SD4002
Quick Start Guide

Thank you for purchasing the SD4002 console server. This Quick Start walks you through installation, configuration and local operation. More details are available in the *User Manual* which can be downloaded from *http://opengear.com/documentation*.

Step1   Check kit contents

SD4002
console server

UTP cables (2) and DB9F-RJ45S
straight and cross-over

12VDC
power pack

Step 2   Connect the hardware

➢ Attach the four rubber feet to the base (unless SD4002 is to be DIN rail mounted)

➢ Plug the power pack into the AC mains and connect the DC power cable to the *9V 12VDC* power socket on the SD4002 (Alternately the SD4002 can be powered from any +9V DC to +48V DC power source. Connect these power lines to the IN-GND and IN-VIN+ screw jacks)

➢ Connect the SD4002 *LAN* port to your network

➢ Connect your serial devices to the two serial ports

o Port 1 is a dedicated RS232 port with DB-9 male pinout. With the 319018 RJ adapter you can connect to a Cisco RJ-45 serial console using the UTP cable. With the 319018 + UTP + 319017 you can connect to any appliance with a DB9 male serial console.

o Port 2 can be software configured to be either an RS232 port (which uses the Port 2 DB-9 connector) or an RS422/ RS485 port (which uses the TX+/TX- and RX+/RX- pairs on the terminal block):

1	2	3	4	5	6	7	8
+V DC IN	GND	RX+	RX-	TX+	TX-	+3.3V DC OUT	GND

Step 3   Set up the console server

The default console server IP address is *192.168.0.1* (subnet mask *255.255.255.0*). With a web browser on any computer that is LAN connected to the console server:

> ➢ Enter **https://192.168.0.1** into the address bar

Note: The LAN connected computer must have an IP address in the same network range (192.168.0.xxx) as the console server. If this is not convenient, you can use the *ARP Ping* command to set the IP address (refer *User Manual* or online FAQ for details). The console server also has its DHCP client enabled by default, so it will automatically accept any network IP address assigned by any DHCP server on your network – and will then respond at both 192.168.0.1 and its DHCP address.

> ➢ Log in using the default system user name *root* and the default password *default,* a **Welcome** screen listing the basic configuration steps is displayed

> ➢ Select **System: Administration**, enter and confirm a new **System Password** and click **Apply**

> ➢ To assign your console server a static IP address or to permanently enable DHCP, select **System: IP** then **Network Interface** and check **DHCP** or **Static** for **Configuration Method**

Step 4   Configure serial & network devices

> ➢ Select **Serial & Network: Serial Port** to display the label, mode and protocol options currently set for the serial port – by default, the two serial ports are set to Console Server mode (refer the *User Manual* if other modes are required)

> ➢ To configure a serial port, click **Edit**

> ➢ Configure the **Common Settings** (Baud Rate, Parity, Data Bits, Stop Bits and Flow Control) to match those of the device being controlled
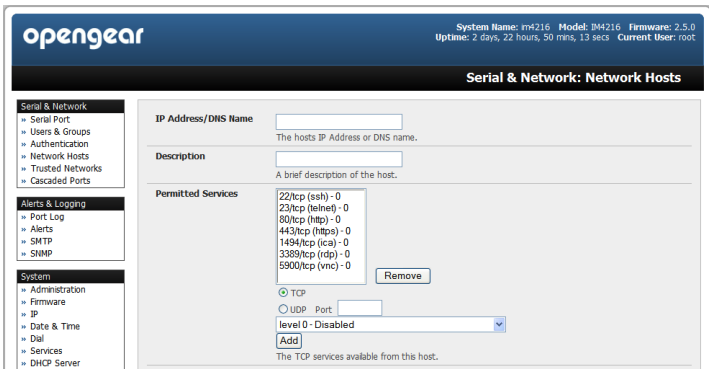

- ➢ Select the **Console Server** protocols (Telnet, SSH, TCP and RFC2217) that are to be used for the data connection to the serial port

- ➢ A **Logging Level** may also be set to specify the level of information to be logged and monitored for the serial port

---

Note: On Port 1 you will be presented with the option to configure the port for modem access. So if you plan to use out-of-band (OoB) dial-in access connect this serial port to an external modem

---

- ➢ Click **Apply**

- ➢ To enable access through the console server to a locally networked computer (referred to as a *host*), select **Serial & Network: Network Hosts** and click **Add Host**

opengear

System Name: im4216 Model: IM4216 Firmware: 2.5.0
Uptime: 2 days, 22 hours, 50 mins, 13 secs Current User: root

Serial & Network: Network Hosts

Serial & Network
» Serial Port
» Users & Groups
» Authentication
» Network Hosts
» Trusted Networks
» Cascaded Ports

Alerts & Logging
» Port Log
» Alerts
» SMTP
» SNMP

System
» Administration
» Firmware
» IP
» Date & Time
» Dial
» Services
» DHCP Server

IP Address/DNS Name
The hosts IP Address or DNS name.

Description
A brief description of the host.

Permitted Services
22/tcp (ssh) - 0
23/tcp (telnet) - 0
80/tcp (http) - 0
443/tcp (https) - 0
1494/tcp (ica) - 0
3389/tcp (rdp) - 0
5900/tcp (vnc) - 0   [Remove]

⊙ TCP
○ UDP   Port
level 0 - Disabled
[Add]
The TCP services available from this host.

- ➢ Enter the **IP address/DNS Name** of the host

- ➢ Edit the **Permitted Services** used for accessing this host, e.g. HTTPS (TCP port 443), VNC (TCP port 5900), or add custom TCP or UDP port numbers – only the services specified here are tunneled through to the host, all other services are blocked

- ➢ At this stage you may also specify the level of information to be logged and monitored for each host access

- ➢ Click **Apply**

Step 5   Add new users

Note: It is recommended that you set up a new Administrator user (in the *admin* group with full access privileges) and login as this new user for all ongoing administration functions (rather than continuing as *root*).

- ➢ For each new user, select **Serial & Network: Users & Groups** and click **Add User**

- ➢ Enter a **Username** and confirmed **Password**, and nominate the **Accessible Hosts** and **Accessible Ports** the user is allowed to access

- ➢ To grant limited access to the Management Console, check the *user* **Group**, to grant full access to the Management Console, check the *admin* **Group** – by default the user is granted no Management Console access. Click **Apply**

Step 6 Advanced configurations

The console server offers many more advanced functions including:

- ❖ The **Alerts & Logging: Alerts** facility monitors serial ports, hosts, user logins, UPSes (Uninterruptible Power Supplies), RPCs (Remote Power Controllers such as PDUs and IPMI devices) and EMDs (Environmental Monitoring Devices). A broad selection of trigger events (such data patterns, temperature or battery levels) can be specified. When triggered, a warning email, SMS, Nagios or SNMP alert is sent to a nominated destination.

- ❖ Extensive management of UPSes and RPCs using open source *NUT* and *Powerman* tools. The **Manage: Power** facility enables both administrators and regular users to monitor and control attached PDU power strips, and servers with embedded IPMI BMCs.

- ❖ Historical logs of all communications with serial and network attached devices, system activity, UPS and PDU power status, environmental status, etc. The level of logging is set as ports and devices are configured, **Alerts & Logging: Port Log** allows this history to be saved locally or remotely. Logs can be viewed from the **Status** and **Manage** menus.

- ❖ Other advanced features, such as *Serial Port Cascading*, remote *Authentication*, *Trusted Networks*, *Secure Tunneling*, *Nagios Distributed Monitoring*, the *Command Line* interface – these are covered in detail in the *User Manual*