

GLBB GS3SFP-232-GE User Guide

Firmware version 2.0

April 1, 2026

Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 3 |
| 2 | Product Specifications | 5 |
| 3 | Installation Instructions | 7 |
| | Unbox the device | 7 |
| | Connecting the GS3 to your network | 7 |
| | Connecting to the GS3 | 7 |
| | IP Address Configuration | 7 |
| | Determining the link-local IPv6 address via Multicast | 8 |
| 4 | Logging into the GS3 | 9 |
| | SSH Access | 9 |
| 5 | Usage Instructions | 10 |
| | Navigating and displaying the menu | 10 |
| 6 | Serial Commands | 11 |
| | serial connect | 11 |
| | serial show | 11 |
| | serial delay-crlf <0000> | 11 |
| | serial baudrate | 11 |
| | serial datasize <bits> | 12 |
| | serial parity <none/odd/even> | 12 |
| | serial stopbits <bits> | 12 |
| | serial exitkey | 13 |
| 7 | Connecting the GS3 to the Serial Console | 14 |
| 8 | Network Commands | 15 |
| | network show | 15 |
| | network ipv4 <manual/dhcp/disable> | 15 |
| | network ipv6 <auto/random/manual/linklocal/disable> | 16 |
| | network port cli <port> | 17 |
| | network reverse-ssh <port> | 17 |
| | network timeout <timeout> | 17 |
| | network hostname <host name> | 18 |
| | network ntp <remote-ntp-addr> | 18 |
| | network syslog <remote-syslog-addr> | 18 |
| 9 | Security Management Commands | 19 |
| | user list | 19 |
| | user add <username> <password> <admin/regular> | 19 |
| | user change <username> <new password> | 19 |
| | user delete <username> | 19 |
| | user publickey <username> | 19 |
| | session list | 20 |
| | session kill <sessionId> | 20 |
| | ssh config <kex/host-key> | 20 |
| | ssh publickeyonly <enable/disable> | 21 |
| | acl set <ipv4/ipv6> <ip> | 21 |

| | |
|--|-----------|
| acl del <ipv4/ipv6> <listnum> | 21 |
| acl list <ipv4/ipv6> | 22 |
| 10 Firmware Commands | 23 |
| firmware version | 23 |
| firmware upgrade | 23 |
| firmware server <set/get> | 23 |
| reset <defaults/reboot> | 24 |
| 11 Serial Phrase Locator | 25 |
| keyphrase add <key phrase> | 25 |
| keyphrase list | 25 |
| keyphrase del <list num> | 25 |
| A SSH Security Audit Output | 26 |
| B Deployment Example: Detecting a warm reload | 27 |
| C Deployment Example: Detecting a host recovery | 28 |
| D Firmware Releases and SHA256 Hash Values | 29 |

1 Introduction

The GLBB Secure Smart Serial (GS3) is a small form factor console server, purpose-built for secure remote access to a serial device (TIA-232/RS-232). The GS3 uses the latest SSH security protocols to include post quantum key exchange.

Key Features

1. Versatile Connectivity

The GS3 works when inserted into 100Mbps, 1G, and 10G Ethernet SFP/SFP+ ports, offering flexible deployment options to take control of serial ports from an Ethernet network.

2. Converged Management

The GS3 is designed to simplify network management by converging Ethernet and serial port management on the same switch. Dynamically add serial ports, eliminating the need for separate console management devices in fixed configurations. This reduces hardware costs and offers a more environmentally friendly solution.

3. Serial Communication via RJ-45

The RJ-45 connector on the GS3 is exclusively for serial communications to connect to device serial console ports only. Although standard straight-through Ethernet cables are used, only pins 3, 4, 5, and 6 are required for the connection between the managed device and the GS3.¹

4. Simplified IP-Based Serial Management

Each GS3 device is assigned a unique IP address, enabling direct IP-based serial communication management without the complexity of tracking multiple TCP ports. This simplifies the management of serial devices over a converged Ethernet IP network.

5. Enhanced Security and Stability²

The GS3 provides robust security features, including:

- Supports post quantum key-exchange ML-KEM-768
- Support five locally configured users
- Supports SSH login with public key
- Syslog reporting of user logins and session timeouts
- 5 admin but only 4 regular logins for admin control/disconnect
- Permitted SSH client Access Control Lists (ACLs)
- Fully configurable IPv4/IPv6, support random IPv6 addresses
- Less than 60 seconds to upgrade
- Deprecating SSH from the managed device eliminates risk
- Granular configuration of SSH Key Exchange algorithms and Keys
- Priority to the active console session and not new connections
- JumpServer video captures sessions and can restrict commands
- One IP = One serial console for granular security control

¹A standard straight-through Ethernet cable is suitable for an RJ-45 to RJ-45 connection. If custom cables are required, please visit our website: <https://www.glbb.jp/en/hardware/g3/>

²For independent verification of the GS3 SSH security posture, an example `ssh-audit` output is provided in Appendix A.

