



QUICK START GUIDE

Remote Site Gateway

Includes: ACM7004-2, ACM7004-2-M, ACM7008-2,
ACM7008-2-M, ACM7004-5



12032018

1. REGISTER

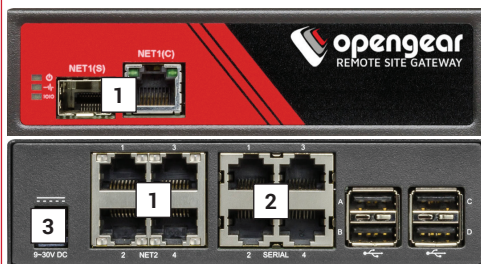
Register your product: <https://opengear.com/product-registration>

For licensing information and access to source code, visit:

<https://opengear.com/software-licenses>

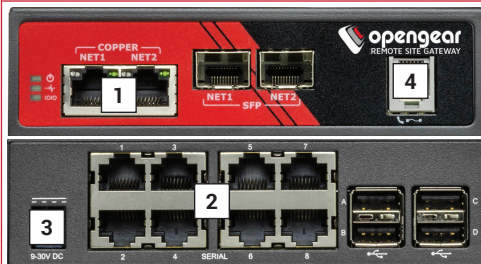
2. WHAT'S IN THE BOX?

ACM7004-5



1. NET1 & NET2
2. Serial Ports
3. Power
4. RJ-11 port

ACM7008-5-M





For the complete list of what's inside the box, visit:

<https://opengear.com/products/remote-site-gateway#inside>



After opening the box:

DO NOT POWER ON RIGHT AWAY

3. ASSEMBLE

If free-standing, attach the adhesive-backed rubber feet. If rack-mounted, attach the rack kit.

If you have an ACM7004-2-M or an ACM7008-2-M, plug an RJ-11 cable into the front-facing RJ-11 port to connect to the built-in V.92 modem.

Connect the NET1 port to your network. The NET2 port is inactive by default. Refer to the User Manual for instructions to activate it.

NOTE: 7004-5 models have a single uplink port 1 x Ethernet/SFP (NET1) as well as a 4-port Ethernet switch (NET2) on the back of the unit.

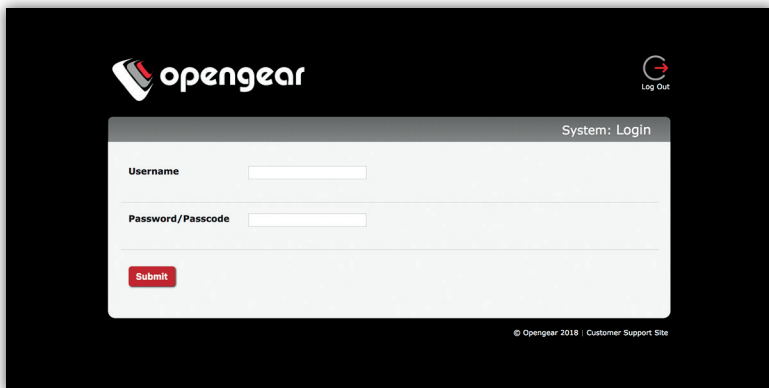
Connect other devices to the serial and USB ports.

Plug in the 12V DC power supply.

4. LOG IN

Browse to **192.168.0.1** (subnet mask 255.255.255.0) with a computer on the same LAN as the console server. The device will also get a DHCP address.

NOTE: The device has a self-signed SSL certificate. Untrusted connection errors appear. Click through the errors to the login page.

The image shows a web browser window displaying the Opengear login page. The page has a dark background. In the top left corner is the Opengear logo, which consists of a stylized 'O' icon followed by the word 'opengear' in lowercase. In the top right corner is a circular 'Log Out' button with a red arrow pointing right. The main content area is a light gray box with a title bar that says 'System: Login'. Inside this box, there are two input fields: 'Username' and 'Password/Passcode'. Below these fields is a red 'Submit' button. At the bottom right of the page, there is a small copyright notice: '© Opengear 2018 | Customer Support Site'.

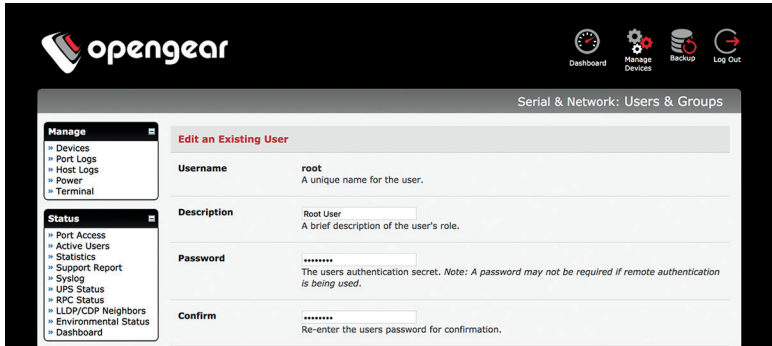
Log in with username **root** and password **default**. Click **Submit**.

