Security Dashboard Console Quick Installation Guide

(for VMware Workstation and ESXi)

Version 1.3, March 2022

Technical Support Contact Information
www.moxa.com/support

P/N: 180200000A023

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, VMware Workstation 14 or above, KVM 2.x or above						

Installing SDC on a VMware Workstation

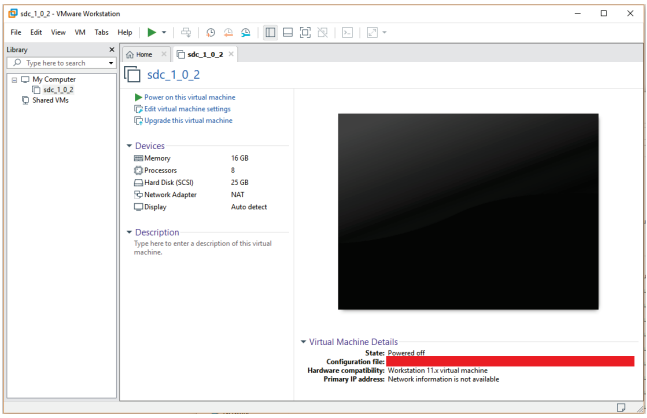
This section describes how to deploy Security Dashboard Console (SDC) on a VMware Workstation system.

Requirements

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

Deploying the 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, then click **Import**.
5. Check the detailed VM information of the imported SDC VM (Virtual Machine).



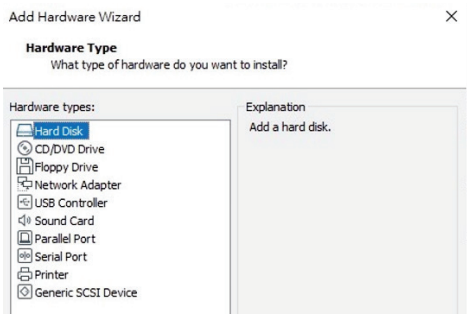
6. Add an external disk. The SDC requires one external disk with at least 50 GB of available storage, otherwise the SDC will not finish initialization and the boot process will not be completed. The external disk is used to store the system configurations and event

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**.



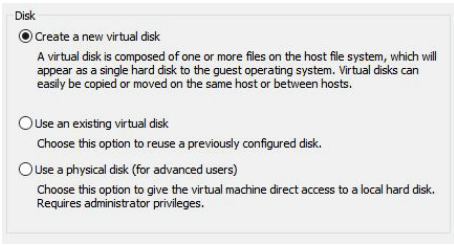
c. Select a disk type.

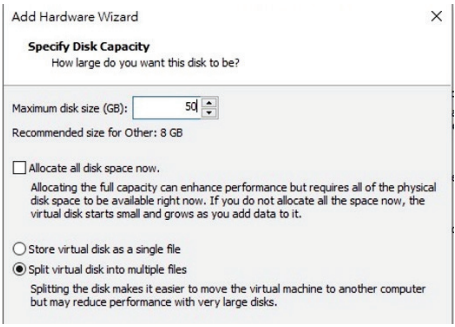
d. Specify the disk size. You can decide the external disk size depending on the number of logs you want to store, as shown in the table below.

Number of Logs	Disk Size
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 need to be stored, 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.





e. Select path to store the disk.
f. Click **OK**.

7. **(Optional)** Adjust the resource configuration of your SDC instance based on the following sizing table or use the default settings (8 CPU cores, 16 GB of memory).

   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. 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 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 on the old SDC.
- The system configuration set from the old SDC including its license, accounting information, and security policies.
- The security event logs stored by the old SDC.

Procedure

1. Launch the new instance of SDC. (For more details, see "Deploying the Security Dashboard Console" under "Installing SDC on a VMware Workstation".)
2. Power off the old SDC.
3. Attach the external disk of the old SDC to the new SDC.
4. A pop-up window will appear. Select which settings and data will be migrated to the new SDC. Once confirmed, the selected data of the old SDC will be migrated over to the new SDC.

Installing SDC on a VMware ESXi System

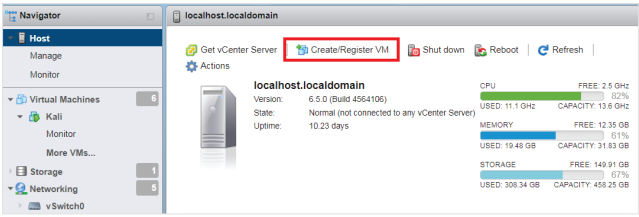
This chapter describes how to deploy the Security Dashboard Console on a VMware ESXi system.

