# Hardening and Securing Opengear Devices



## Executive Summary and Purpose

Security is a growing concern in today’s Information Technology (IT) infrastructure. Upper level managers and IT managers alike are held to a higher accountability for the integrity and availability of their data. While host clients and servers often are the focus of security discussions, securing network devices such as switches and routers should not be ignored. All data traverses these devices, and properly securing them is paramount to a stable infrastructure.

This document is intended to inform network administrators about best practices for hardening and securing Opengear devices. For up-to-date product CLI configuration syntax and advanced features, please view product manuals http://opengear.com/manual/Opengear%20User%20Manual.pdf.

Prerequisites: None
Requirements: Version 3.6 firmware and above

## System Configuration

These topics contain operational recommendations that you are advised to implement. These topics highlight specific critical areas of configuration and are not comprehensive.

**Trusted Networks**
You can restrict remote access to serial ports based on the source IP address. Nominate specific IP addresses that trusted users can access from. Further restrictions and settings can be adjusted in the firewall settings.

**SNMPv1/2c vs. SNMPv3**
Opengear devices can use SNMPv3 to ensure secure SNMP messages. SNMPv2 uses community names for read and write access, much like passwords are used for authentication. These community names are sent across the wire as clear text. If a malicious user were to be captured these community names, they could issue SNMP set commands to reconfigure your network device. SNMP version 3 was developed to overcome these weaknesses. It uses asymmetric cryptography to encrypt SNMP traffic over the wire.

**SSL Certificate**
The console server uses the Secure Socket Layer (SSL) protocol for encrypted network traffic between itself and a connected user. The default certificate that comes with the console server device upon delivery is for testing purpose only and should not be relied on for secured global access. It is recommended you generate and install a new base64 X.509 certificate that is unique for a particular console server.

**Firmware Updates**
Periodically the Opengear device will require firmware updates, good policy is to keep current with the latest release. These updates are necessary for one or more of the following reasons: to fix known security vulnerabilities, to improve performance or support new features (perhaps some that allow more advanced security policies).

**Logging**
Interacting with system logs is a crucial aspect of both security and system administration. Monitoring the log files is also key to track down who, when, and where an attacker entered the network. When correlating logs from multiple devices, it is critical to have the time synchronized between them. To do this, you use NTP. If you do not have internal NTP servers, you can use public NTP servers from pool.ntp.org.

**MOTD Banner**
Security experts will advise all networking devices include a MOTD in order to prosecute anyone that may access your systems. The banner message should advise that unauthorized access is prohibited and that if you continue, then you accept that all activities may be monitored and/or recorded. With SSH, a username must be received before a banner message can be displayed.

**Example MOTD:**

> This is a private computer system and is the property of <company name>. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site personnel, law enforcement personnel, as well as authorized officials of other agencies. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized UPS personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning

### FIPS Mode

The ACM5000, ACM5500, IM4200 and IM7200 family of advanced console server families all use an embedded cryptographic module that has been validated to meet the FIPS 140-2 standards. When configured in FIPS mode all SSH, HTTPS and SDT Connector access to all services on the advanced Opengear devices will use the embedded FIPS compliant cryptographic module. To connect you must also be using cryptographic algorithms that are FIPs approved in your browser or client or the connection will fail.

### Services

Opengear devices can be configured to disable unused daemons and services to ensure only the most secure methods of access are available. For the most secure applications users can enable SSH and HTTPS only on each interface for secure, encrypted access.

### Firewall rules

Firewall rules can be used to block or allow traffic through an interface based on port number, the source and/or destination IP address (range), the direction (ingress or egress) and the protocol. This can be used to allow custom onbox services, or block traffic based on policy. Setting firewall rules to allow only permitted inbound traffic is recommended to further secure the Opengear device.

## Serial Port Configuration

### SSH

It is recommended that you use SSH as the protocol where the User or Administrator connects to the console server (or connects through the console server to the attached serial consoles) over the Internet or any other public network. This will provide authenticated SSH communications between the SSH client program on the remote user's computer and the console server, so the user's communication with the serial device attached to the console server is secure.

**Console Server Mode**
Default serial port protocols are all turned off, enable Console Server Mode and check the box for SSH.

**Disable unsecured protocols**
Disable unsecured protocols on each serial port to ensure encrypted access only.
Serial Port Protocols to ensure are *Disabled* when configured for Console Server Mode:

- Telnet
- Raw TCP
- RFC2217
- Unauthenticated Telnet
- Terminal Server Settings
- Serial Bridge Settings

### Serial Port Logs

There are 4 levels of Serial Port Logging in each serial port setting. Determine if serial port logging is a desired function, if so ensure the protection of a clear text password sent across the serial connection to a target device. Best practice is to set the logging level to 4 – Output Logging on Ports +1.

