



IM7208, IM7216, IM7232 & IM7248

Quick Start Guide

Thank you for purchasing the IM7208/16/32/48-2 infrastructure manager. This Quick Start walks you through installation, configuration and local operation. More details are available in the *User Manual*, located at: <http://opengear.com/documentation>

Step 1 Check kit contents

- ❑ **IM7208/16/32/48-2 Infrastructure Manager**
- ❑ **Rack Mount Kit**
- ❑ **2 x Power Cables**
- ❑ **2 x UTP Patch Cables**
- ❑ **4 x Serial Adapters, X2 Pinout Mode:** 319014 DB9F-RJ45 Straight, 319015 DB9F-RJ45 Crossover, 319016 DB9M-RJ45 Straight, Loopback Test Cable
- ❑ **4 x Serial Adapters, X1 Pinout Mode:** 319017 DB9F-RJ45 Straight, 319018 DB9F-RJ45 Crossover, 319019 DB9M-RJ45 Straight, Loopback Test Cable
- ❑ **Wi-Fi SMA Antenna**

Step 2 Connect the hardware

- Power on the infrastructure manager. The -DAC models have dual universal AC power supplies (with automatic failover) built in, that plug into the mains. The -DDC models have dual DC supplies (with auto failover) and external screw connector blocks for connecting to the DC power sources
- Connect the *NET1* port on the infrastructure manager to your network

Note: Your IM7200 has four physical connections that are logically bundled as two network ports (*NET1* & *NET2*). Each network port consists of a 10/100/1000 copper connection (*C*) and a fiber-optic small form-factor pluggable (*SFP*) connection. Only one connection per network port may be active at a time. When no SFP module present, *NET1/NET2 (C)* is active. When an SFP module is plugged in, *NET1/NET2 (SFP)* becomes active and *NET1/NET2 (C)* is immediately deactivated.

- Connect your serial devices to the serial ports numbered *1 – 8/16/32/48*

Note: To use out-of-band (OoB) dial-in access, connect the internal modem to the phone line. To use broadband OoB, connect the access device to *NET2*.

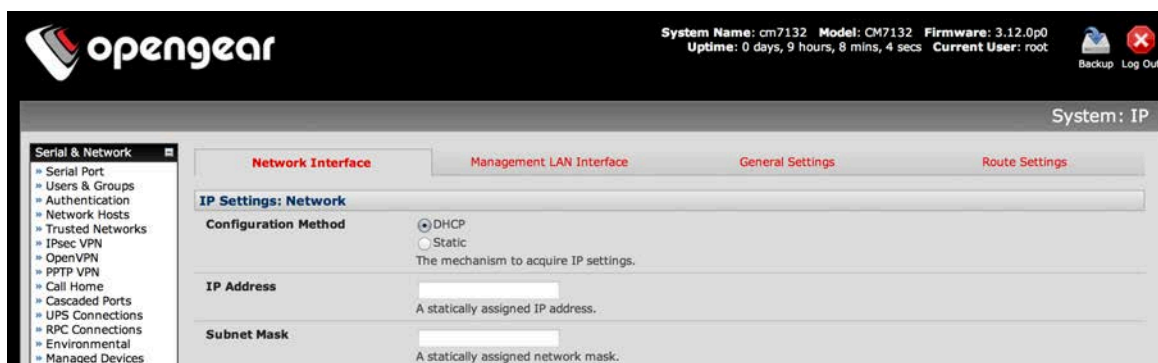
Step 3 Set up the infrastructure manager

The infrastructure manager's default IP address is *192.168.0.1* (subnet mask *255.255.255.0*). With a web browser on any computer that is connected to the infrastructure manager via LAN:

- Enter **https://192.168.0.1** into the address bar
- Log in using the default system user name *root* and the default password *default*, a **Welcome** screen listing the basic configuration steps is displayed

Note: The computer must have an IP address in the same network range (*192.168.0.x*) as the infrastructure manager. Alternatively, you can use the *arping* command to set the IP address (refer to the *User Manual* or online *Knowledge Base FAQ* for details). The infrastructure manager also has DHCP client enabled by default. 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.

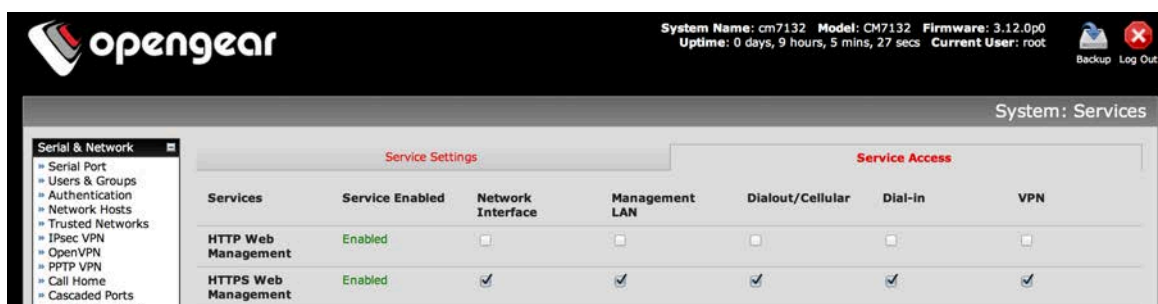
- Select **Serial & Network: Users & Groups** and **Edit** the *Root User*, enter and confirm a new **Password** and click **Apply**
- Select **System: IP** then **Network Interface** and check **DHCP** or **Static** for **Configuration Method**