Requirements

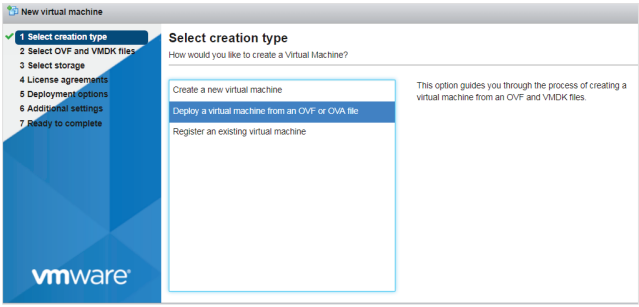
- The OVA packages provided by Moxa must be available and accessible to VMware ESXi.
- ESXi version 6 or above with the required specifications.
- The necessary networks have been properly created in ESXi.

Deploying the Security Dashboard Console

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

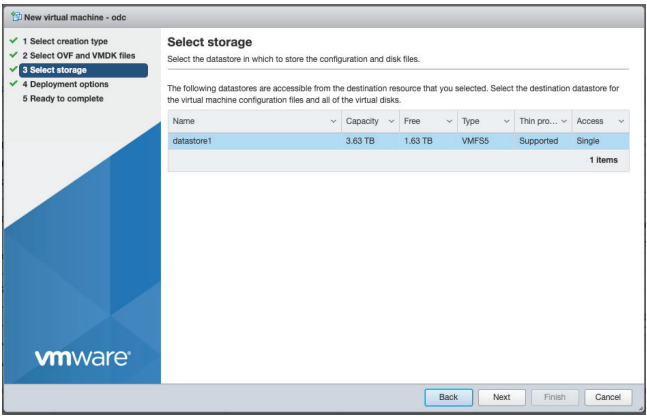


3. Select **Deploy a virtual machine from an OVF or OVA file**.

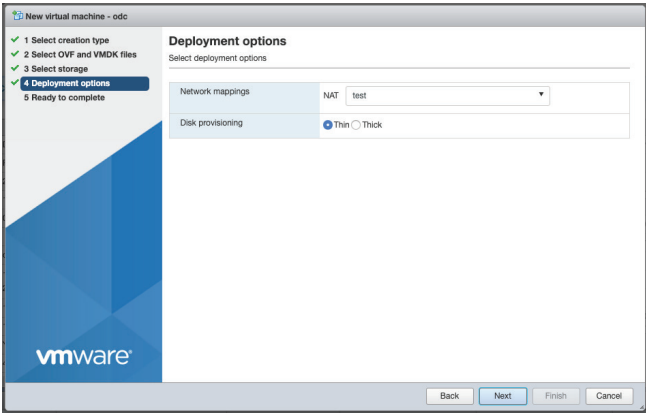


4. Enter a name for your SDC instance and then select the SDC image to upload.

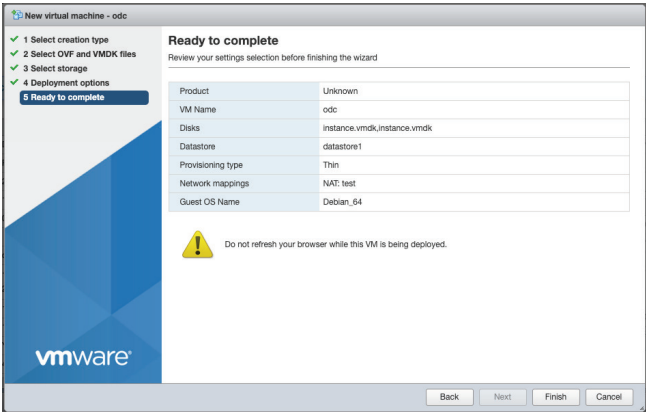
5. Choose a storage location for the SDC virtual machine.



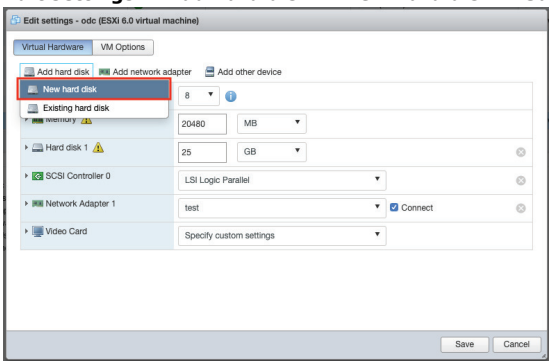
6. Select the deployment options.

