

Security Dashboard Console Quick Installation Guide

(for VMware Workstation and ESXi)

Version 1.2, June 2021

Technical Support Contact Information
www.moxa.com/support

MOXA[®]

© 2021 Moxa Inc. All rights reserved.

P/N: 180200000A022



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	150	200	300	400	500
CPU (virtual cores)	4	4	6	8	12	14	16
RAM (GB)	8	16	16	32	64	128	256
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						

Installing SDC on a VMware Workstation

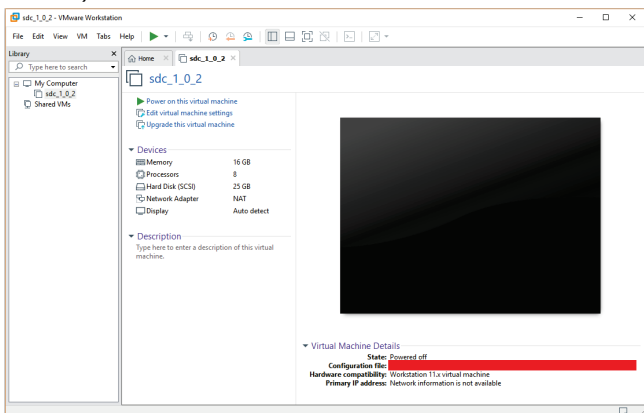
This section describes how to deploy Security Dashboard Console (SDC) to a VMware Workstation system.

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** on 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 for the new virtual machine, and the storage path for the new virtual machine, and then click **Import**.
5. Check the detailed VM information of the imported SDC VM (Virtual Machine).



6. Add an external disk. The SDC requires one external disk with at least 50 GB of available storage, otherwise the SDC will not finish initialization and the boot process will not be completed. The external disk is used to store the system configurations and event

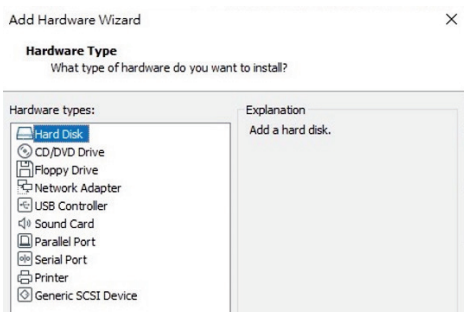
logs. You may attach the external disk of a terminated SDC instance here instead of adding a new disk if you want to migrate the previous configurations and logs to the new SDC instance.



ATTENTION

Due to software architecture changes, SDC v1.0 and v1.1 are not fully compatible. If you are migrating from SDC v1.0 to v1.1, we highly recommend attaching a new external drive and not use the old drive. Refer to the **System Migration** section for more information.

- a. Click **Edit virtual machine settings**
- b. Click **Add**, then choose **Hard Disk**



- c. Select a disk type



- d. Select Disk size. You can decide the external disk size depending on the number of logs you want to store, as shown in the table below.

# of Logs	Disk
10,000,000	50 GB
50,000,000	150 GB
100,000,000	300 GB

If the SDC needs to increase the number of the logs that can be stored, please perform the following steps:

- i. Power off the SDC.
- ii. Enlarge the external disk size to fit the maximum log requirement.
- iii. Power on the SDC instance.

Disk

Create a new virtual disk

A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.

Use an existing virtual disk

Choose this option to reuse a previously configured disk.

Use a physical disk (for advanced users)

Choose this option to give the virtual machine direct access to a local hard disk. Requires administrator privileges.

Add Hardware Wizard

Specify Disk Capacity

How large do you want this disk to be?

Maximum disk size (GB):

Recommended size for Other: 8 GB

Allocate all disk space now.

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

Store virtual disk as a single file

Split virtual disk into multiple files

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

- e. Select path to store the disk
 - f. Click **OK**
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
150	6 cores	32 GB
200	8 cores	32 GB
300	12 cores	64 GB
400	14 cores	128 GB
500	16 cores	256 GB

- a. Click **Edit virtual machine settings**.
 - b. Configure the amount of memory.
 - c. Configure the number of CPU cores.
8. **(Optional)** Change the network adapter setting from 'NAT' to 'Bridged'.
- 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.

