** window, you can view the status of the logs stored on the hard drive of the system running SDC and configure log purging methods. Purging logs may be useful when the system generates a lot of event logs, which may impact network performance.

The SDC system maintains logs and reports in its appliance hard disk. You can purge the logs in the following ways:

- Automatic purge: The log can be automatically deleted based on a specified threshold number of log entries, a retention period for log data, or both.
- Manual log purge: The logs can be manually deleted based on a specified condition.

Viewing Database Storage Usage

The **Database Storage Usage** window shows the used and total size of the database storage.



1. Navigate to **Administration → Log Purge**.

Configuring Automatic Log Purge

Automatic log purging will cause the system to periodically clear the log database based on the defined criteria. You can configure purging rules each individual log type.

1. Navigate to **Administration → Log Purge**.

2. In the **Automatic Purge** section, specify the automatic log purge criteria.

The number shown for **keep at most xxxxx entries** is calculated based on the disk storage allocated to the SDC.

Automatic Purge

Purge Assets Detection Log older than	60 month(s) ▼	and keep at most	100,000,000 ▼	entries.
Purge Audit Log older than	48 month(s) ▼	and keep at most	100,000,000 ▼	entries.
Purge Cyber Security Log older than	no limit ▼	and keep at most	100,000,000 ▼	entries.
Purge Policy Enforcement Log older than	48 month(s) ▼	and keep at most	100,000,000 ▼	entries.
Purge Protocol Filter Log older than	60 month(s) ▼	and keep at most	100,000,000 ▼	entries.
Purge System Log older than	48 month(s) ▼	and keep at most	100,000,000 ▼	entries.

3. Click **Save**.

NOTE When the number of a log type reaches the preconfigured threshold value, the SDC system will start to clear the logs, beginning with the oldest records.

Manually Purging Logs

1. Navigate to **Administration → Log Purge**.

2. In the **Purge Now** section, specify the criteria and click **Purge Now**. Any logs that meet the criteria will be purged immediately.

Purge Now

Purge	--Select-- ▼	older than	no limit ▼	and keep at most	0 ▼	entries.	Purge Now
-------	--------------	------------	------------	------------------	-----	----------	------------------

Back Up/Restore

You can export settings from the management console to back up the configuration of your Security Dashboard Console. If a system failure occurs, you can restore the settings by importing the configuration file that you previously backed up.

We recommend the following:

- Back up the current configuration before importing any configuration.
- Perform configuration backups and restores when the SDC is idle. Importing and exporting configuration settings affects the performance of SDC.
- Back up your configuration frequently.

You can back up the following settings to a configuration file:

- Administration > Account Management
- Administration > System Time
- Administration > Syslog
- Administration > Log Purge
- Administration > Updates (only schedule settings)
- Administration > Proxy
- Node Management > IEC-G102-BP Series

1. Navigate to **Administration → Back Up / Restore**.
2. In the **Back Up Configuration** section, click **Back Up**.
The **File Download** window appears.
3. Click **Save** to save the configuration file to the local storage.

Restoring a Configuration

If necessary, you can restore a previously backed up SDC configuration. This will overwrite the existing configuration.

1. Navigate to **Administration → Back Up / Restore**.
2. In the **Restore Configuration** section, click **Select File** or **Browse** and navigate to the configuration file on the local storage.
3. Click **Restore**.
All services will restart. It may take some time to restart services after applying imported settings and rules.

License

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

NOTE Log in to the management console using the administrator account to access the License tab.

Introduction to the Licenses

Three license types are used for SDC:

- Node License
- IEC-G102-BP pattern upgrade license
- IEF-G9010 pattern upgrade license

Node license - Determines the maximum number of nodes to be managed by SDC.

IEC-G102-BP/ IEF-G9010 pattern upgrade license - The number of seats allowed in the license should be equal to or greater than the nodes managed by the SDC, such that the nodes can update pattern/firmware via the SDC.

In SDC, only one node license is used at a time. Thus, when more than one node license is applied to the SDC, only the latest one will be kept in the SDC.

Multiple IEC-G102-BP/ IEF-G9010 pattern upgrade licenses can co-exist in the same SDC instance. When multiple pattern upgrade licenses are applied to the SDC, all the licenses will be kept in the SDC.

Viewing Your Product License Information

1. Navigate to **Administration** → **License**.

The **License** screen appears.

