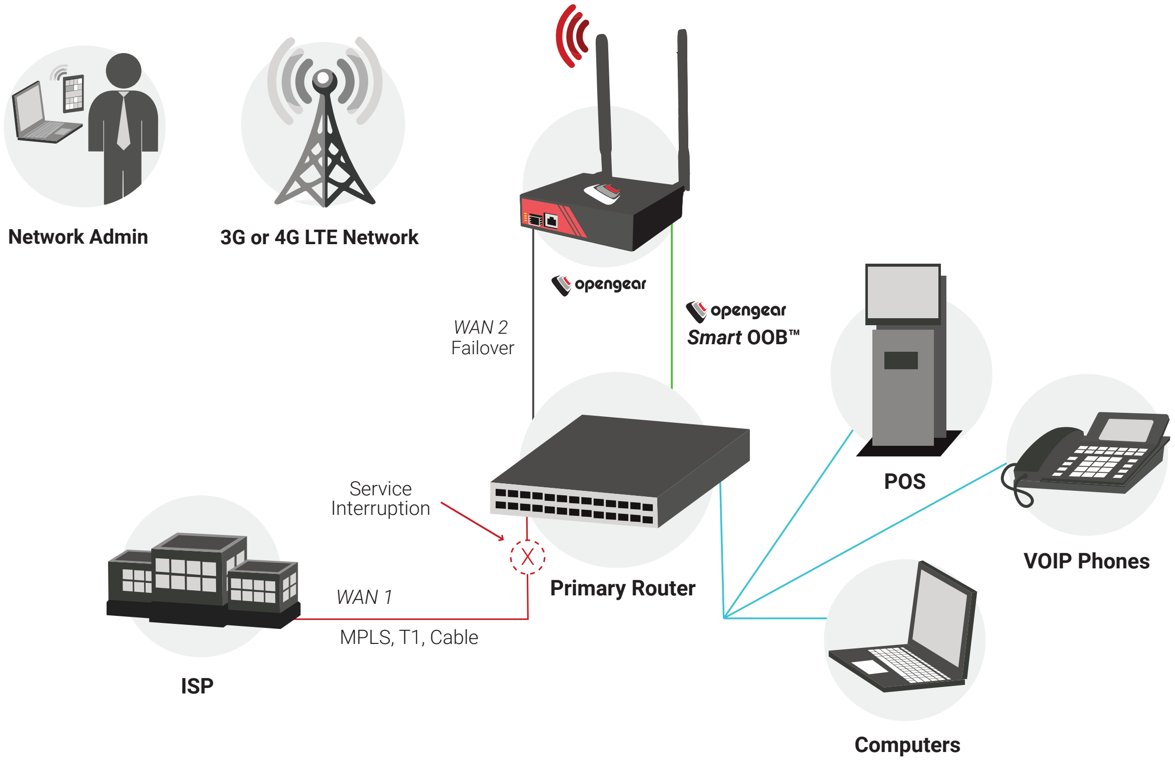
KEEPING YOUR CELLULAR MODEM SECURE

Practical guidelines for keeping your connection safe.

Opengear devices with internal cellular modems give you a wireless broadband IP connection for high-speed access to your remote sites. While this provides you with a number of great benefits, you need to make sure that you address potential security weaknesses right from the start. This paper looks at vulnerabilities and suggests practical ways to help you manage cellular modem security as well as measures to monitor data usage to reduce the risk of data overage charges.

THE OPENGEAR CELLULAR MODEM

Even though it's called a modem, the Opengear cellular modem is quite different from traditional analog dial-up modems. A cellular modem presents a packet-based IP interface that has much in common with a Wi-Fi or Ethernet connection. You access the device via the Internet or private carrier network using standard IP networking. This means that you need to secure your cellular IP connection as you would an IP broadband.



WAYS TO SECURE YOUR CELLULAR IP

If you make your cellular IP address publicly available, operators can open a browser anywhere and type in the IP of their remote Opengear cellular modem and gain access. While this remote access is convenient, it is also available to an attacker.