6. **Firmware Upgradeable and User-Friendly Reset**

The GS3 is firmware upgradeable via SFTP, ensuring currency with the latest features and security updates. You can get the latest firmware from the GS3 site: <https://glbb-japan-odoo-b2c-up.odoo.com/hardware/gs3> If the device's password is forgotten, the GS3 can reset to default settings by removing and re-inserting the RJ-45 interface more than four times in ten seconds while connected to an active serial console, which triggers a simple fail safe recovery mechanism to the default settings.

7. **Operational Features**

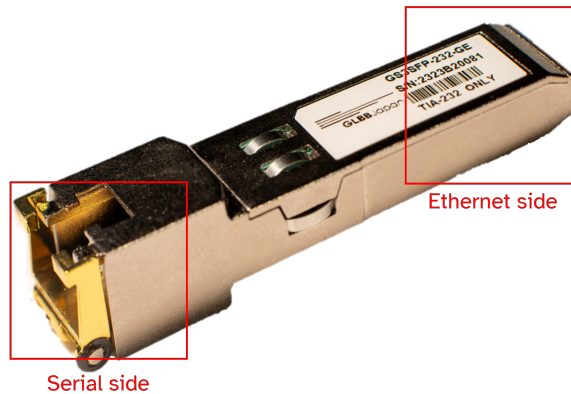
The GS3 supports multiple serial rates and includes a CR/LF transmit delay. The transmit delay can prevent garbled text such as when copy/paste to the management interface via SSH requires delay. Some terminal emulation clients provide a delay setting but not all such as ssh by command line, GS3 can add the delay if necessary.

8. **24/7 Monitoring and Alerts**

The GS3 allows for continuous monitoring of connected devices and can send alerts to one or two configured Syslog servers when specific key phrases, login events, and reloads are detected. For example, a keyphrase of "SYSLOG" would send all syslog messages reported to a console to the syslog server until the end of the line or 100 characters whichever is first.

2 Product Specifications

The GLBB Secure Smart Serial (GS3) is a versatile and secure networking device designed to manage Ethernet and serial communications across both enterprise and service provider environments. It brings together advanced features that meet the complex demands of large-scale deployments and mission-critical applications.



Ethernet Communication

- **SFP & SFP+ Compatibility:** Supports 100Mbps, 1G, and 10G Ethernet through SFP/SFP+ ports.
- **Receptacle:** Follows the SFF-8432 specification³ for small form-factor pluggable modules.
- **Interface:** 20-pin INF-8074i compliant, supporting high-speed Ethernet communication via SFP ports.

Serial Communication

- **Connector:** RJ-45 connector for serial communications.
- **Serial Function:** Supports Reverse SSH for secure remote management of serial devices.
- **Serial Standard:** TIA-232 (RS-232).
- **Supported Baud Rates:** Beyond the standard 9600 and 115200 bps, the GS3 supports a wide range of baud rates, offering flexibility for various service provider and enterprise environments.

Power

- **Maximum Power Consumption:** 0.65W - an energy-efficient choice for environments where power consumption is a concern.

Security and Management

- Supports SSHv2 for secure remote management.
- Permitted SSH client ACLs for enhanced security.

³SFF-8432: Specification for Enhanced Small Form-Factor Pluggable Module (SFP+) and Cage

- Firmware is upgradable via SFTP, with a robust bootloader that safeguards against failed updates.
- DNS and NTP Support: The GS3 supports both DNS and NTP, allowing it to work with NTP pools to ensure accurate timestamps and logs, which are critical for precise event tracking and network troubleshooting.

Certifications

- RoHS, FCC, CE, and VCCI certified, ensuring compliance with environmental and safety standards.

Other Features

- Unique IP address per device for easy management of serial ports over Ethernet.
- Supports up to five locally configured users.
- IPv4 and IPv6 support, including an IPv6 link-local address for recovery.
- Continuous monitoring and alert system via Syslog.
- CR/LF Transmit Delay: This feature helps prevent garbled text during SSH management sessions, especially when pasting large amounts of data to the serial console. Even Ethernet-based SSH sessions can experience data corruption, and some terminal emulators implement a CR/LF delay to mitigate such issues.
- Supports direct access to the serial console via reverse SSH (default TCP port 922), allowing secure inbound connectivity without exposing the GS3 to incoming connections.⁴

⁴Reverse SSH access is enabled by default and can be disabled to restrict access to the CLI only.

3 Installation Instructions

Unbox the device

Carefully remove the GS3 from the package and ensure it includes:

- GS3 Unit
- Quick Start Guide

Connecting the GS3 to your network

- Insert the GS3 module.
- Plug the GS3 into an SFP or SFP+ port on your media converter, router, switch, or other compatible device.⁵ Some 10G SFP+ ports may require manual configuration to set the speed to 1G if auto negotiation does not succeed.
- Verify link status: The link light should activate within a few seconds after inserting the GS3. If the light does not turn on within 10 seconds, verify the connection, as there may be an issue.

Connecting to the GS3

To communicate with the GS3, connect your laptop to the device (e.g., the media converter or switch) where the GS3 is plugged in. Ensure that you are in the same network/broadcast domain.⁶

IP Address Configuration

The GS3 has a default IPv4 address of 192.168.11.11/24, with a gateway address of 192.168.11.1. Configure your laptop's IP address within the 192.168.11.0/24 subnet to communicate with the GS3. You can also connect using the IPv6 link-local address. The default IPv6 link-local address is in EUI-64 format as fe80::8e12:c2ff:fexx:xxxx where "xx:xxxx" is the serial number.

