Security Dashboard Console Quick Installation Guide

(for VMware Workstation and ESXi)

Version 1.0, May 2020

Technical Support Contact Information www.moxa.com/support

<u>Moxa Americas</u>: Toll-free: 1-888-669-2872 Tel:1-714-528-6777 Fax: 1-714-528-6778

<u>Moxa Europe</u>: Tel:+49-89-3 70 03 99-0 Fax: +49-89-3 70 03 99-99

<u>Moxa India</u>: Tel: +91-80-4172-9088 Fax: +91-80-4132-1045 <u>Moxa China (Shanghai office)</u>: Toll-free: 800-820-5036 Tel:+86-21-5258-9955 Fax: +86-21-5258-5505

<u>Moxa Asia-Pacific</u>: Tel:+886-2-8919-1230 Fax: +886-2-8919-1231



© 2020 Moxa Inc. All rights reserved.

P/N: 18020000A020

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).
- 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**.
- 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. (More information can be found in the "Installing SDC on a VMware Workstation" section.)
 - a. Click Edit virtual machine settings
 - b. Click Add, then choose Hard Disk

Add Hardware Wizard		×
Hardware Type What type of hardware do	you want to install?	
Hardware types:	Explanation	
Hard Disk G CD/DVD Drive Floppy Drive Vetwork Adapter G USB Controller J Sound Card Derailel Port Parallel Port Printer G Generic SCSI Device	Add a hard disk.	

c. Select a disk type

● SCSI	(Recommended)
OSATA	
○ NVMe	
💭 NVMe	devices are not supported on Workstation 11.x virtual machines.

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



a ×
ity I want this disk to be?
50
ther: 8 GB
now.
acity can enhance performance but requires all of the physical able right now. If you do not allocate all the space now, the all and grows as you add data to it.
single file
ultiple files
es it easier to move the virtual machine to another computer mance with very large disks.
rcoulou ou pailina a m ko

e. Select path to store the disk

f. Click OK

 (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	16 GB
200	8 cores	16 GB

- a. Click Edit virtual machine settings.
- b. Configure the amount of memory.
- c. Configure the number of CPU cores.
- (Optional) Change the network adapter setting from 'NAT' to 'Bridged'.
 - a. Right click the SDC VM icon and select **Settings**.
 - 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

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

- 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.

 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 Navigator, 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.

1 New virtual machine - odc						
✓ 1 Select creation type ✓ 2 Select OVF and VMDK files ✓ 3 Select storage ✓ 4 Deployment options 5 Ready to complete	Select storage Select the datastore in which to store the conflip The following datastores are accessible from the the virtual machine configuration files and all of	guration and disk e destination res the virtual disks	k files. source that you :	selected. Select	the destination	datastore for
	Name ~	Capacity ~	Free ~	Type ~	Thin pro \sim	Access ~
	datastore1	3.63 TB	1.63 TB	VMFS5	Supported	Single
						1 items
vm ware						
			Back	Next	Finish	Cancel

6. Select deployment options.

쓥 New virtual machine - odc							
 ✓ 1 Select creation type ✓ 2 Select OVF and VMDK files ✓ 3 Select storage 	Deployment options Select deployment options						
4 Deployment options 5 Ready to complete	Network mappings	NAT	test			•	
	Disk provisioning	 Thir 	Thick				
VIIIvvale							
				Back	Next	Finish	Cancel

7. 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 	Ready to complete Review your settings selection before fini	ishing the wizard
4 Deployment options 5 Ready to complete	Product Mame	Unknown
	Disks	instance.vmdk,instance.vmdk
	Datastore	datastore1
	Provisioning type	Thin
	Network mappings	NAT: test
	Guest OS Name	Debian_64
	Do not refresh your brown	ser while this VM is being deployed.
vm ware [®]		
		Back Next Finish Cancel

- 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.
- 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.

Add hard disk. Will Add network add Add hard disk. Will Add network add Image: Image of the add the add network add Image of the add th	apter Add of 8 V (1) 20480 25 50 LSI Logic Para	MB GB GB	•			
Add hard disk Mill Add network add CPU ▲ Mill Add network add Mill Network Addpter 1	apter Add a 8 • (i) 20480 25 50 LSI Logic Para	MB GB GB	• •			
	8 V (i) 20480 25 50 LSI Logic Pare	MB GB GB	• •			
	20480 25 50 LSI Logic Para	MB GB GB	• •			
Hard disk 1 Hard disk 1 New Hard disk SCSI Controller 0 Metwork Adapter 1	25 50 LSI Logic Pare	GB GB	•			
Aww Hard disk A SCSI Controller 0 Metwork Adapter 1	50 LSI Logic Para	GB	•			0
SCSI Controller 0	LSI Logic Para					0
Retwork Adapter 1		mer		۲		0
	test			٠	Connect	0
Uideo Card	Specify custor	m settings		•		
dit settings - odc (ESXI 6.0 virtual ma rtual Hardware VM Options	achine)				Save	Cancel
Add hard disk Ma Add network add	apter 🔚 Add (
New hard disk	8 7 🚯	other device				
Existing hard disk	8 🔻 🚺	MB	T			
New hard disk Existing hard disk wemany 42 Hard disk 1	8 V () 20480 25	MB GB	• •			0
New hard disk Existing hard disk wemuly Hard disk 1 G SCSI Controller 0	8 V () 20480 25 LSI Logic Para	MB GB	•	•		0
	8 V (1) 20480 25 LSI Logic Para test	MB GB	• •	T	Connect	0