2. The following table describes the license information.

Field	Description
License Type	The type of license key
License Key	The license key currently in use.
Seat	The number of nodes that can be managed by this SDC
End Date	The expiration date of the license key
Remark	Additional information for this license key

The following table describes further information for the **Remark** field.

Message	Description
Expired license	The license has expired.
Void license	The license is invalid or has been revoked.
Will expire in X days	The license will expire in the displayed number days.
Not enough seats to support the IEC-G102-BP/IEF-G9010 pattern upgrade licenses	Insufficient IEC-G102-BP and IEF-G9010 node seats to support additional pattern upgrade licenses.

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. If the logged in user is the admin, then the license key will be displayed on the screen. Other types of users will not be able to see the license key in the alert message.

Message	Description
The license (xxx-xxx-xxx-xxx) expires in (xx) days. To continue using all features, specify a new license key.	This message appears 30 days before the license expiration date. The (xx) represents the days remaining before the license expires
The license (xxx-xxx-xxx-xxx) has expired. You will stop receiving product updates and technical support in xx days. To continue using all features, specify a new license key.	The license has expired and has entered a grace period to renew the license. If the license is not renewed within this period, you will be required to purchase a new license to continue using the product.
The license (xxx-xxx-xxx-xxx) has expired. To restore all features, specify a valid license key.	The license has expired and cannot be renewed.

When the IEC-G102-BP/IEF-G9010 pattern upgrade license's seat number is insufficient for the current amount of managed nodes, the nodes will not be able to update their patterns and firmware. Alert messages will pop up in the web management console.

Activating or Renewing Your Product License

1. Navigate to **Administration → License**.

Administration > License

Apply License Key		Refresh		
License Type	License Key	Seat	End Date	Remark
No data to display				

2. Click **Apply License Key** button.
The **Apply License Key** screen appears.
3. Enter the new license key.
4. Click **Check**.
5. Verify the license information shown and click **OK**.

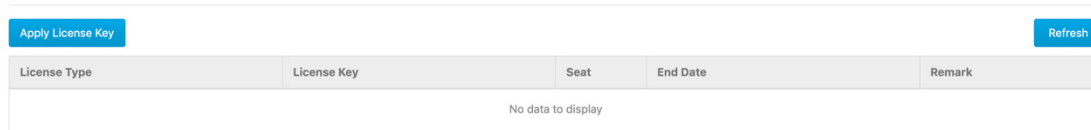
NOTE The SDC must be connected to the Internet when applying the license key in order to connect to odc.cs.txone-networks.com via HTTPS to register the license key and retrieve the license information.

Manually Refresh the License

If the values of your license is changed by the backend license management server for example the expiration date being extended or the seat number being increased, you can manually refresh your license at your web management console to reflect these changes.

1. Navigate to **Administration → License**.

Administration > License



The screenshot shows the 'License' page in the Administration console. At the top, there are two buttons: 'Apply License Key' on the left and 'Refresh' on the right. Below these buttons is a table with the following headers: 'License Type', 'License Key', 'Seat', 'End Date', and 'Remark'. The table body is empty, and a message 'No data to display' is centered at the bottom of the table area.

2. Click the **Refresh** button.

NOTE The SDC must be connected to the Internet when refreshing the license key in order to connect to odc.cs.txone-networks.com via HTTPS to retrieve the license information.

Proxy

If required, you can configure SDC to use a proxy server for component and license updating.

Configuring Proxy Settings

1. Navigate to **Administration → Proxy**.
2. Click **Use a proxy server when connecting to the servers for pattern, device firmware, and license updates**.
3. Specify the following details:
 - The IP address of the proxy server
 - The port of the proxy server
4. If the server requires authentication, select **Proxy server requires authentication**, and enter the required credentials.
5. Click **Save**.

Setting SDC's Connection

Setting up a Connection to SDC Via the IEC-G102-BP Series Web Console

A node is an IEC-G102-BP Series product that is managed by the SDC. A managed node can be configured by SDC and send event logs to SDC. Before the node can be managed remotely, you will need to configure the connection to the SDC through the device's web configuration interface.

1. Open a web browser and enter the device's IP address in the address field. The default IP address is **192.168.127.254**.
2. Log in using your username and password. If this is your first time logging in, use the default administrator login credentials:
 - User name: **admin**
 - Password: **moxa**
3. Navigate to **Administration → Sync Settings**.
4. Specify the IPv4 address of SDC in the **SDC Server Address** field.
5. Ensure that **Enable SDC Management** is enabled.
6. Click **Save**.