Testing the Connection

After configuring your laptop's IP, test the connection by pinging⁷ the GS3.

Example IPv4 ping:

```
ping 192.168.11.11
```

Example IPv6 ping:⁸

```
ping -6 fe80::8e12:c2ff:fexx:xxxx%interface
```

⁵Please note that SFP28 ports are not supported at this time.

⁶If the GS3 is connected to a router, you may need to first SSH into the router and then SSH from the router to the GS3, unless the router's interfaces are bridged.

⁷On macOS, use the `ping6` command to ping IPv6 addresses.

⁸Replace `%interface` with your network interface (e.g., 20), as IPv6 requires specifying the interface to use for link-local addresses.

Determining the link-local IPv6 address via Multicast

If you do not want to retrieve the serial number directly from the device, you can ping the IPv6 all-nodes multicast address to locate the GS3 on your network:

Example:

```
ping -6 ff02::1%20
```

```
Pinging ff02::1%20 with 32 bytes of data:  
Request timed out.
```

On Windows, the ping response may not appear, but you can view the neighbors using:⁹

```
netsh interface ipv6 show neighbors
```

| Internet Address | Physical Address | Type |
|--------------------------|-------------------|-----------|
| fe80::8e12:c2ff:fe00:253 | 8c-12-c2-00-02-53 | Reachable |
| ff02::1 | 33-33-00-00-00-01 | Permanent |
| ff02::2 | 33-33-00-00-00-02 | Permanent |
| ff02::16 | 33-33-00-00-00-16 | Permanent |
| ff02::fb | 33-33-00-00-00-fb | Permanent |
| ff02::1:2 | 33-33-00-01-00-02 | Permanent |
| ff02::1:3 | 33-33-00-01-00-03 | Permanent |

⁹IPv6 link-local addresses use the EUI-64 format, where the second hexadecimal character "C" is changed to "E", and FFFE is inserted between the modified OUI and the device serial number.

4 Logging into the GS3

SSH Access

Once you confirm that you can ping the GS3, you are ready to log in via SSH. Use a terminal emulator (e.g., PuTTY) or a command-line interface.

The default login credentials are: username `admin`, password `password`.

Example: IPv4 SSH

```
ssh admin@192.168.11.11
admin@192.168.11.11's password:
You are connected to GS-3 SFP Module
The console escape key is CTRL+]
[admin@ssh-to-serial]>
```

Example: IPv6 SSH

```
ssh admin@fe80::8e12:c2ff:fe00:253%20
admin@fe80::8e12:c2ff:fe00:253%20's password:
You are connected to GS-3 SFP Module
The console escape key is CTRL+]
[admin@ssh-to-serial]>
```

5 Usage Instructions

Navigating and displaying the menu

Use the ? command to display the menu (Tab completion is supported).

The menu is divided into the following sections: Serial Commands, Network Commands, Security Management, Firmware Commands, and Serial Phrase Locator Commands.

Example:

```
You are connected to GS-3 SFP Module CLI
The console escape key is CTRL+]
[admin@ssh-to-serial]>?
### Serial Commands
  serial connect
  serial show
  serial delay-crlf <0000>
  serial baudrate <rate>
  serial datasize <bits>
  serial parity <none/odd/even>
  serial stopbits <bits>
  serial exitkey
### Network Commands
  network show
  network ipv4 <manual/dhcp/disable>
  network ipv6 <auto/random/manual/linklocal/disable>
  network port cli/reverse-ssh <port>
  network timeout <timeout>
  network hostname <hostname>
  network ntp <remote-ntp-addr>
  network <syslog1/syslog2> <remote-syslog-addr>
  network reverse-ssh <enable/disable>
### Security Management
  user list
  user add <admin/regular> <username> <password>
  user change <username> <new_password>
  user delete <username>
  user publickey <username>
  session list
  session kill <sessionId>
  ssh config <kex/host-key>
  ssh publickeyonly <enable/disable>
  acl set <ipv4/ipv6> <ip>
  acl del <ipv4/ipv6> <listnum>
  acl list <ipv4/ipv6>
### Firmware Commands
  firmware version
  firmware upgrade
  firmware server <set/get>
  reset <defaults/reboot>
### Serial Phrase Locator Commands
  keyphrase add <key_phrase>
  keyphrase del <list_num>
  keyphrase list
```

6 Serial Commands

The serial commands section provides users with the necessary tools to manage and configure the GS3's serial communication settings. These commands allow users to display the current configuration and adjust settings such as baud rate, data size, parity, stop bits, and transmit delay.

serial connect

Establishes a connection to the serial console.

Example:

```
[admin@ssh-to-serial]>serial connect
Starting serial session...
The console escape key is CTRL+]
```

serial show

Displays the current serial configuration.

Example:

```
[admin@ssh-to-serial]>serial show
UART Config - Base: 0x4000D000
Clock: 120000000 Hz
Baud: 115200
Data Size: 8
Parity: N
Stop Bits: 1
Flow Control: N
Transmit Delay: 100 ms
Current configuration displayed.
```

serial delay-crlf <0000>

Sets the transmit delay, which can range from 0 to 86,400,000 milliseconds (up to 24 hours).

