ACM5000
Quick Start Guide

Thank you for purchasing the ACM5000 advanced console server. This Quick Start walks you through installation, configuration and local operation. For more details please refer to the *User Manual* on the CDROM.

Step1 Check kit contents

ACM5000
Console server

UTP cables (2) and DB9F-RJ45S straight (319014) and cross-over (319015)

Quick Start & CDROM

12VDCPower pack

Step 2 Connect the hardware

- Attach the four rubber feet to the base, or attach the mounting bracket
- Plug the power pack into the AC mains and connect the DC power cable to the *PWR* power socket on the ACM5000
- Connect the Ethernet port (*LAN USB1*) to your network. Plug your serial console devices in to the *Serial Ports.* The RJ45 sockets on the ACM5000 use the standard Cisco pin-out

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 network connected to the console server:

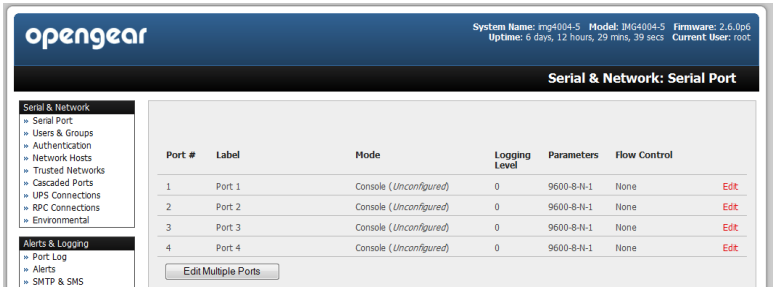
- Enter **https://192.168.0.1** into the address bar

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 DHCP 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

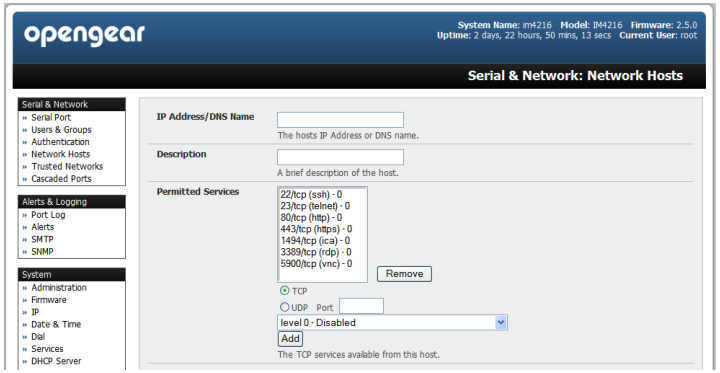
- Log in using the default system user name *root* and the default password *default.* A **Welcome** screen listing the basic configuration steps is displayed
- Select **System: Administration** .Enter and confirm a new **System Password** and click **Apply**
- To assign your console server a static 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 each serial port. By default, Port 1 is set up as a Local Console (enabling command line access) and each other serial port is set in *Console Server* mode (refer the *User Manual* if other modes are required). To configure a particular serial port, click **Edit**



- Configure the **Common Settings** (Baud Rate, Parity, Data Bits, Stop Bits and Flow Control) to match those of the serial console/device being controlled
- Select the **Console Server** protocols (Telnet, SSH, TCP, 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. Click **Apply**
- To enable access through the console server to a locally networked computer or device (referred to as a *host*) select **Serial & Network: Network Hosts** and click **Add Host**

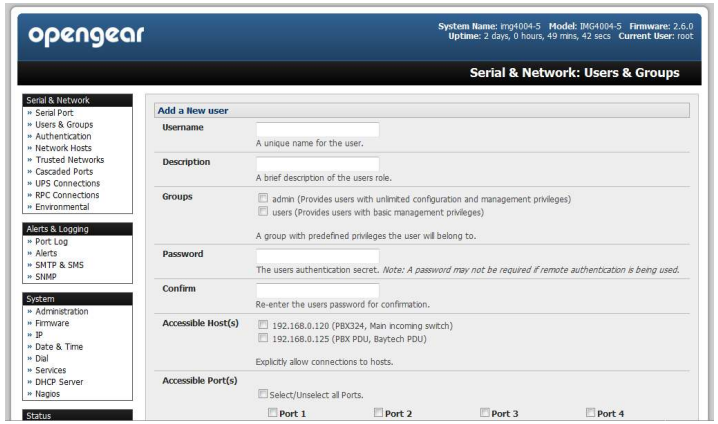


- Enter the **IP address/DNS Name** of the host, and edit the **Permitted Services** used for accessing this host, e.g. HTTPS (TCP port 443), VNC (TCP port 5900), or add custom TCP or UDP port numbers. Only the services specified here are SSH tunneled through to the host. All other services are blocked
- 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**. Click **Add User**
- Enter a **Username** and enter and confirm a **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



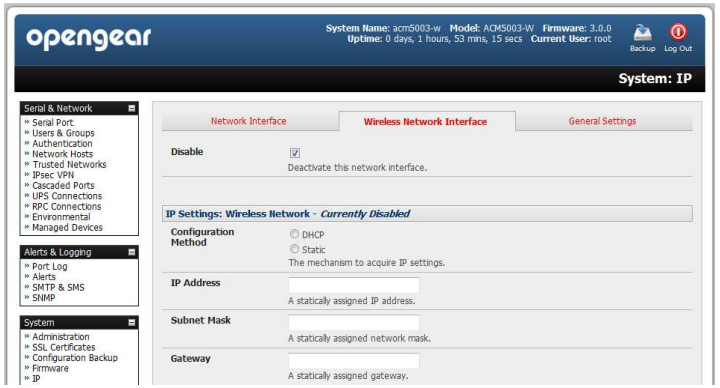
- Click **Apply**

Step 6 Advanced configurations

Note: The ACM5000 family has various models and optional features. Below we cover their configuration and provide introductory notes on some advanced features

- All ACM5000 models have an internal temperature sensor which can be monitored and used to trigger alerts. External EMDs can also be connected to the ACM5000 serial ports. The ACM5000-E models also support the direct connection of external temperature, humidity, physical access, smoke alarms.
- The ACM5003M has an internal modem which can be configured for dial-in access (or dial-out failover connection) using the **Internal Modem Port** tab under **System: Dial**

- The ACM5003W comes with an internal 802.11 wireless modem which can be configured using the **Wireless LAN Interface** menu in the **System: IP** menu. The wireless LAN is deactivated by default and when enabled will operate as the main network connection. Failover is available (though it not *enabled* by default)



Please register your product to activate the warranty and to automatically receive advice of future firmware updates. Go to: *http://opengear.com/product-registration.html*

The ACM5000 also 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 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* on the CDROM.

Note: On the CDROM you will find the *PortShare* and *SDT Connector* software tools.

SDT Connector provides you with secure, point and click access to the console server and all the attached devices

PortShare connects the COM/tty port applications on your Windows PC, Linux server or virtual machine to the serial devices attached to the ACM5000

Refer to the provided *Quick Starts* for details