Introduction to the vShell

vShell is the SDC CLI (command line interface) tool that you can use to monitor status, troubleshoot, and configure settings using commands.

The following topics are covered in this appendix:

❑ **First Time Using vShell**

- Accessing vShell
- Change the Default Password to Activate

❑ **How to Set Up a Network**

- Displaying the Network Settings
- Update the Interface

❑ **How to Set Up the ACL**

- Querying the Status
- Adding Clients to the Whitelist
- Deleting Clients from the Whitelist
- Enable/Disable the ACL of Modules
- Shortcut Table

❑ **List of Command Prompt Commands**

- Summary
- access-list
- env
- exit
- help
- iface
- ping
- poweroff
- reboot
- resolv
- scp
- service
- sftp

First Time Using vShell

Accessing vShell

You can access vShell using one of the following methods:

1. On a local machine
2. On a remote machine over SSH

The default administrator credentials are:

User: **root**

Password: **moxa**

Change the Default Password to Activate

When signing in to vShell for the first time, you will see the following warning messages.

```
Caution: please type the command ``oobe`` to activate the vShell.  
Caution: please type the command ``oobe`` to activate the vShell.  
Caution: please type the command ``oobe`` to activate the vShell.  
Caution: please type the command ``oobe`` to activate the vShell.  
Caution: please type the command ``oobe`` to activate the vShell.
```

Please follow the steps below to activate the terminal.

Enter the **oobe** command.

```
$ oobe
```

Enter the the default password:

```
Type current password:
```

Enter a new password to change the default password.

NOTE The password field will only accept alphanumerical and some additional characters: !@#%^*_+}:?~[]'./
--

NOTE The password can be between 8 and 32 characters in length.
--

```
Type the new password:
```

Confirm the new password:

```
Retype it:
```

After activating the vShell successfully, please log in again.

```
"Success! Please log in again."
```

How to Set Up a Network

Displaying the Network Settings

To see the network details of a specific interface, enter the following command:

```
$ iface ls
```

Below, the part in the square brackets shows the interface's configuration, and the part under the closed square brackets describes the current network settings running on the system.

```
[
  {
    "Name": "lo",
    "Family": "inet",
    "Method": "loopback"
  },
  {
    "Name": "eth0",
    "Family": "inet",
    "Method": "dhcp"
  }
]
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:0c:29:07:05:2c brd ff:ff:ff:ff:ff:ff
    inet 10.7.19.155/24 brd 10.7.19.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe07:52c/64 scope link
        valid_lft forever preferred_lft forever
```

Update the Interface Settings

Using STATIC



WARNING

The designated network interface name is **eth0**, so any edits to the configuration of this interface could affect the system's ability to connect to the internet.

To use a static connection to connect to SDC, you need to manually enter an IP address, gateway, and subnet mask for the device.

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

Below is an example of a static connection.

```
$ iface ls
[
  {
    "Name": "lo",
    "Family": "inet",
    "Method": "loopback"
  },
  {
    "Name": "eth0",
    "Family": "inet",
    "Method": "static",
    "Address": "192.0.2.4",
    "Netmask": "255.255.255.0",
    "Gateway": "192.0.2.254"
  }
]
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:0c:29:07:05:2c brd ff:ff:ff:ff:ff:ff
    inet 10.7.19.155/24 brd 10.7.19.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe07:52c/64 scope link
        valid_lft forever preferred_lft forever
```

After confirming the changes, restart eth0 to apply the new network settings.

```
$ iface restart eth0
Successfully restart! Please check the network status
```

Using DHCP



WARNING

The designated network interface name is **eth0**, so any edits to the configuration of this interface could affect the system's ability to connect to the internet.

```
$ iface update eth0 --method dhcp
Interface settings are changed. Please restart interface
```

(Optional) Under the Static IP method, an extra step is needed to remove the properties:

```
$ iface trim eth0 address
Interface settings are changed. Please restart interface
$ iface trim eth0 gateway
Interface settings are changed. Please restart interface
$ iface trim eth0 netmask
Interface settings are changed. Please restart interface
```

Below is an example of a static connection.

```
$ iface ls
[
  {
    "Name": "lo",
    "Family": "inet",
    "Method": "loopback"
  },
  {
    "Name": "eth0",
    "Family": "inet",
    "Method": "dhcp"
  }
]
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:0c:29:07:05:2c brd ff:ff:ff:ff:ff:ff
    inet 10.7.19.155/24 brd 10.7.19.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe07:52c/64 scope link
        valid_lft forever preferred_lft forever
```

After confirming the changes, restart eth0 to apply the new network settings.