The second network port (*NET2*) is inactive by default. It can be set up for failover/OoB access (refer to the *User Manual*) or as a management LAN gateway. To activate:

- Select **Management LAN Interface** and uncheck **Disable**
- Enter the **IP Address** and **Subnet Mask** for this segment of the Management LAN (leaving **Gateway** and **DNS** fields blank) – refer to the *User Manual* if you wish to enable the DHCP server or change default firewall/router settings

Note: The built-in firewall determines which protocols and services can be used to access which ports and devices. By default only HTTPS and SSH access is enabled to the infrastructure manager itself. Use the **Service Access** menu on **System: Services** to change settings for the infrastructure manager itself (and for connected serial ports). Similarly using the **Forwarding & Network** menu on **System: Firewall** you can permit IP access between devices on Network or Management LAN.



Alternatively, to use *NET2* as a redundant connection sharing the same network settings as *NET1*:

- Select **System: IP**, choose an **Interface Aggregation** method and click **Apply**

Step 4 Configure serial & USB devices

Note: In the default X2 pinout mode, most RJ45 serial devices connect to the infrastructure manager using a straight UTP patch cable. DTE DB9M and DCE DB9M serial devices connect to the infrastructure manager using the included 319015 and 319014 adapters respectively. Otherwise, for a list of cabling instructions for common devices, refer to the online *Knowledge Base FAQ*.

- Select **Serial & Network: Serial Port** to display the labels, modes and protocol options currently set for each serial port. By default all serial ports are set in *Infrastructure manager* mode (refer to 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

Note: The cabling pinout for each of the RJ45 serial ports can be set to be either X2 (Cisco Straight) or X1 (Cisco Rolled) using **Port Pinout**

- Select the **Infrastructure manager** protocols (SSH, Telnet, Web Terminal and RFC2217) that are to be used for the network connection to that port
- A **Logging Level** may also be set to specify the direction and level of information to be logged for that port
- Click **Apply**
- Your infrastructure manager has two USB ports on the front, which can be used for connecting to USB consoles (on UPS supplies or Cisco devices) or for attaching external USB flash for loading updated firmware or configuration files

Step 5 Add local users & groups

Note: Alternatively, if you wish to use a remote AAA server to authenticate user access, refer to the *User Manual*.

- For each new user, select **Serial & Network: Users & Groups** and click **Add User**
- Enter a **Username** and enter and confirm a **Password**, and nominate the **Accessible Ports** the user is allowed to access
- To grant limited access to the infrastructure manager's management UI and CLI, check the *user Group*, to grant full access to the infrastructure manager's management UI and CLI, check the *admin Group* (by default the user is granted no management access), click **Apply**

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*).

Step 6 Access device consoles

Your infrastructure manager is now ready to serve console access on your network. There are many ways to access device consoles, depending on the protocols chosen.

- *SSH* – for console access using your preferred SSH client (e.g. PuTTY, SecureCRT, OpenSSH):
 - To connect to the *pmshell chooser* menu, SSH to the infrastructure manager and login appending *:serial* to your username, e.g.: *root:serial*
 - To connect directly to a given console, SSH to the infrastructure manager and login adding the port number or port label to your username, e.g.: *root:port02* or *root:MyRouter*
 - To connect directly to a given serial port, SSH to the infrastructure manager at TCP port 3000 + the port number, e.g.: *3002* for serial port 2
- *Telnet* – Telnet to the infrastructure manager at TCP port 2000 + the port number, e.g.: *2002* for serial port 2
- *Web Terminal* – for console access using just your browser, select **Manage: Devices: Serial** and click the port's Web Terminal link

Step 7 Advanced configurations

The infrastructure manager offers many more advanced functions including:

- ❖ The Wi-Fi **System: IP: Wireless Network Interface** is inactive by default. It supports Client or Access Point (WAP) mode, using the provided Wi-Fi antenna.
- ❖ The **Alerts & Logging: Auto-Response** 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 *Check Conditions* (such serial data patterns, temperature or battery levels) can be specified. When triggered, one or more *Trigger Actions* are performed, e.g. a warning email, SMS, Nagios and/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** and *pmshell Power Menu* facility enables both administrators and regular users to monitor and control attached PDU power strips, and servers with embedded IPMI BMCs.
- ❖ Connect EMDs to any serial port (with an adapter) and remotely monitor the temperature, humidity, physical access, smoke alarms, etc. Details are provided in the *EMD5000 Quick Start* supplied with the EMD.
- ❖ Historical logs of all communications with serial and network attached devices, system activity, UPS and PDU power status, environmental status, etc. **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 are covered in detail in the *User Manual*.



Please register your product to activate the warranty and to automatically receive advice of future firmware updates. Go to:

<http://opengear.com/product-registration>