The welcome screen appears with a list of basic configuration steps.

5. CHANGE ROOT PASSWORD

Click **Serial & Network > Users & Groups**.

Click Edit next to the root user. On the **Edit an Existing User** page, enter and confirm your new password.



The screenshot shows the OpenGear web interface. The top navigation bar includes the OpenGear logo and icons for Dashboard, Manage Devices, Backup, and Log Out. The main content area is titled 'Serial & Network: Users & Groups'. On the left, there are two expandable menus: 'Manage' (containing Devices, Port Logs, Host Logs, Power, and Terminal) and 'Status' (containing Port Access, Active Users, Statistics, Support Report, Syslog, UPS Status, APC Status, LLDP/CDP Neighbors, Environmental Status, and Dashboard). The main panel displays the 'Edit an Existing User' form for the 'root' user. The form fields are: Username (root), Description (Root User), Password (masked with asterisks), and Confirm (masked with asterisks). A note below the password field states: 'The users authentication secret. Note: A password may not be required if remote authentication is being used.'

Serial & Network: Users & Groups

Edit an Existing User

Username root
A unique name for the user.

Description Root User
A brief description of the user's role.

Password *****
The users authentication secret. Note: A password may not be required if remote authentication is being used.

Confirm *****
Re-enter the users password for confirmation.

Scroll to the bottom of the page and click **Apply**.

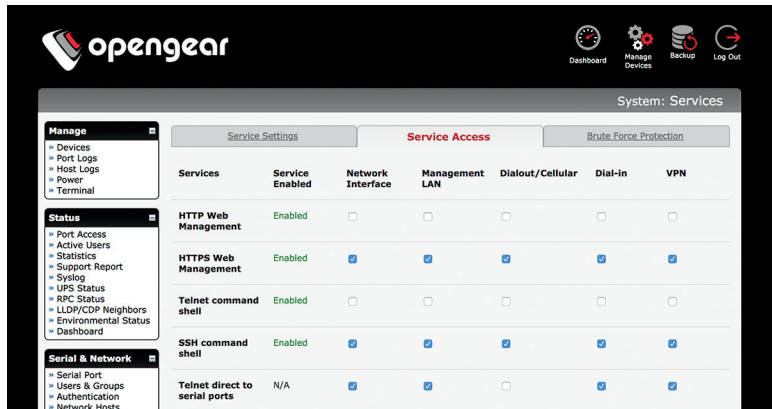
6. OPTIONAL: CHANGE IP SETTINGS

DHCP is enabled by default. If desired, you can set a static IP.

Click **System > IP**. Under the **Network Interface** tab, change the **Configuration Method** to **Static IP**.

7. CHANGE ACCESS & FIREWALL SETTINGS

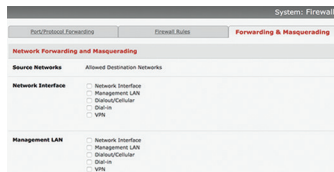
The console server's firewall controls which protocols and services can access which ports and devices. By default, the firewall only allows HTTPS and SSH access. To change settings, click **System > Services** and click the **Service Access** tab.



The screenshot shows the OpenGear console interface. The top navigation bar includes the OpenGear logo and icons for Dashboard, Manage Devices, Backup, and Log Out. The left sidebar contains a 'Manage' section with links to Devices, Port Logs, Host Logs, Power, and Terminal, as well as a 'Status' section with links to Port Access, Active Users, Statistics, Support Report, Syslog, UPS Status, RPC Status, LLDP/CDP Neighbors, Environmental Status, and Dashboard. The 'Serial & Network' section includes links to Serial Port, Users & Groups, Authentication, and Network Hosts.

The main content area is titled 'System: Services' and features three tabs: 'Service Settings', 'Service Access' (selected), and 'Brute Force Protection'. The 'Service Access' tab displays a table with the following columns: Services, Service Enabled, Network Interface, Management LAN, Dialout/Cellular, Dial-in, and VPN.

Services	Service Enabled	Network Interface	Management LAN	Dialout/Cellular	Dial-in	VPN
HTTP Web Management	Enabled	☐	☐	☐	☐	☐
HTTPS Web Management	Enabled	☒	☒	☒	☒	☒
Telnet command shell	Enabled	☐	☐	☐	☐	☐
SSH command shell	Enabled	☒	☒	☒	☒	☒
Telnet direct to serial ports	N/A	☒	☒	☐	☒	☒



The screenshot shows the 'System: Firewall' page with the 'Forwarding & Masquerading' tab selected. The page is divided into two main sections: 'Network Forwarding and Masquerading' and 'Allowed Destination Networks'.

The 'Network Forwarding and Masquerading' section includes a 'Source Networks' table with the following columns: Network Interface, Management LAN, Dialout/Cellular, and VPN.

Source Networks	Management LAN	Dialout/Cellular	VPN
Network Interface	☐	☐	☐

The 'Allowed Destination Networks' section includes a 'Management LAN' table with the following columns: Network Interface, Management LAN, Dialout/Cellular, and VPN.

Management LAN	Management LAN	Dialout/Cellular	VPN
Network Interface	☐	☐	☐

To permit IP access between devices on the network or management LAN, click **System > Firewall**. Click on the **Forwarding & Masquerading** tab, make any changes, and click **Apply**.

8. CONFIGURE NET1 AND NET2

Select **System > IP**.

For NET1, click **Network Interface** and choose either **DHCP** or **Static**.

For NET2, click **Management LAN Interface**. Uncheck **Deactivate this network interface** to activate NET2. For **Configuration Method**, choose **DHCP** or **Static**.

If you choose Static, enter an **IP Address** and **Subnet Mask** for the NET2 interface. If using OOB, these should correspond to your management network.

9. CONFIGURE SERIAL & USB DEVICES

Click **Serial & Network > Serial Port**. Click **Edit** to modify a specific port.

Serial & Network: Serial Port							
Port #	Label	Connector	Mode	Logging Level	Parameters	Flow Control	
1	Port 1	RJ45	SDT (<i>root</i>)	3	115200-8-N-1	None	Edit
2	catalystswitch	RJ45	Console (<i>SSH, Web Terminal</i>)	3	9600-8-N-1	None	Edit
3	Port 3	RJ45	Console (<i>SSH, Web Terminal</i>)	0	115200-8-N-1	None	Edit

You can modify common settings including Baud Rate, Parity, Data Bits, Stop Bits, and Flow Control as well as port connection settings including SSH, Telnet, Web Terminal, and RFC2217.

Click **Apply** to save any modified settings.

10. ADD USERS AND GROUPS

To add a new user, click **Serial & Network > Users & Groups**. Scroll to the bottom of the page and click **Add User**.

Enter a **Username** and enter and confirm a **Password**. Select the appropriate groups and scroll down to choose the **Accessible Ports** the user is allowed to access.

Serial & Network: Users & Groups

Add a New user

Username

A unique name for the user.

Description

A brief description of the user's role.

Groups

☐ admin (Provides users with unlimited configuration and management privileges)

☐ pptpd (Group to allow access to the PPTP VPN server - Users in this group will have their password stored in clear text.)

☐ dialin (Group to allow dialin access via modems - Users in this group will have their password stored

Click **Apply** to create the new user account.

NOTE: You should create a new administrative user rather than continuing as the root user. To do so, add a new user to the **admin** group with full access privileges. Log out and log back in as this new user for all administrative functions.

To create a new group, click **Serial & Network > Users & Groups**. At the end of the list of existing groups, click **Add Group**.

Enter a new group name in the **Groups** field. Select any appropriate **Roles**, **Hosts**, **Ports**, and **RPC outlets**.

Serial & Network: Users & Groups

Add a New group

Groups

A group with predefined privileges the user will belong to.

Description

A brief description of the group's role.

Roles

☐ Full administration & access

☐ Access to all serial ports and managed devices

☐ Web UI access to the 'Manage' pages

☐ CLI connections provide access to the Port Manager shell (This takes precedence over the UNIX Shell Role)

☐ CLI connections provide access to a UNIX shell

Click **Apply** to create the new group.

11. ACCESS DEVICE CONSOLES

Your console server is now ready to access device consoles on your network, depending on the protocols you chose in Step 9.

SSH:

- To connect to the pmshell chooser menu, SSH to the console server and log in appending *:serial* to your username, e.g. *root:serial*.
- To connect to a given console, SSH to the console server 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 port, SSH to the console server at TCP port 3000 + the port number, e.g. 3002 for serial port 2.

Telnet:

Telnet to the console server at TCP port 2000 + the port number, e.g. 2002 for serial port 2.

Web Terminal:

For console access using your browser, click **Manage > Devices > Serial** and click the port's **Web Terminal** link.

LIGHTHOUSE CENTRALIZED MANAGEMENT

Lighthouse is a powerful tool that simplifies the way you manage your out-of-band network through a single pane of glass. Better control and visibility provides 24/7 resilient access to your connected IT infrastructure.

Lighthouse features:

- Centralized scalable administration and automation of nodes
- Easy to maintain user groups and permissions
- Secure accessibility for all connections using Lighthouse VPN
- Responsive UI designed and built for NetOps
- Integrated RESTful API

“Deployment is made very easy as Lighthouse learns about attached devices during node enrollment and will dynamically update itself as new devices attach.”

– Network Computing Magazine Product Review – Dec 2017



Ready to learn more?

Visit lighthouse.opengear.com to download a free evaluation of Lighthouse (up to 5 nodes) and to learn more about Opengear's Centralized Management solutions.