NOTE

Enter the **iface ls** command to check that the interface has successfully restarted and is working properly.

```
$ iface restart eth0
Successfully restart! Please check the network status
```

How to Set Up the ACL

vShell provides whitelisting to block all clients who are not on the whitelist.

You can manage access using one of three methods:

- SSH: Manage SSH server connection privileges.
- Device: Manage IEC-G102-BP Series connection privileges.
- Web: Manage users' dashboard connection privileges.

Querying the Status

You can check the status of the whitelist at any time, as well as the port number and IP/CIDR.

```
$ access-list ls
SSH(tcp:22)
Status: Disabled
Network

Device(udp:123, tcp:7590, tcp:9093)
Status: Enabled
Network
1.1.1.1/32

Web(tcp:443)
Status: Disabled
Network
```

Adding Clients to the Whitelist

You can add client IPs or Classless Inter-Domain Routing (CIDR) to the whitelist.

```
$ access-list append SSH 1.1.1.1
added! Please check the whitelist
$ access-list append SSH 1.1.1.0/24
1.1.1.0/24 added! Please check the whitelist
```

Deleting Clients from the Whitelist

You can delete client IPs or Classless Inter-Domain Routing (CIDR) from the whitelist.

```
$ access-list trim SSH 1.1.1.1
removed! Please check the whitelist
$ access-list removed SSH 1.1.1.0/24
1.1.1.0/24 removed! Please check the whitelist
```


Enable/Disable the ACL of Modules

**WARNING**

If you log in over SSH, enabling the SSH ACL will immediately force you out of your SSH session.

**WARNING**

Before you enable the ACL, please add clients to the whitelist. If clients are not added before ACL is enabled, all clients will be blocked.

```
$ access-list up Device
Device enabled! Please check the whitelist
$ access-list down Device
Device disabled! Please check the whitelist
```

Shortcut Table

Tab	Auto-complete or choose the next suggestion on the list
Ctrl + A	Go to the head of the line (Home)
Ctrl + E	Go to the tail of the line (End)
Ctrl + D	Delete the character located at the cursor
Ctrl + L	Clear the screen

List of Command Prompt Commands

Summary

Commands	Description
access-list	Manage the IP whitelists.
env	Manage system environment variables.
exit	Exit this shell.
help	List all commands
iface	Manage the network interfaces.
ping	Test the reachability of a host.
poweroff	Shut down the machine immediately.
reboot	Restart the machine immediately.
resolv	Set up the domain name server.
scp	Send files via SCP.
service	Manage the dashboard service.
sftp	Send files via SFTP.

access-list

Manage the IP whitelists.

SSH: Manage the connections to the SSH server.

Device: Manage the IPS or IEF connections.

Web: Manage the dashboard user connections.

ls - List all ip in the whitelists.

```
$ access-list ls
```

append - Append an IP/CIDR to the whitelist.

```
$ access-list append Device 192.168.1.1
```

```
$ access-list append Device 192.168.0.0/16
```

trim - Delete an IP/CIDR from the whitelist.

```
$ access-list trim Device 192.168.1.1
```

```
$ access-list trim Device 192.168.0.0/16
```

up - Whitelist the IP address.

```
$ access-list up Device
```

down - Do not whitelist the IP address.

```
$ access-list down Device
```

env

Manage system environment variables.

hostname - Assign /etc/hostname value

NOTE The host name should be between 1 and 64 characters long.

```
$ env hostname NAME
```

exip - Assign /acus/external_ip value

NOTE Entering **default** is equal to the eth0 IP address.

```
$ env exip 192.168.1.1
```

```
$ env exip default
```

ls - List the environment variables in this server.