System Migration



IMPORTANT!

Because SDC v1.0 and v1.1 are not fully compatible due to software architecture changes, all logs, patterns, and firmware stored on SDC v1.0 cannot be migrated to SDC v1.1 automatically. Only policy enforcement rules, DDoS protection rules, and objects can be migrated from the SDC v1.0 over to SDC v1.1.

Follow the instructions below if you are upgrading from SDC v1.0 to v1.1:

1. Back up your current SDC v1.0 configurations.
2. Install the new SDC (v1.1) with a new external disk.
3. Activate the SDC v1.1 license key, followed by any IEC or IEF Series licenses.
4. Load the SDC v1.0 configuration backup file onto the new SDC v1.1 instance.
5. Confirm all your devices appear correctly in SDC v1.1.

When a new version of SDC is released, the settings of the old SDC can be migrated by attaching the external disk of the old SDC to the new SDC VM. The settings that will be migrated to the SDC includes:

- 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, accounting information, security policies, and so on.
- The security event logs stored by the old SDC.

Procedure

1. Launch the new instance of SDC. (For more details, see "Deploying Security Dashboard Console" under the "Installing SDC on a VMware Workstation".)
2. Power off the old SDC
3. Attach the external disk of the old ODC to the new SDC.
4. A window will pop up where you can select which settings and data will be migrated into the new SDC, and after your confirmation the old SDC's selected information will be migrated into the new SDC.

Installing SDC on a VMware ESXi

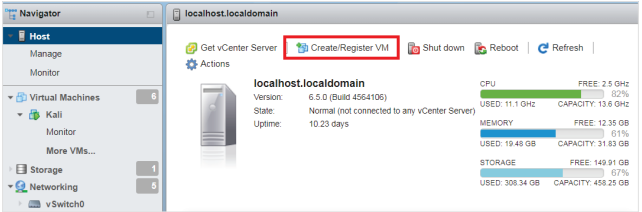
This chapter describes how to deploy the Security Dashboard Console to a VMware ESXi system.

Requirements

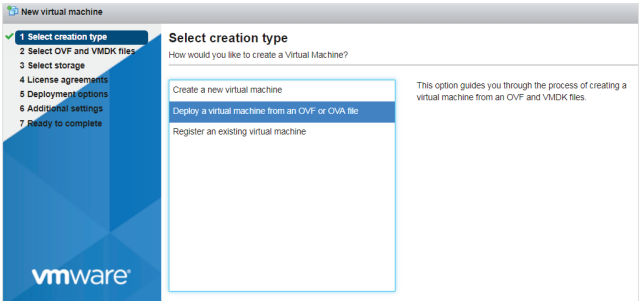
- The OVA packages provided by Moxa must be available and accessible to VMware ESXi.
- ESXi version 6 or above with the required specifications.
- The necessary networks have been properly created in ESXi.