Example:

```
[admin@ssh-to-serial]>serial delay-crlf 300
UART Config - Base: 0x4000D000
Clock: 120000000 Hz
Baud: 115200
Data Size: 8
Parity: N
Stop Bits: 1
Flow Control: N
Transmit Delay: 300 ms
Transmit delay set to 300 milliseconds.
```

serial baudrate <rate>

Sets the baud rate. The default setting is 115200. The minimum value is 1200 and the maximum setting is 115200 bits per second.

Example: The following example configures the serial baud rate to 9600.

```
[admin@ssh-to-serial]>serial baudrate 9600
UART Config - Base: 0x4000D000
Clock: 120000000 Hz
Baud: 9600
Data Size: 8
Parity: N
Stop Bits: 1
Flow Control: N
Transmit Delay: 300 ms
Serial baud rate set to 9600.
```

serial datasize <bits>

Sets the data size for transmission, with a range of 5 to 8 bits.

Example: The following example configures the serial data size to 5 bits.

```
[admin@ssh-to-serial]>serial datasize 5
UART Config - Base: 0x4000D000
Clock: 120000000 Hz
Baud: 9600
Data Size: 5
Parity: N
Stop Bits: 1
Flow Control: N
Transmit Delay: 100 ms
Serial data size set to 5 bits.
```

serial parity <none/odd/even>

Sets the parity mode to None, Odd, or Even.

Example: The following example configures the transmission parity mode to Odd.

```
[admin@ssh-to-serial]>serial parity odd
UART Config - Base: 0x4000D000
Clock: 120000000 Hz
Baud: 9600
Data Size: 5
Parity: 0
Stop Bits: 1
Flow Control: N
Transmit Delay: 100 ms
Serial parity set to 0.
```

serial stopbits <bits>

Configures the number of stop bits (either 1 or 2).

Example: The following example configures the serial stop bits to 2.

```
[admin@ssh-to-serial]>serial stopbits 2
UART Config - Base: 0x4000D000
Clock: 120000000 Hz
Baud: 115200
Data Size: 8
Parity: N
Stop Bits: 2
Flow Control: N
Transmit Delay: 300 ms
Serial stop bits set to 2.
```

serial exitkey

Modifies the key combination used to exit the console session.

Example: The following example sets the exit key to CTRL + A.

```
[admin@ssh-to-serial]>serial exitkey
Press the key you want to use as the exit key...

Exit key set to: CTRL+A
```

7 Connecting the GS3 to the Serial Console

The GS3 functions as a DCE (Data Communications Equipment). Configure the GS3 with settings that match the DTE (Data Terminal Equipment), connect its cable to the serial console's connector.¹⁰

The serial cable

| RJ-45 to RJ-45 | | | | |
|----------------|-----|-------------|-----|---------|
| GS3 | Pin | Color | Pin | Console |
| Rx | 3 | White/Green | 3 | Tx |
| Tx | 6 | Green | 6 | Rx |
| GND | 5 | White/Blue | 5 | GND |
| GND | 4 | Blue | 4 | GND |

| RJ-45 to Mini-B | | | | |
|-----------------|-----|-------------|-----|---------|
| GS3 | Pin | Color | Pin | Console |
| Rx | 3 | White/Green | 3 | Tx |
| Tx | 6 | Green | 2 | Rx |
| GND | 4 | Blue | 5 | GND |

| RJ-45 to DB-9 | | | | |
|---------------|-----|-------------|-----|---------|
| GS3 | Pin | Color | Pin | Console |
| Rx | 3 | White/Green | 3 | Tx |
| Tx | 6 | Green | 2 | Rx |
| GND | 4 | Blue | 5 | GND |

If the device remains inaccessible after connecting the cable, verify that it is connected to the correct port — not an Ethernet port or an RS-232 port with CTS/RTS support. **The mistake of connecting to an ethernet port by using a conventional ethernet cable will promptly stop GS3 from running.** The GS3 module will recover after you take the cable out of the ethernet port.

¹⁰In rare cases, a DTE device, such as the Brocade/Extreme MLXe-4, may be wired as a DCE; however, the MLXe-8 and MLXe-16 are wired as DTE.

8 Network Commands

The network commands section provides tools for configuring and managing the GS3's network settings. These commands allow users to view the current network configuration, modify IPv4 and IPv6 settings, enable or disable DHCP, and configure time synchronization with an NTP server. Users can also set the system hostname, manage the network port, and configure remote logging via a Syslog server. For added security, the GS3 also supports per-host Access Control Lists (ACLs) to restrict SSH client access.

network show

Displays the current network configuration of the GS3, including IPv4 and IPv6 settings, DNS servers, MAC address, Interface Name, Hostname, Reverse SSH configuration, and remote services such as NTP and Syslog.