## User Configuration

**Local Authentication**
Local username and passwords are configured on each Opengear device and provide configurable access levels. Local authentication is often used as the secondary login method to provide user access should the primary method fail.

If the primary authentication method fails for any reason, (e.g., the authenticating server(s) are unreachable), the secondary method will be used to authenticate users. Authenticating users via remote user authentication and accounting servers provides a secure and centralized way to manage user access. This allows the administrator to make modifications to the set of authorized users without having to make changes on every Opengear device.

Supported remote user authentication method with primary and secondary options:

- LocalTACACS
- TACACS
- TACACSLocal
- TACACSDownLocal
- LocalRADIUS
- RADIUS
- RADIUSLocal
- RADIUSDownLocal
- LocalLDAP
- LDAP

- LDAPLocal
- LDAPDownLocal
- LocalKerberos
- Kerberos
- KerberosLocal
- KerberosDownLocal

**Change default root System Password**
For security reasons, only the administration user named root can initially log into your console server. So only those people who know the root password can access and reconfigure the console server itself.

**Disable root user**
With a strong password, you can limit your exposure to a brute force attack. However, it may still be possible and the root user name is a common target. Disable the root user and build a new user with admin privileges that will assume the root users permissions. This adds another layer of security because an additional username and password must now be entered before gaining the root user privileges.

**Key based authentication**
SSH pass-key authentication can be used to further secure local authentication. This is more secure than password based authentication. Paste the public keys of authorized public/private keypairs for this user in the Authorized SSH Keys field

Check Disable Password Authentication if you wish to only allow public key authentication for this user when using SSH for even greater security.

## Out-of-band connections

The console server has a number of out-of-band access capabilities and transparent fail-over features, to ensure high availability. So if there's difficulty in accessing the console server through the main network path, all console server models provide out-of-band (OOB) access and the Administrator can still access it (and its Managed Devices) from a remote location

### Dial-in

Opengear devices support both dial-in and dial-out using internal or external modems. Best practice can include dial-back per-user for greater security. In the dial settings page users can enable encrypted authentication (MS-CHAP v2): The strongest type of authentication to use; this is the recommended option.

If CHAP or MSCHAPv2 is selected, the dial-in authentication will be encrypted. However, the traffic itself may not be. Consider using secure protocols (HTTPS/SSH) to access network resources over a dial-in link.

### Cellular 3G & 4G

Opengear devices internal or external cellular connections can enhance security starting with the available carrier data plans. Many carriers offer private IP services such as a machine to machine (M2M) data plans that provide a segmented VLAN assigned to the end user. These private IP options enhance security by limiting exposure to the internet and keep traffic isolated to internal corporate networks.

Cellular interfaces should be treated no different than any other interface and recommended protocols such as IPSec, OpenVPN, SSHv2, HTTPS should be used for access.

**Enable IP Masquerading (SNAT)**
IP Masquerading is used to translate private network traffic onto public networks such as the Internet. This is generally required when using the interface as an Internet gateway.

## VPN

By using a VPN, businesses ensure security -- anyone intercepting the encrypted data can't read it. Opengear devices include several VPN methods to encrypt data:

**OpenVPN**
The ACM5000, ACM5500, IM4200 and IM7200 family of advanced console servers with Firmware V3.2 and later, include OpenVPN which is based on TSL (Transport Layer Security) and SSL (Secure Socket Layer). With OpenVPN, it is easy to build cross-platform, point-to-point VPNs using x509 PKI (Public Key Infrastructure) or custom configuration files.

**PPTP VPN**
The ACM5000, ACM5500, IM4200 and IM7200 family of IM42xx advanced console servers with Firmware V3.5.2 and later, include a PPTP (Point-to-Point Tunneling Protocol) server. PPTP is typically used for communications over a physical or virtual serial link. The PPP endpoints define a virtual IP address to themselves. Routes to networks can then be defined with these IP addresses as the gateway, which results in traffic being sent across the tunnel. PPTP establishes a tunnel between the physical PPP endpoints and securely transports data across the tunnel. The strength of PPTP is its ease of configuration and integration into existing Microsoft infrastructure.

**IPsec VPN**
The ACM5000, ACM5500, IM4200 and IM7200 family of advanced console servers include Openswan, a Linux implementation of the IPsec (IP Security) protocols, which can be used to configure a Virtual Private Network (VPN). The VPN allows multiple sites or remote administrators to access the Opengear advanced console server (and Managed Devices) securely over the Internet.

## Summary

The security features described by this document are an excellent starting point for hardening Opengear devices, and should be used in the context of an organization's greater security policy.