Deploying Security Dashboard Console

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

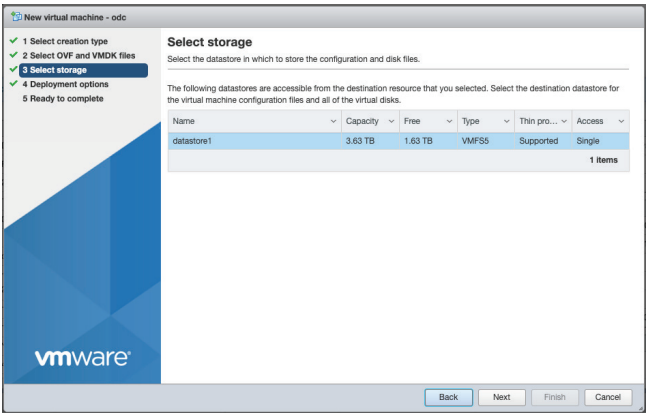


3. Select **Deploy a virtual machine from an OVF or OVA file**.

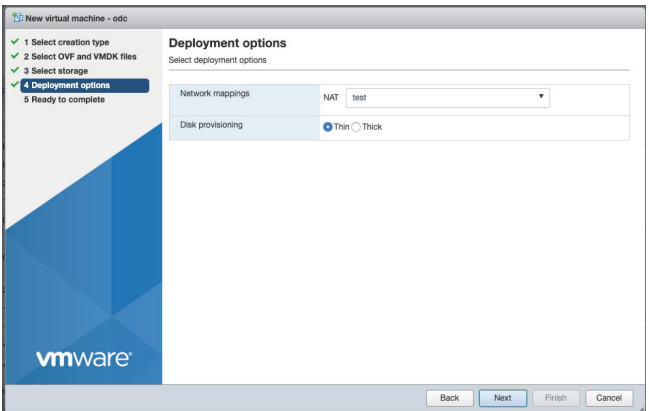


4. Input a name for your SDC and then select an SDC image to upload.

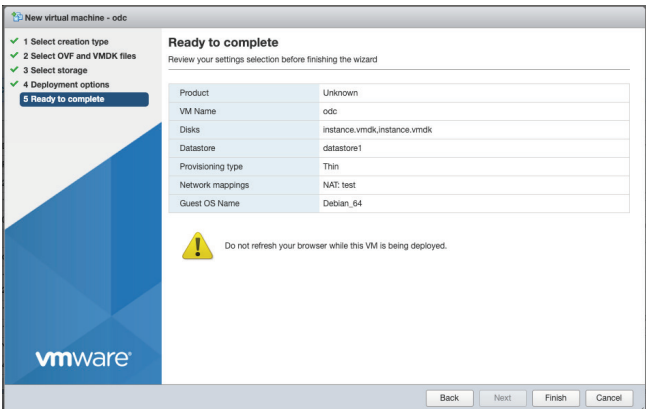
5. Choose a storage location for the SDC virtual machine.



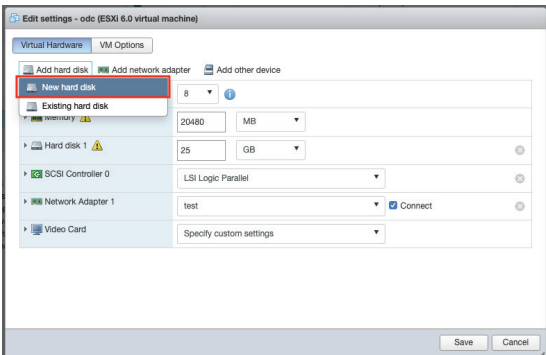
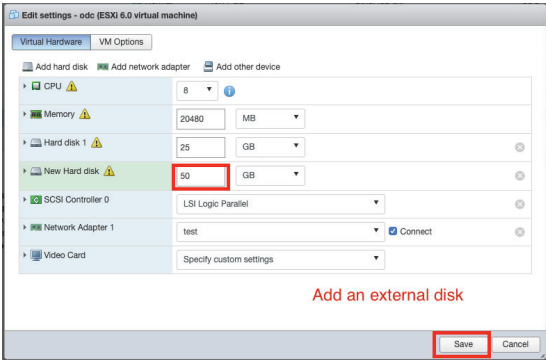
6. Select deployment options.



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



8. Under the **Recent tasks** pane, you will see a progress bar indicating that the SDC image is being uploaded. Please wait until the upload is finished.
9. Add an external disk with at least 50 GB free to the SDC instance.
 - a. Power off the SDC instance if it is powered on.
 - b. Add the external disk by taking the following steps: **Actions** → **Edit settings** → **Add hard disk** → **Save**.



- c. You can decide the external disk size depending on the number of logs to be stored, as shown on the table below.

#of Logs	Disk
10,000,000	50 GB
50,000,000	150 GB
100,000,000	300 GB

- d. **(Optional)** If the SDC needs to increase the number of logs that need to be stored, the steps are as follows: (1) power off the SDC, (2) enlarge the external disk size to fit the maximum log requirement, and (3) power on the SDC instance. After that, the SDC will have enlarged the available storage for log files.
- e. **(Optional)** 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 and the minimum size of the external disk must be above 50 GB, otherwise the SDC will not finish initialization and the boot process will not be completed.

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 here instead of adding a new disk if you want to migrate the previous configurations and logs to the new SDC instance.