> You can find out if you have a public IP by clicking **Status > Statistics > Interfaces**. Look at the address of wwan0 (4G models) or dialout0 (3G models).
>
> If this address begins with 192.168.x.x, 10.x.x.x or is between 172.16.x.x and 172.31.x.x, it is not accessible from the public Internet.
>
> If the address is anything else, your cellular IP is probably accessible from the public Internet.

Another approach is to make your cellular IP private, which means you may have to:

- Use Lighthouse or a VPN concentrator to get "reverse" tunnelled access, which requires more setup overhead and introduces a central single point of failure
- Use a carrier or MVNO supplied private network. Keep in mind that this is expensive and frequently unavailable to smaller account holders

This paper presents an overview of a number of options that can help you greatly lessen the security risks to your open cellular IP.

These include:

- Use failover to expose your cellular IP only when you need to
- Configure an admin group account and require strong passwords
- Lock down the firewall
- Restrict inbound connections to VPN client

And while it's not a direct security risk, monitoring cellular data usage is important to keeping the cost of cellular usage under control and can serve as a warning of an attack.

> You could see a massive increase in data usage from worm script trying hundreds or thousands of SSH logins per hour to brute force entry. Or a botnet DDoS could cause a very large spike very quickly.

ONLY USE CELLULAR WHEN NECESSARY

One of the most effective ways to secure a public cellular connection is to keep it disabled when it is not needed. Your Opengear device can automatically turn the cellular connection off when not needed and back on when failover occurs.

Opengear console servers with cellular modems can be configured to use the cellular connection in the case of failover. When the primary network connection encounters a disruption, the console server automatically activates the secondary connection to reestablish inbound and outbound network access. When the primary network connectivity is restored, the console server automatically fails forward to the primary connection and resumes normal operation.

The advantage of this mode is that the cellular connection is completely inactive during normal operation. The goal is to keep the interface off the Internet as much as possible to both avoid high data charges and lessen exposure of this potential target from malicious actors.

For the steps to set up failover for your device's cellular modem, see Cellular Security Best Practices in the Opengear Knowledgebase.

After setting up Failover to Cellular™, you should make sure that you test your system by simulating failover scenarios such as shutting down upstream interfaces or blocking pings to the probe addresses. You should also perform scheduled maintenance tests to further confirm that your cellular connection is working as expected. You can find more details on available failover modes in the Opengear Knowledgebase article, Automatic Failover to Alternate Broadband, Cellular or Dial-Out Internet Connection.

CONFIGURE AN ADMIN GROUP ACCOUNT

You can help lock down access by creating an admin group account with a strong password. Once created, you should then disable the root account. The admin account provides enough access while not allowing a root user with complete control via the cellular IP.

1. Click **Serial & Network > Users & Groups**
2. Scroll down to Users and locate the root user
3. Click **Disable**

PROTECTING USER ACCOUNTS

Additional steps to help secure user accounts include:

- Making sure all users have strong passwords. We recommend that you follow the guidelines provided by the National Institute of Standards and Technology (NIST). The official NIST publication is here, but you may find reading this overview from Auth0 more straightforward

> Two strong random password generation sites you may want to check out are:
>
> http://correcthorsebatterystaple.net/
> https://www.random.org

- Removing *zombie accounts*. These are accounts of users who no longer need access, for example, former employees or users who have changed roles

  The most convenient way to enforce this is using a remote AAA service, in which the Opengear console server offloads authentication to an external server, e.g. TACACS or Active Directory. This can be set up on the Opengear console server software under
  Serial & Network > Authentication

  You can find out how Opengear console servers interact with remote authentication servers to check authorization in the Opengear Knowledgebase article, How Do I Grant Privileges to Remote AAA Users.

- Mandating SSH public key authentication for local users. SSH keys of appropriate type and length (e.g. RSA 2048 bit or longer) are not susceptible to brute force cracking like passwords are, however the private part of the key must be kept secure. For the specific steps to add private keys for users, see Cellular Security Best Practices in the Opengear Knowledgebase

- Enabling brute force protection (fail2ban) for the cellular IP. This limits the number of authentication attempts a user can make before a temporary ban is put in place. You can enable this on the Opengear console server software under
  System > Services > Brute Force Protection

CONSIDER MANDATING VPN

If you are able to avoid using a publicly available cellular modem IP, you should consider restricting inbound connections to a VPN client to secure remote access. This means remote access to the IP is only available through an authenticated and encrypted network tunnel. And if the VPN is configured with strong keys and ciphers, it will be virtually uncrackable.