Example: The following output shows the GS3's default network configuration.

```
[admin@ssh-to-serial]>network show
Compiled: Dec 23 2025 04:34:08

Static IPv4 Address: 192.168.11.11
IPv4 Subnet Mask: 255.255.255.0
IPv4 Default Gateway:
IPv4 Primary DNS:
IPv4 Secondary DNS:
IPv6 Link-Local Address: fe80::8e12:c2ff:fe00:16d
IPv6 Global Address: ::
IPv6 Default Router: ::
IPv6 Primary DNS:
IPv6 Secondary DNS:
Reverse SSH Port: 65535
CLI SSH Port: 22
Reverse SSH Timeout: 300 seconds
Interface Name: eth0
Hostname: ssh-to-serial
MAC Address: 8C-12-C2-00-01-6D
DHCP: disabled
SLAAC: enabled
Stable Address: enabled with EUI-64
IPv4: enabled
Remote NTP Server: 0.0.0.0
Remote Syslog Server 1: 192.168.11.11
Remote Syslog Server 2: 0.0.0.0

Current configuration displayed.
```

Warning: Running the network configuration commands will disconnect all SSH sessions, as the GS3 restarts its network stack.

network ipv4 <manual/dhcp/disable>

Configures the IPv4 settings for the GS3. You can choose between manually assigning a static IP address (manual), enabling dynamic IP assignment via DHCP (dhcp), or disabling IPv4 entirely (disable).¹¹

¹¹If no argument is provided, running `network ipv4` will enter manual configuration mode by default.

Example:

```
[admin@ssh-to-serial]>network ipv4 manual
Enter Host Address:
192.168.11.11

Host Address is set to 192.168.11.11
Enter Subnet Mask:
255.255.255.0

Subnet Mask is set to 255.255.255.0
Enter Default Gateway:
192.168.11.1

Default Gateway is set to 192.168.11.1
Enter Primary DNS:
8.8.8.8

Primary DNS is set to 8.8.8.8
Enter Secondary DNS:
1.1.1.1

Secondary DNS is set to 1.1.1.1
All ipv4 configurations are set.
```

Example:

```
[admin@ssh-to-serial]>network ipv4 dhcp
DHCP is enabled
Rebooting the system...
```

Example:

```
[admin@ssh-to-serial]>network ipv4 disable
IPV4 is disabled
```

network ipv6 <auto/random/manual/linklocal/disable>

Configures the IPv6 settings for the GS3. You can assign a global address manually, generate one automatically using SLAAC (auto), generate a random address (random), use only a link-local address (linklocal), or disable IPv6 entirely (disable).

Example:

```
[admin@ssh-to-serial]>network ipv6 manual
Enter Global IPv6 Address:
2001:db8:abcd:0012::1
Global Address is set to 2001:db8:abcd:0012::1

Enter Prefix Length:
64
Prefix Length is set to 64

Enter Default Router (Gateway):
2001:db8:abcd:0012::fffe
Default Router is set to 2001:db8:abcd:0012::fffe

Enter IPv6 Prefix:
2001:db8:abcd:0012::
IPv6 Prefix is set to 2001:db8:abcd:0012::

Enter Primary DNS:
2001:4860:4860::8888

Primary DNS is set to 2001:4860:4860::8888
```

```
Enter Secondary DNS:
2001:4860:4860::8844

Secondary DNS is set to 2001:4860:4860::8844

Global Address is set to 2001:db8:abcd:0012::1
Prefix Length is set to 64
Default Router is set to 2001:db8:abcd:0012::ffffe
Link Local Address set using EUI-64: fe80::8e12:c2ff:fe00:c9
```

```
[admin@ssh-to-serial]>network ipv4 disable
Ipv6 is disabled
```

network port cli <port>

Configures the TCP port used for incoming command line interface management SSH connections to the GS3. The port value must be in the range of 1 to 65,535. The default port is 22.

Example:

```
[admin@ssh-to-serial]>network port cli 22
CLI port is set to 22
Rebooting the system...
```

network reverse-ssh <port>

Configures the TCP port used for incoming reverse SSH connections to the GS3. The port value must be in the range of 1 to 65,535. The default port is 922.

Example:

```
[admin@ssh-to-serial]>network port reverse-ssh 922
Reverse SSH port is set to 922
Rebooting the system...
```

network timeout <timeout>

Sets the SSH timeout duration, defined in seconds. The allowed range is from 60 to 86,400 seconds (1 minute to 24 hours). The default timeout is 300 seconds. This setting controls how long the GS3 will keep cli and/or reverse SSH sessions active before closing them due to inactivity.¹²

Example:

```
[admin@ssh-to-serial]>network timeout 60
Reverse SSH Timeout is set to 60 seconds.
```

¹²Please note that the GS3 does not have an internal clock, and all timeouts are approximate.

network hostname <host name>

Sets the system hostname for the GS3. Hostnames can be up to 32 characters and must start with a letter.

Example:

```
[admin@ssh-to-serial]>network hostname example-host
Host name is set to example-host
[admin@example-host]>
```

network ntp <remote-ntp-addr>

Configures the remote NTP server for time synchronization (can be set as either an IP address or a hostname). Currently, only IPv4 is supported.

Example:

```
[admin@example-host]>network ntp time.example.com
NTP server is set to time.example.com
```

network syslog <remote-syslog-addr>

Sets the IP address of the remote syslog server to which the GS3 sends system log messages. This enables centralized log collection for monitoring, auditing, and troubleshooting purposes.