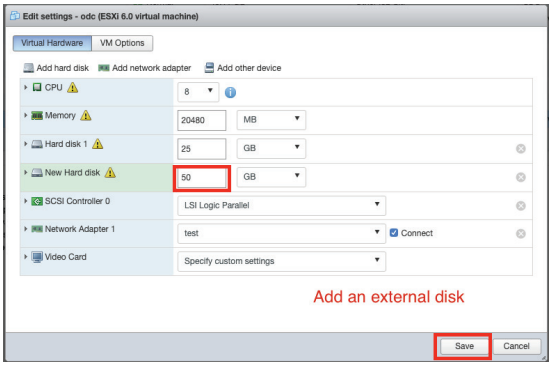


7. When you see the **Ready to complete** screen, click **Finish** to start the deployment.



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** → **New hard disk** → **Save**.





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

Number of Logs	Disk Size
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:
      i. Power off the SDC instance.
      ii. Enlarge the external disk size to fit the maximum log requirement.
      iii. Power on the SDC instance.
   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 of at least 50 GB or higher, otherwise the SDC will not finish initialization and will be unable to complete the boot 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 here instead of adding a new disk if you want to migrate the previous configurations and logs to the new SDC instance.

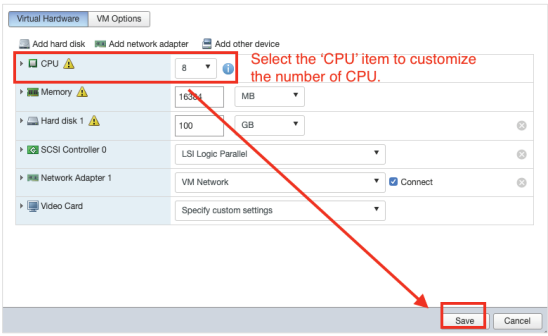
ATTENTION

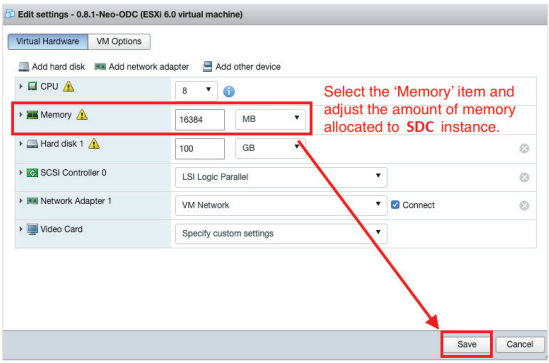
Due to software architecture changes, SDC v1.0 and v1.1 are not fully compatible. If you are migrating from SDC v1.0 to v1.1, we highly recommend attaching a new external drive and not use the old drive. Refer to the ***System Migration*** section for more information.

10. Power on the VM.
11. **(Optional)** Adjust the resource configuration of your SDC instance based on the following sizing table or use the default settings (8 CPU cores, 16 GB of memory).
    a. Shut down the SDC instance and click **Edit**.
    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.

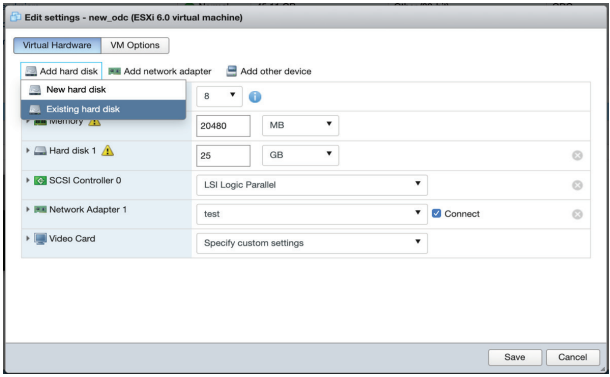
When a new version of SDC is released, the settings of the old SDC can be migrated by attaching the external disk of the old SDC to the new SDC VM. The settings that will be migrated to the SDC include:

- 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 on the old SDC.
- The system configuration set from the old SDC including its license, accounting information, and security policies.
- 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 ESXi".)
2. Power off the old SDC.
3. Attach the external disk of the old ODC to the new SDC.