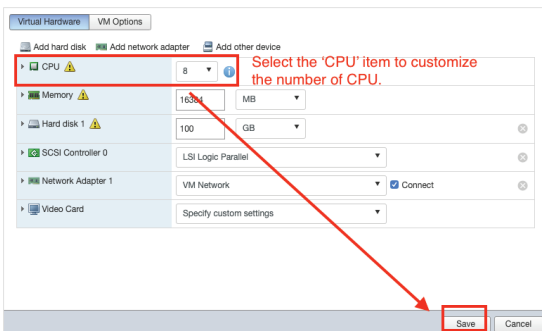
ATTENTION

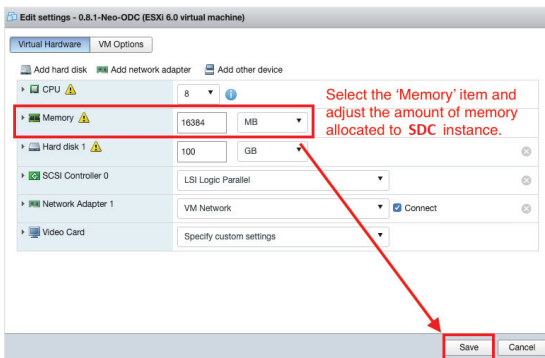
Due to software architecture changes, SDC v1.0 and v1.1 are not fully compatible. If you are migrating from SDC v1.0 to v1.1, we highly recommend attaching a new external drive and not use the old drive. Refer to the **System Migration** section for more information.

10. Power on the VM.
11. **(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).
 - a. Shut down the instance of SDC and click **Edit**, and the **Edit settings** window will appear.
 - b. Configure the number of CPU cores.
 - c. Configure the amount of memory.
 - d. Boot the SDC instance.

Sizing Table

Nodes	CPU	Memory
50	4 cores	8 GB
100	4 cores	16 GB
150	6 cores	32 GB
200	8 cores	32 GB
300	12 cores	64 GB
400	14 cores	128 GB
500	16 cores	256 GB





System Migration



IMPORTANT!

Because SDC v1.0 and v1.1 are not fully compatible due to software architecture changes, all logs, patterns, and firmware stored on SDC v1.0 cannot be migrated to SDC v1.1 automatically. Only policy enforcement rules, DDoS protection rules, and objects can be migrated from the SDC v1.0 over to SDC v1.1.

Follow the instructions below if you are upgrading from SDC v1.0 to v1.1:

1. Back up your current SDC v1.0 configurations.
2. Install the new SDC (v1.1) with a new external disk.
3. Activate the SDC v1.1 license key, followed by any IEC or IEF Series licenses.
4. Load the SDC v1.0 configuration backup file onto the new SDC v1.1 instance.
5. Confirm all your devices appear correctly in SDC v1.1.

When a new version of SDC is released, the settings of the old SDC can be migrated by attaching the external disk of the old SDC to the new SDC VM. The migration of settings includes:

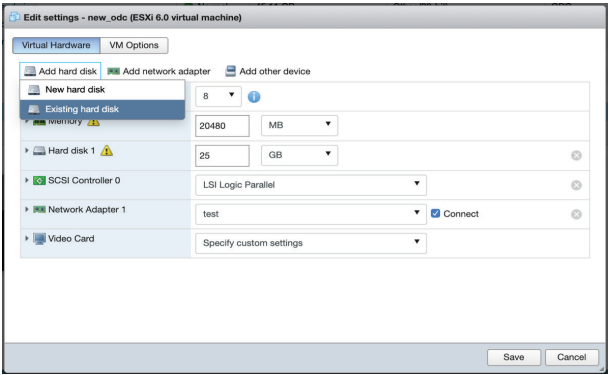
- The UUID of the old SDC (To ensure all virtual machines are identified properly, each virtual machine is automatically assigned a universal unique identifier (UUID).)
- The pattern and firmware downloaded by the old SDC.
- The system configuration set from the old SDC including its license, accounting information, security policies etc.
- The security event logs stored by the old SDC.

Procedure

Launch the new instance of SDC. (For more details, see "Deploying Security Dashboard Console" under the "Installing SDC on a VMware ESXi".)

1. Power off the old SDC.
2. Attach the external disk of the old ODC to the new SDC.

3. 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 "root/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. Type the following command to change the default password
\$ oobe
 - b. Change the default password.
 - c. Re-log in to the SDC 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. After re-logging in to the SDC, you can type the "help" command to see a list of available commands for the instance.

```
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. Type the following command to get the IP address of the SDC Instance.