GS3 supports configuration of up to two remote syslog servers for redundancy or multi-destination logging.

Both Ipv4 and IPv6 are supported. The syslog server must be reachable from the GS3. Log messages are sent using the standard syslog UDP port 514.

When syslog is configured, the GS3 reports security-relevant SSH events, including:

- SSH session establishment (successful login)
- SSH authentication failures
- SSH session termination (logout or disconnect)

These events support centralized auditing, access monitoring, and security analysis.

Example (IPv4):

```
[admin@example-host]>network syslog 192.0.2.15
Syslog server is set to 192.0.2.15
```

Example (IPv6):

```
[admin@example-host]>network syslog 2001:db8::15
Syslog server is set to 2001:db8::15
```

9 Security Management Commands

The Security Management commands section provides tools for managing user accounts, Access Control Lists (ACLs), and SSH sessions on the GS3.

user list

Displays a list of all user accounts configured on the GS3, including their username and roles (admin or regular).

Example:

```
[admin@ssh-to-serial]>user list
User 1: admin (admin)
```

user add <admin/regular> <username> <password>

Adds a new user account to the GS3 with the specified role. Usernames and passwords can be up to 33 characters long.

Example:

```
[admin@ssh-to-serial]>user add regular regular password
User regular added successfully.
```

user change <username> <new password>

Changes the password for an existing user account.

Example:

```
[admin@ssh-to-serial]>user change regular password
Password for user regular changed successfully.
```

user delete <username>

Deletes the specified user account.

Example:

```
[admin@ssh-to-serial]>user delete regular
You are attempting to delete the regular user: regular.
Confirm deletion (attempt 1/3). Type 'y' to confirm, 'n' to abort:
Confirm deletion (attempt 2/3). Type 'y' to confirm, 'n' to abort:
Confirm deletion (attempt 3/3). Type 'y' to confirm, 'n' to abort:
User regular deleted successfully.
```

user publickey <username>

Associates an SSH public key with the specified user account. The configured public key is used to authenticate the user when SSH public key authentication is enabled.

Example:

```
[admin@ssh-to-serial]>user publickey admin
Enter public key for user admin:
ssh-ed25519 AAAAC3NzaC11ZDI1NTE5AAAAI... user@example-host
Public key for user admin set successfully.
```

session list

Displays a list of all active SSH sessions, including session ID and the associated user. Regular users can have a total of 4 active sessions and admin users can have one additional session allowing them to kill regular user sessions if required. Session ID's begin with 1 and go to 1024 then reset back to 1.

Example:

```
[admin@ssh-to-serial]>session list
Active sessions:
Session ID: 5, User: admin, Source IP: 192.168.17.8, Session Time: 10 seconds
```

session kill <sessionId>

Terminates a specific SSH session based on its session ID.

For enhanced security, the GS3 limits new incoming SSH connections to a maximum of five connection attempts per second.

Example:

```
[admin@ssh-to-serial]>session list
Active sessions:
Session ID: 1, User: admin, Source IP: 192.168.17.8, Session Time: 19
Session ID: 2, User: regular, Source IP: 192.168.11.18, Session Time: 10
[admin@ssh-to-serial]>session kill 2
Session ID: 2 killed.
```

ssh config <kex/host-key>

Interactively configures the SSH cryptographic algorithms used by the GS3. This command allows administrators to enable or disable specific key exchange (KEX) algorithms or SSH host key types in order to meet security policy requirements or maintain compatibility with legacy SSH clients.

When `kex` is specified, the GS3 prompts for each supported key exchange algorithm. When `host-key` is specified, the GS3 prompts for each supported SSH host key algorithm. Take care to enable the appropriate kex algorithm for the key. Example, if you enable `ssh-rsa` hostkey also enable `diffie-hellman-group14-sha1` and/or `diffie-hellman-group1-sha1`.

Example:

```
[admin@ssh-to-serial]>ssh config kex
kex ecdh-sha2-nistp256 [Y]:
kex ecdh-sha2-nistp384 [Y]:
kex diffie-hellman-group14-sha256 [Y]:
kex diffie-hellman-group14-sha1 [n]:
kex diffie-hellman-group1-sha1 [n]:
KEX algorithms configuration saved. Rebooting the system...
```

```
[admin@ssh-to-serial]>ssh config host-key
key ssh-ed25519 [Y]:
key ecdsa-sha2-nistp256 [Y]:
key ssh-rsa [n]:
Host key algorithms configuration saved. Rebooting the system...
```

ssh publickeyonly <enable/disable>

Enables or disables SSH authentication using public key credentials only. To enable, a public key must first be associated with the target user account using the `user publickey <username>` command.

Example:

```
[admin@ssh-to-serial]>user publickey admin
Enter public key for user admin:
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAI... user@example-host
Public key for user admin set successfully.
[admin@ssh-to-serial]>ssh publickeyonly enable
Public key only authentication is enabled. Rebooting the system...
```

When public key-only authentication is enabled, password-based SSH logins are rejected. Clients that attempt to connect without a valid private key will receive a permission denied error.