4. Add the external disk by taking the following steps: **Actions → Edit settings → Add hard disk → Existing hard disk → Save**.

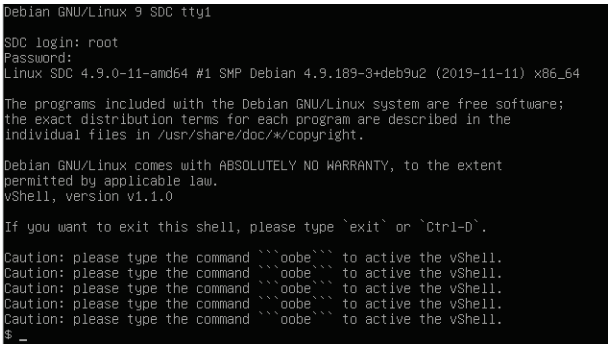


5. The old SDC's information will be migrated over to the new SDC.

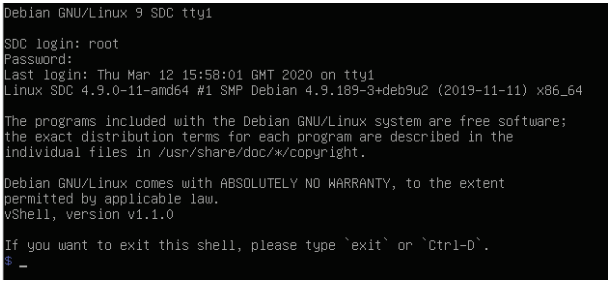
Configuring the SDC system

Accessing the SDC CLI

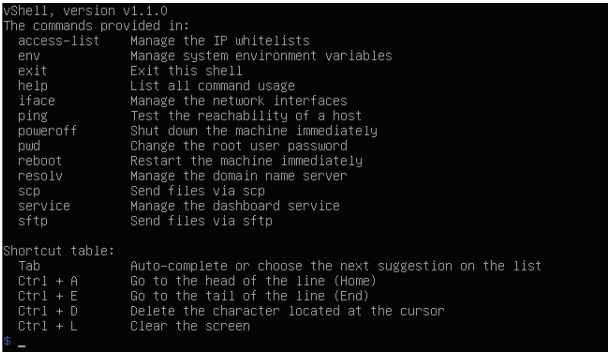
1. Open the SDC VM console.
2. Log in with login **root** and password **moxa**.



3. Change the default password:
   a. Enter the following command:
      ```
      $ oobe
      ```
   b. Change the default password.
   c. Log in to the SDC again with your new password.



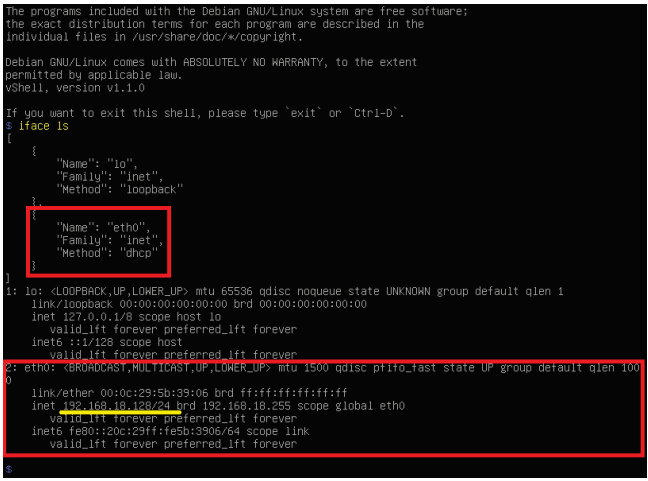
4. After logging in to the SDC, you can enter the “help” command to see a list of available commands for the instance.