```
$ ifconfig
```

```
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`.
$ ifconfig
{
  {
    "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 adaptor setting is using NAT, please set up port forwarding rules and specify NAT outbound IP to allow traffic to pass from the IEC-G102-BP Series to the SDC:

- a. Setup port forwarding rules. Please click **Edit → Virtual Network Editor**, and then select the right network subnet. Click **NAT Settings** to create the following port forwarding rules:
 - i. To access a web management console, forward packets from host TCP port 8443 to the SDC server IP TCP port 443.
 - ii. To allow users to configure the IEC-G102-BP Series through the SDC including all configuration settings and commands, packets should be forwarded from the host TCP port 7590 to the SDC server IP TCP port 7590.
 - iii. To allow IEC-G102-BP Series to upload logs to the SDC, packets should be forwarded from the host TCP port 9093 to the SDC server IP TCP port 9093.

Host Port	Type	Virtual Machine IP Address	Description
7590	TCP	192.168.18.128:7590	SDC Command Channel
9093	TCP	192.168.18.128:9093	SDC Logging Channel
8443	TCP	192.168.18.128:443	Web Console Access

- b. 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 your host PC is using Windows, you can type "ipconfig" to find it.

```

Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix . . . :
Link-local IPv6 Address . . . . . : fe80::2c60:31ac:7a0a:67b4%3
IPv4 Address. . . . . : 192.168.152.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix . . . :
Link-local IPv6 Address . . . . . : fe80::a005:7be4:8f8c:4eb1%27
IPv4 Address. . . . . : 192.168.18.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

```

- 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) Configure the IP Address Settings

You can choose to configure the IP address manually.

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 following 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

```

- Use the "resolv add" command to add a DNS server and "resolv ls" to list the DNS servers that have been added. For example, the following command adds "8.8.8.8" to the DNS server list.

```
$ resolv mode custom [the name of server]
$ resolv add 8.8.8.8
```

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

```
$ resolv ls
```

```
vShell
File Edit View Help
: resolv ls
: resolv add 8.8.8.8
8.8.8.8 is added.
: resolv ls
nameserver 8.8.8.8
```

- Open the TCP and UDP communication ports below to allow IEC-G102-BP and IEF-G9010 Series devices to communicate with SDC.

Service	UDP	TCP	Description
Command Channel	7590		Send commands to devices, bi-directional
Events Log	9093		Send event logs to SDC
NTP Services		123	NTP time synchronizing services
Syslog	601	514	Send syslog to SDC
Web Console	443		Allow SDC to access the device web console
SSH	22		(Optional) Allow SDC to access the device command line

- Execute the following command to reboot the VM:

```
$ reboot
```

Opening the Management Console

The 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.

Procedure

- 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 will appear.

- Enter your user name and password.

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

- User name: admin
- Password: moxa

- Click **Log On**.

If this is your first time to log on, the Login Information Setup frame will appear.

NOTE You must change the default login name and password at first log on before you can access the management console.

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

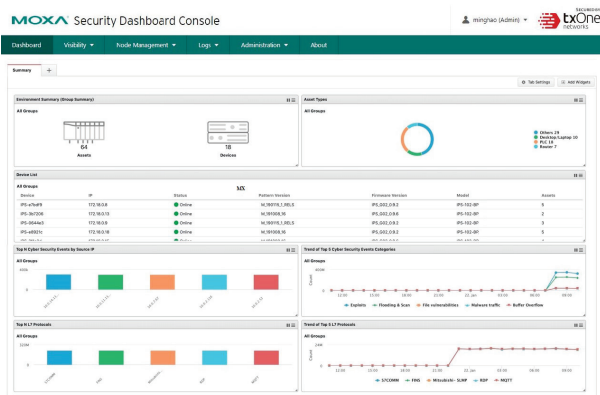
a. Confirm your password settings.

- 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 on again using your new credentials.



Register IEC-G102-BP devices to SDC

On the web console of the IEC-G102-BP device, please go to **Administration** → **Sync Settings**, and set up the SDC IP address and enable SDC management.