Example:

```
% ssh admin@192.168.11.11
admin@192.168.11.11: Permission denied (publickey).
```

acl set <ipv4/ipv6> <ip>

Adds an IP address to the Access Control List (ACL) for either IPv4 or IPv6. Only addresses included in the ACL will be permitted to initiate SSH connections to the GS3. ACL does not impact the current logged in user until re-login.

Example:

```
[admin@ssh-to-serial]>acl set ipv4 192.0.2.100
IP address 192.0.2.100 added to ACL
[admin@ssh-to-serial]>acl set ipv6 2001:db8:abcd:0012::10
IP address 2001:db8:abcd:0012::10 added to ACL
```

acl del <ipv4/ipv6> <listnum>

Removes an IP address from the Access Control List (ACL) based on its index number. Use this command to revoke access for previously allowed IPv4 or IPv6 address.

Example:

```
[admin@ssh-to-serial]>acl del ipv4 0
IP address at index 0 removed from ACL
[admin@ssh-to-serial]>acl del ipv6 0
IP address at index 0 removed from ACL
```

acl list <ipv4/ipv6>

Displays the current entries in the Access Control List (ACL) for either IPv4 or IPv6. Each entry is listed with its corresponding index number.

Example:

```
[admin@ssh-to-serial]>acl list ipv4
0. 192.10.2.100
[admin@ssh-to-serial]>acl list ipv6
0. 2001:db8:abcd:0012::10
```

10 Firmware Commands

The firmware commands section provides tools for managing and maintaining the GS3's firmware. These commands allow users to view the current firmware, perform upgrades, and configure the necessary server settings and credentials for upgrades via SFTP. GS3 admins can reset firmware-related settings to their default state by CLI or reload the GS3 perhaps to test the rapid GS3 reboot time.

firmware version

Displays the current firmware version and build information.

Example:

```
[admin@ssh-to-serial]>firmware version
Version: 2.0
Compiled on: Dec 23 2025 at 04:34:07
```

firmware upgrade

Initiates a firmware upgrade.¹³

Example:

```
[admin@ssh-to-serial]>firmware upgrade
Firmware update started...
Firmware update successful. Triggering bootloader...
Read from remote host 192.168.11.11: Connection reset by peer
Connection to 192.168.11.11 closed.
client_loop: send disconnect: Broken pipe
```

firmware server <set/get>

Sets or retrieves the credentials and settings for the SFTP server where the firmware file is stored.

Example:

```
[admin@ssh-to-serial]>firmware server set
Enter SFTP Server Name:
192.0.2.10
Enter SFTP Server Port:
22
Enter SFTP Username:
sftpuser
Enter SFTP Password:
*****
Enter SFTP Filename:
firmware.bin
SFTP server credentials updated successfully!
[admin@ssh-to-serial]>firmware server get
SFTP Server Name: 192.0.2.10
SFTP Server Port: 22
SFTP Username: sftpuser
SFTP Password: [REDACTED]
SFTP Filename: gs3_2_0.bin
Trusted Host Keys:
```

¹³Note the firmware update will timeout with a 220 error if another admin level user is logged in while performing the "firmware upgrade" command.

```
[admin@ssh-to-serial]>firmware server get
SFTP Server Name: 192.168.11.12
SFTP Server Port: 22
SFTP Username: jbolton
SFTP Password: [REDACTED]
SFTP Filename: gs3_2_0.bin
Trusted Host Keys:
ssh-ed25519 AAAAC3NzaC11ZDI1NTE5AAAAIBRZb2N1bWVudGF0aW9uT25seUt1eTAwMDAwMDAw
```

reset <defaults/reboot>

reset defaults

Resets the device configuration to factory default settings. All user-defined configuration parameters are erased, and the system is restored to its initial state.

reset reboot

Reboots the device without modifying the current configuration.

Examples:

```
[admin@ssh-to-serial]>reset defaults
System configuration reset to factory default values.
```

```
[admin@ssh-to-serial]>reset reboot
Rebooting the system...
```

Physical Reset:

A physical factory reset can be triggered by rapidly plugging and unplugging the console cable while the GS3 is powered on more than five times within ten seconds. This action is equivalent to running `reset defaults`.

11 Serial Phrase Locator

This feature monitors the output of the serial console port for specific key phrases. You can configure up to ten phrases. When a match is detected, the GS3 generates a Syslog message and sends it to the configured remote servers.

keyphrase add <key phrase>

Adds a key phrase to the list of phrases monitored in the serial console output. The system supports up to ten key phrases. When a configured phrase is detected in the serial output, the GS3 will trigger a syslog message to the appropriate remote server.

Example:

```
[admin@ssh-to-serial]>keyphrase add ERROR: Link Down
0: ERROR: Link Down
[admin@ssh-to-serial]>keyphrase add CPU Overheat Warning
0: ERROR: Link Down
1: CPU Overheat Warning
```

keyphrase list

Displays all currently configured key phrases being monitored in the serial console output.

Example:

```
[admin@ssh-to-serial]>keyphrase list
0: ERROR: Link Down
1: CPU Overheat Warning
```

keyphrase del <list num>

Removes a key phrase from the monitored list using its index number, as displayed by the **keyphrase list** command. Once deleted, the system will no longer monitor or trigger alerts based on the removed phrase.