The trade-off is that that you lose the convenience and minimal configuration of direct SSH, and that a VPN client, or route via a shared VPN tunnel, must be configured at each remote access location.

Please refer to the Opengear Knowledgebase article, Should I Use VPN to Secure My Connection, to learn more about the pros and cons of using VPN for your use cases.

You may want to take the even more secure step of restricting VPN to an outbound tunnel only, such as your central NOC, just as you would do if you had a private IP address.

LOCK DOWN THE FIREWALL

If you are allowing direct inbound connections to your cellular modem IP, you need to take extra care in setting up your firewall. Your first instinct may be to leave everything open and come back later to tighten it up. But it's often the case that you never come back to make these changes. It's best to start with more restrictions than you think you'll need.

You may want to take these steps:

- Disable ping responses. This can help thwart ping sweeps of public address space by attackers seeking targets.
- Disable any unencrypted or insecure services and limit listening ports
- Consider running services on alternate ports to provide some degree of security by obscurity against attacks specifically targeting ports 22 and 443. Use care when changing ports, as this will also affect the ports used for access from internal networks
- Whenever possible, restrict access to trusted source networks only. If you have a known range of addresses, you may block all connections originating from other networks. Refer to the Opengear Knowledgebase article, How Do I Restrict Service Access to Connections From a Trusted Source Network Only, for configuration steps

For specific steps to modify firewall settings for increased cellular IP security, see Cellular Security Best Practices in the Opengear Knowledgebase.

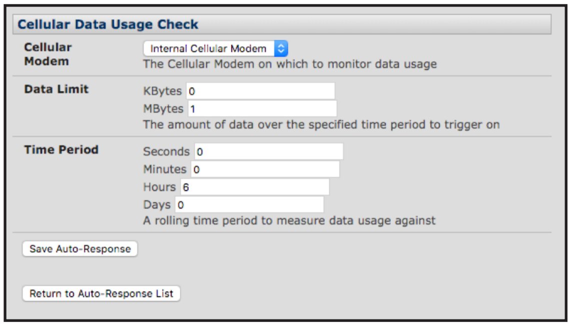
MONITOR DATA USAGE

To use your cellular modem, you'll need to sign up with a cellular carrier and pay for data usage. To avoid having to pay for more than you need, you should make a point of monitoring cellular data usage.

Blocking inbound connections may lower data charges, but you could still see runaway data usage. Things like a misconfigured Opengear console server, connected network host, or **a malicious worm script** may result in unexpected data usage, so you need to monitor data usage in as many ways possible.

To monitor a particular SIM, you can use its unique International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Number (IMEI), which is displayed under **Status > Statistics > Cellular** in the **SIM IMSI** and **IMEI** fields. You may want to make a note of the IMSI and IMEI at the time you deploy your new Opengear console server.

- One way to monitor usage is to take advantage of any data that your cellular carrier has to offer. They may provide automated reports or a portal with feedback on the data usage by your SIM or SIM estate
- The Opengear device itself can be configured to monitor data usage based on the traffic it transmits and receives. Even better, it can send you an alert when it hits a given data limit



Cellular Data Usage Check

Cellular Modem: Internal Cellular Modem
The Cellular Modem on which to monitor data usage

Data Limit:
KBytes 0
MBytes 1
The amount of data over the specified time period to trigger on

Time Period:
Seconds 0
Minutes 0
Hours 6
Days 0
A rolling time period to measure data usage against

For the specific steps to set up an alert when data usage passes a threshold, see Cellular Security Best Practices in the Opengear Knowledgebase

WRAPPING UP

You can feel secure in using your cellular modem by taking a few key steps during installation, including exposing your cellular IP only when you need to, creating an admin group and having users with strong passwords, locking down the firewall, and using a VPN to restrict access.

By doing what you can to keep your cellular modem IP secure and keeping an eye on your cellular modem data usage, you'll be able to take full advantage of the power of your cellular connection.

Be sure to subscribe to our blog for industry updates and best practices