NOTE If the External IP value reads **Not Set**, it will use the eth0 IP address as the default value.

```
$ env ls
```

```
Hostname:      my-dashboard-server
```

```
ID:            55365266-108d-11ea-bca4-080027171302
```

```
Web Version:   1.0.0
```

```
External IP:   Not Set
```

exit

Exit this shell.

```
$ exit
```

help

List all help commands

```
$ help
vShell, version v1.0.0
The commands provided in:
access-list    Manage the IP whitelists
env            Manage system environment variables
exit          Exit this shell
help          List all command usage
iface         Manage the network interfaces
ping          Test the reachability of a host
poweroff      Shut down the machine immediately
reboot        Restart the machine immediately
resolve       Manage the domain name server
scp           Send files via scp
service       Manage the dashboard service
sftp          Send files via sftp

Shortcut table:
Tab           Auto-complete or choose the next suggestion on the list
Ctrl + A     Go to the head of the line (Home)
Ctrl + E     Go to the tail of the line (End)
Ctrl + D     Delete the character located at the cursor
Ctrl + L     Clear the screen
```

iface

Manage the network interfaces.

ls - List all the interfaces and display 'ip addr'.

```
$ iface ls
```

add - Add the interface in /etc/network/interfaces, if the interface name is not repeated

Options

```
--address
--netmask
--gateway

$ iface add INTERFACE METHOD [OPTIONS]
$ iface ls
[
{
  "Name": "lo",
  "Family": "inet",
  "Method": "loopback",
  "Address": "1.2.3.4",
},
{
  "Name": "eth0",
  "Family": "inet",
  "Method": "dhcp"
}
]
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
link/ether 08:00:27:a0:4b:ec brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0
valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fea0:4bec/64 scope link
valid_lft forever preferred_lft forever

$ iface add eth1 static --address 192.168.1.3 --netmask 255.255.255.0 --
gateway 192.168.1.1

$ iface up eth1
```

update - Update the existing interface in `/etc/network/interfaces`

Options

```
--method
--address
--netmask
--gateway

$ iface update INTERFACE [OPTIONS]
$ iface update eth0 --method dhcp
$ iface restart eth0
```

trim - Remove some options from the interface in `/etc/network/interfaces`

Options

```
--address
--netmask
--gateway

$ iface trim INTERFACE [OPTIONS]
$ iface trim eth0 gateway
$ iface restart eth0
```

rm - Remove and shut down the interface from `/etc/network/interfaces`

```
$ iface rm INTERFACE
```

up - Activate the interface in /etc/network/interfaces

Options

--force

```
$ iface up INTERFACE
```

// you can force it up, if needed

```
$ iface up eth0 --force
```

down - Deactivate the interface in /etc/network/interfaces

Options

--force

```
$ iface down INTERFACE
```

// you can force it down, if needed

```
$ iface down eth0 --force
```

restart - Deactivate and then active the interface in /etc/network/interfaces

Options

--force

```
$ iface restart INTERFACE
```

FAQ for iface

Q: What should I do when the message displays "ifdown: interface INTERFACE_NAME not configured"?

A: Execute the command "iface up INTERFACE_NAME".

Q: What can I do to resume network service if all commands are unavailable?

A: Reboot the machine and restart the interface.

ping

Test the reachability of a host.

```
$ ping www.google.com
```

poweroff

Shut down the machine immediately.

```
$ poweroff
```

reboot

Restart the machine immediately.

```
$ reboot
```

resolv

Manage the DNS settings.

ls - List the DNS on the resolv.conf

```
$ resolv ls
```

add - Add the DNS to the /etc/resolvconf/resolv.conf.d/tail

```
$ resolv add NAMESERVER
```

replace - Replace the DNS in the /etc/resolvconf/resolv.conf.d/tail

```
$ resolv replace OLD_NAMESERVER NEW_NAMESERVER
```

trim - Remove the DNS from the /etc/resolvconf/resolv.conf.d/tail

```
$ resolv trim NAMESERVER
```

scp

Send file via SCP.

dlog - The OS and service debug logs.

```
$ scp dlog USER IP DIRECTORY
```

```
$ scp dlog my-debugger 10.7.6.123 '~\Log\ Folder\{1\} '
```

password:

```
$ scp dlog my-debugger 10.7.6.123 ~/Downloads
```

password:

service

Manage web services.

reload - Restart service if service configuration is changed

```
$ service reload
```

sftp

Send files via SFTP.

dlog - The OS and service debug logs.

```
$ scp dlog USER IP DIRECTORY
```

```
$ scp dlog my-debugger 10.7.6.123 '~\Log\ Folder\{1\} '
```

password:

```
$ scp dlog my-debugger 10.7.6.123 ~/Downloads
```

password: