opengear

Resilience Gateway

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

06052019

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-L

ACM7004-2-L

1. NET1 & NET2*
2. Sim Slot 1 & 2
3. Serial Ports
4. CELL (Main)
5. CELL (Aux)
6. Power

*NET2 is the built-in switch on ACM-4-5 units.

For the complete list of what's inside the box, visit:
https://opengear.com/products/acm7000-resilience-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.

Screw the cellular antennas into the CELL (Main) and CELL (Aux) connectors.

By default, the SIM slot 1 is active. Slide your carrier-provided mini SIM into the SIM slot with contacts facing up. *In the CLI and GUI, SIM slot 1 is referencing the bottom SIM slot.*

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 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.

Log Out

System: Login

opengear

Username

Password/Passcode

Submit

© 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.

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 change to 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.

System: Services

Service Settings | Service Access | Brute Force Protection

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	☑	☑	☐	☑	☑

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**.

System: Firewall

Port/Protocol Forwarding | Forwarding & Masquerading | Firewall Rules

Network Forwarding and Masquerading

Source Networks

Network Interface | Allowed Destination Networks

Management LAN

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 (root)	3	115200-8-N-1	None	Edit
2	catalystswitch	RJ45	Console (SSH, Web Terminal)	3	9600-8-N-1	None	Edit
3	Port 3	RJ45	Console (SSH, Web Terminal)	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.

12. CONNECT CELLULAR MODEM

In the Opengear Management Console, select **System > Dial.**

Click the **Internal Cellular Modem** tab. Check the **Allow outgoing modem communication** radio button.

Enter your carrier's Access Point Name in the **APN** field.

If cellular is not the primary network route, you may need to override the provided DNS servers if you have issues with name resolution. Check **Override returned DNS servers** and enter your DNS's addresses.

Click **Apply Modem Dial Settings.**

13. CHECK MODEM STATUS

To check the status of the modem connection:

Select **Status > Statistics.**

Click the **Failover and Out-of-Band** tab.

Make sure the **Always on Out-of-Band -- Internal Cellular Modem's Connection Status** is Connected.

Check the modem's allocated IP Address to see if it is public or private.

You can find more information about cellular features in the Opengear Knowledge Base under the **FAQ > Cellular & Wireless** section:

https://opengear.com/cellular-wireless/

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.