Getting the IP Address of the SDC Instance

1. Enter the following command:

   ```
   $ iface ls
   ```



2. If your VMware network adapter is configured to NAT, set up port forwarding rules and specify the NAT outbound IP to allow traffic to pass from the EtherCatch and EtherFire Series to the SDC:
   a. Set up port forwarding rules. Click **Edit → Virtual Network Editor** and select the right network subnet. Click **NAT Settings** to create the following port forwarding rules:
      i. To access the web management console:

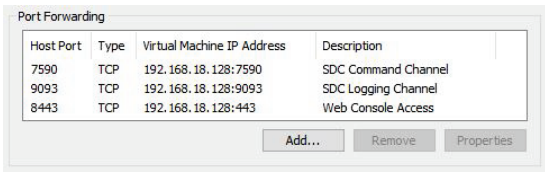
Host Port	Type	VM IP:Port
8443	TCP	[SDC server IP]:443

      ii. To allow users to configure the EtherCatch Series through the SDC including all configuration settings and commands:

Host Port	Type	VM IP:Port
7590	TCP	[SDC server IP]:7590

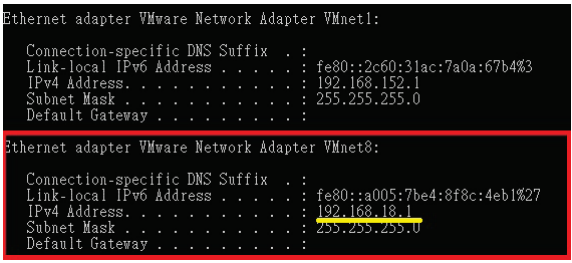
      iii. To allow the EtherCatch Series to upload logs to the SDC:

Host Port	Type	VM IP:Port
9093	TCP	[SDC server IP]:9093



b. Set up the NAT outbound IP address for the SDC environment parameters:

i. Find the NAT outbound IP address of the VM host PC. If your host PC is using Windows, enter "ipconfig" in the command prompt.



ii. Enter 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 the static IP address 10.7.19.157/24 with the gateway IP address 10.7.19.254:

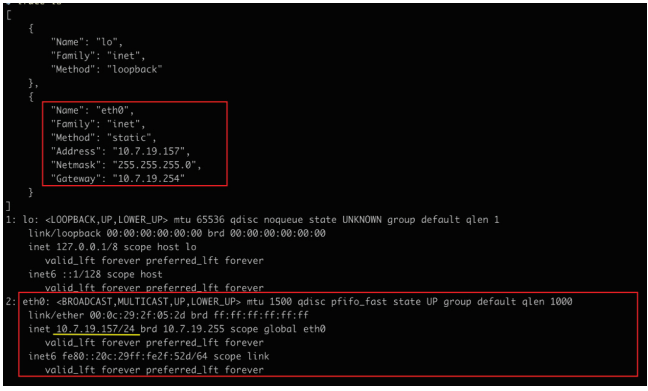
   ```
   $ iface update eth0 --method static --address
   10.7.19.157  --netmask 255.255.255.0 --gateway
   10.7.19.254
   ```

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

   ```
   $ iface restart eth0
   ```

3. Enter the following command to view the network interface settings:

   ```
   $ iface ls
   ```



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

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

   ```
   $ resolv ls
   ```

6. Open the TCP and UDP communication ports below to allow EtcherCatch and EtherFire Series devices to communicate with SDC.

Service	TCP	UDP	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

7. 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 compatible devices. You can access 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

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 will appear.

2. Enter your username 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 screen will appear.

NOTE You must change the default login name and password after logging in for the first time before you can access the management console.

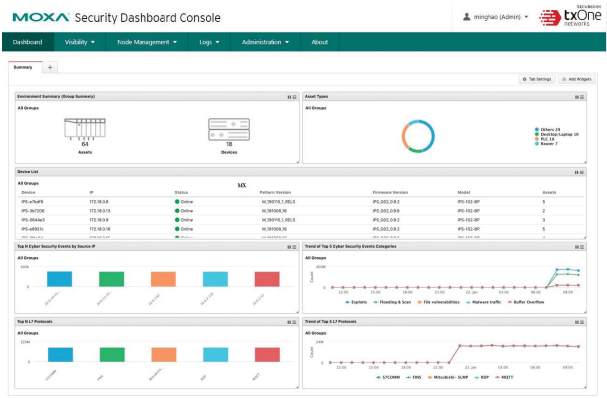
NOTE The new login name cannot be "root", "admin", "administrator" or "auditor" (case-insensitive).

a. Update the login credentials:
   - 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.



Registering EtherCatch and EtherFire Devices to SDC

NOTE The user interface image is for reference only. The instructions are identical for both EtherCatch and EtherFire Series devices.

1. In the web console of the EtherCatch or EtherFire device, go to **Administration → Sync Settings**.
2. Click the **Enable SDC Management** toggle.
3. Enter the SDC IP address.
4. Click **Save**.