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.
- (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.
- 10. 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).
 - 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	16 GB
200	8 cores	16 GB

Virtual Hardware VM Options	idapter 🛛 🚍 Add other device	
> 🖬 CPU 🛕	Select the 'CPU' item to customize the number of CPU.	
Memory A	16334 MB 🔻	
Hard disk 1 A	100 GB 🔻	٢
SCSI Controller 0	LSI Logic Parallel	٢
Network Adapter 1	VM Network 🔻 🗹 Connect	۲
Video Card	Specify custom settings	
	\sim	
	Save	Cancel

🕨 🖬 CPU 🧘	8 🔻 🚺	Select the 'Memory' item and
Memory <u>A</u>	16384 MB	adjust the amount of memory allocated to SDC instance.
🕨 🚍 Hard disk 1 🧘	100 GB	*
SCSI Controller 0	LSI Logic Parallel	•
INTERPORT Network Adapter 1	VM Network	🔻 🗹 Connect 🛛 🚳
Video Card	Specify custom settings	· ·

System Migration

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.

New hard disk	8 -	0				
memory 4	20480	MB	•			
• 🚍 Hard disk 1 🧘	25	GB	¥			\otimes
SCSI Controller 0	LSI Logic	Parallel		•		0
RE Network Adapter 1	test			•	Connect	0
Video Card	Specify cu	istom settings	1	•		

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 active the vShell.

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

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

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

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

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

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

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

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

3. Change the default password

- a. Type the following command to change the default password $\ensuremath{\$}$ 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 `Ctr1-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.

vsnell, version v	/1.1.0
The commands prov	/ided in:
access–list	Manage the IP whitelists
	Manage system environment variables
	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
	Send files via scp
service	Manage the dashboard service
sttp	Send tiles via sttp
Phonetowet toblog	
Tab	Auto-complete on choose the next suggestion on the list
Ptp1 + A	Co to the head of the line (Nome)
Ctrl + F	Go to the tail of the line (Fod)
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.
 - \$ iface ls



- 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:
 - 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:
 - To access a web management console, forward packets from host TCP port 8443 to the SDC server IP TCP port 443.
 - 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	Туре	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
 - Find the NAT outbound IP address on the VM host PC. If your host PC is using Windows, you can type "ipconfig" to find your Ethernet or Wireless adapter Interface IP.
 - 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.

 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:

 Use the "resolv add" command to add a DNS server and "resolv Is" 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
```

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

```
$ resolv ls
```



- 6. 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

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 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 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.

	occurrey	Basiliboara e	onsore				-	network
shboard N	isibility •	Node Management 👻	Logs 💌	Administration •	About			
nnay +								0 Tel: Serrings (2 Aor Wog
invironment Summary (Dr	oop Bummary)				Asset Types			
Li Greups					All Groups			
	64 Assets		0 0 1	3		C)	Others 29 Ones 29 Overbace, Laptop 10 P(C18 Reador 7
evice Lini								
.A Groups				MX				
Device		Statu		Pattern Version		Firmware Torsion	Model	Assets
175-47649	172.16.0.8	• 0+	ine	NUMPERAL PROF		P5.002.09.2	P5-132-8P	5
P5-367206	172.16.0.13	• Or	ine	M_391008_36		P5.002.09.6	P5-132-8P	2
PS-0544e3	172.160.9	• Or	ine	M.39976J.J.RD.5		P5.502.09.2	P5-192-8P	3
IPS-e0925c	172.16.0.18	• Or	ine	M.391008.36		P5,002,09.2	P5-102-02	5
		• ^-					AA 111 AA	
vp N Cyber Security Even	a by Source IP				frend of fop 5 Cyber Ser	curity Eventa Categories		
cii Cessupo					All Groups			
430b					4004			
					1			
and the second	1.75		3	.9	12.00	15.00 18.00	20.00 22.3m 80.0	0 BE 00 EX 00
12.	44	11	at.	and a	+	Explaits - Rooding & Scan - File	vulsesabilities 🛥 Malware traffic	- Buffer Overflow
og H L7 Protocols					Trend of Tap 5 L7 Protos	uta		
II Groups					All Groups			
325M					244			
					1		/	
							. /	

Register IEC-G102-BP devices to SDC

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

MOXA' EtherCatch									
System	Visibility *	Device •	Object Profiles *	Security •	Pattern •	Logs 💌	Administration 🔻	About	
dministra	ation > Sync Set	tings							
SDC Set	ttings								
C Er	nable SDC Mana	igement							
SDC Se	SDC Server Address 192.168.127.12								
SDC S.	inc Connected								