Example:

```
[admin@ssh-to-serial]>keyphrase list
0: ERROR: Link Down
1: CPU Overheat Warning
[admin@ssh-to-serial]>keyphrase del 0
0: CPU Overheat Warning
[admin@ssh-to-serial]>keyphrase list
0: CPU Overheat Warning
```

A SSH Security Audit Output

This appendix provides an example of an independent SSH security assessment performed against the GS3 using the industry-standard `ssh-audit` tool. The output is included for transparency and to assist security teams in evaluating the cryptographic posture of the GS3 SSH service.¹⁴

Audit Method

- Tool: `ssh-audit`
- Target: GS3 SSH service
- Protocol: SSHv2
- Execution environment: External client host

Command Executed

```
ssh-audit <GS3-IP-address>
```

Audit Output

```
# general
(gen) banner: SSH-2.0-CycloneSSH_2.5.2
(gen) compatibility: OpenSSH 9.9+, Dropbear SSH 2020.79+
(gen) compression: disabled

# key exchange algorithms
(kex) mlkem768x25519-sha256
(kex) curve25519-sha256
(kex) curve25519-sha256@libssh.org
(kex) ext-info-s
(kex) kex-strict-s-v00@openssh.com

# host-key algorithms
(key) ssh-ed25519

# encryption algorithms (ciphers)
(enc) aes128-gcm
(enc) aes128-gcm@openssh.com
(enc) aes256-gcm
(enc) aes256-gcm@openssh.com
(enc) aes128-ctr
(enc) aes192-ctr
(enc) aes256-ctr

# message authentication code algorithms
(mac) hmac-sha2-256-etm@openssh.com
(mac) hmac-sha2-512-etm@openssh.com
```

¹⁴The results reflect the default SSH configuration of the GS3 at the time of testing and may change across firmware versions.

B Deployment Example: Detecting a warm reload

To detect a warm reload on the Cisco Catalyst 2950, observe the following boot sequence:

```
C2950 Boot Loader (C2950-HB00T-M) Version 12.1(11r)EA1, RELEASE SOFTWARE (fc1)
Compiled Mon 22-Jul-02 17:18 by antonino
WS-C2950-12 starting...
Base ethernet MAC Address: 00:12:7f:38:a4:40
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 87 files, 3 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7741440
flashfs[0]: Bytes used: 6511104
flashfs[0]: Bytes available: 1230336
flashfs[0]: flashfs fsck took 8 seconds.
...done initializing flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4
Loading "flash:/c2950-i6q4l2-mz.121-22.EA1.bin"...###
```

To track this event, add the first line as a keyphrase using the following command:

```
[admin@ssh-to-serial]>keyphrase add C2950 Boot Loader (C2950-HB00T-M) Version 12.1(11r)EA1,
    RELEASE SOFTWARE (fc1)
0. C2950 Boot Loader (C2950-HB00T-M) Version 12.1(11r)EA1, RELEASE SOFTWARE (fc1)
```

Verify that the keyphrase was added successfully:

```
[admin@ssh-to-serial]>keyphrase list
0. C2950 Boot Loader (C2950-HB00T-M) Version 12.1(11r)EA1, RELEASE SOFTWARE (fc1)
```

When a warm reload occurs, the GS3 will match this keyphrase and send an alert to the configured syslog server:

```
Oct 10 15:33:37 192.0.2.15 ssh-to-serial Match found: C2950 Boot Loader (C2950-HB00T-M)
    Version 12.1(11r)EA1, RELEASE SOFTWARE (fc1)
```

C Deployment Example: Detecting a host recovery

To detect a host recovery on the Cisco Catalyst 2950, observe the following sequence:

```
00:00:15: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
00:00:17: %SYS-5-CONFIG_I: Configured from memory by console
00:00:18: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Mon 12-Jul-04 08:18 by madison
00:00:18: %SNMP-5-COLDSTART: SNMP agent on host Switch is undergoing a cold start
00:00:18: %LINK-5-CHANGED: Interface Vlan1, changed state to administratively down
00:00:19: %LINK-5-CHANGED: Interface Vlan2, changed state to administratively down
00:00:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:20: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to down
Switch>
```

To track this event, add the following line as a keyphrase using the keyphrase below:

```
[admin@ssh-to-serial]>keyphrase add %SYS-5-RESTART:
0: %SYS-5-RESTART:
```

Verify that the keyphrase was added successfully:

```
[admin@ssh-to-serial]>keyphrase list
0. %SYS-5-RESTART:
```

When the host recovers, the GS3 will match this keyphrase and send an alert to the configured syslog server:

```
Oct 10 15:35:38 192.0.2.15 ssh-to-serial Match found: 0. %SYS-5-RESTART:
```

D Firmware Releases and SHA256 Hash Values

Below is a list of GS3 supported firmware releases and SHA256 hash values:

| |
|---|
| Version 2.0 filename GS3_2_0.bin SHA256 Hash: E7DD92333F1FB389E80DE73B3A26AC657AC846A09EDA9081FAAFEBFFD14C0E5A |
|---|

Please confirm GLBB Japan's website <https://www.glbb.ne.jp/hardware/g3> to verify this PDF and use this PDF to verify binary with above SHHA256 hash.