



GE MDS *PRODUCT RELEASE NOTES v7.2.9 Rev A*

RELEASE NOTE For: MDS Master Station Firmware Version 7.2.9
RELEASE DATE: May 31, 2019

FIRMWARE

©2019 GE MDS LLC, 175 Science Parkway, Rochester, NY 14620 USA
Phone +1 (585) 242-9600, FAX +1 (585) 242-9620
<http://www.gegridsolutions.com/communications/wireless.htm>

MDS™ Master Station

COVERING FIRMWARE – v7.2.9

Overview

This section describes Software/Firmware updates for the MDS Master Station.

- Products: MDS Master Station
 - Variants: MPRS, MPRL, MPRU
- System Firmware Version: v7.2.9
 - SD Radio Module Firmware: v3.8.7
 - LN Radio Module Firmware: v3.0.7
 - NX Radio Module Firmware: v0.7.2

NOTICE FOR CUSTOMERS UPGRADING TO THIS VERSION

As part of an enhanced security posture this release uses a SHA256 firmware certificate. When upgrading from earlier firmware versions (before 7.0) it is necessary to overwrite the previous GE MDS firmware certificate with this new one. Related information:

- The new certificate can be found at the GE Industrial Communications website at http://www.gegridsolutions.com/Communications/MDS/software.asp?directory=Orbit_MCR/Support_Items
- Certificates can be loaded individually (see Certificate Management, at the bottom of the navigation pane)
- Certificates can be broadcast to a network using remote management.

IMPORTANT NOTES:

- Version 7.2.9 applies to all MPR (MPRS/MPRL/MPRU) except as described below
 - This firmware does NOT support Evolution/Migration Master station (serial-router).
- Once running 4.x or later system firmware, 3.x system firmware **cannot** be downloaded into the Master Station. To preserve the ability to boot back to 3.x firmware, **do not** overwrite your inactive 3.x firmware image.
 - See the section labeled “Special Instructions: Booting to 3.x firmware in the inactive image (MPRS Only)” later in the release notes for detailed instructions.
- Both active and inactive Radio Modules have their own firmware that the MPR upgrades together and keeps in sync. The Radio modules use different versioning than the Master Station system firmware. See the firmware version list in the Overview section for the expected radio module firmware versions.

Supported Radio Modules

- **MDS Master Station with LN Radio Modules (MPRL)**
 - LN1B
 - LN2X
 - LN4A
 - LN4C
 - LN4E
 - LN7A
 - LN9C
- **MDS Master Station with SD Radio Modules (MPRS):**
 - SDM4B
 - SDM4C
 - SDM4D
 - SDM9C
 - SDM9K
- **MDS Master Station with Unlicensed 900MHz Radio Modules (MPRU)**
 - NX

New Features

- **Features applicable to all MDS Master Station since v5.0.8**
 - Extension of Virtual Radio Channels (VRC) to the U91 (NX, Unlicensed 900MHz) facilitating quick and simple configuration of serial networks
 - Diagnostic Enhancements
 - New CLI based serial protocol analyzer (serdump) for monitoring serial port data
 - New ability to view active IP Connections, (Web Interface under Troubleshooting and CLI)
 - Facility to export PCAP files from a TCPDUMP session
 - Stateful Packet Inspection with UDP
 - Orbit Configuration support for Zero Touch Provisioning (requires a separate ZTP server)
- **MDS Master Station with LN Radio Modules (MPRL) since v5.0.8:**
 - LN MAC improvements
 - Support for RF-based QOS, “Fairness”, and improvements to adaptive modulation for serial networks
- **MDS Master Station with SD Radio Modules (MPRS) since v5.0.8:**
 - Added DLINK QAM Broadcast command. This command broadcasts a DLINK command to all Orbit remotes in backwards compatible mode, instructing them to change radio mode to QAM (Standard) mode.

Changes to Existing Features

- Orbit now properly checks for serial port conflicts to prevent accidental reuse of the same COM port.
- The Orbit LN interface now offers improved alarms and warnings for failure conditions.
- Security: An option is provided to allow users to set the ADMIN password to ADMIN. (NOTE: Best practice security strongly discourages this option and it is disabled by default).
- Changing the user password now requires a user to enter retype the password for change verification.
- To change a user password on the CLI, use the command “change-password user”.
- Remote Management (via Web Proxy) has been optimized to load faster.
- The Web UI now allows a user to extend a session prior to a web idle-timeout.
- Clicking on the Firmware version listed on the top right of the Web UI redirects the user to the Firmware service.
- Clicking on Web UI alarms in the event-log now provides an expanded log with more details.
- For MPRS, running MODEM 4800B, the system now requires serial port baud rate to be 4800bps.

Resolved Issues (Fixed) & Improvements

Note: numbers in brackets [] represent internal issue tracking numbers.

- **MDS Master Station since v5.0.8:**
 - General improvements made to web page robustness
 - General improvements made to NETMON based service recovery.
 - The Firewall Wizard was previously limited to displaying no more than 10 entries.
 - UDP multipoint operation: “+++” escape sequence to the CLI now works properly in cases where configuration was incomplete.
 - When attempting to reprogram, if a Firmware Certificate is missing, Orbit now displays a more descriptive message
 - Time is now updated properly when a timezone-location offset is deleted.
 - QOS: Use of IPv4 Custom Protocol = 0 is now properly prevented.
 - When updating firmware from LOCAL FILE, the browser timeout is now properly suspended.
 - SNMP configuration dump now works properly.
 - Static ARP entries are now properly preserved across a device reboot.
 - Passthrough mode using DNP3 Traffic with encryption now works properly
 - Fixed an issue where GPS service could update system time to the wrong value.

- **MDS Master Station with LN Radio Modules (MPRL) Since v5.0.8:**
 - LN store-and-forward with assigned gateway ID now works properly.
- **MDS Master Station with SD Radio Modules (MPRS) since v5.0.8:**
 - Fixed an issue where Receiver could become non-responsive in x710 and Transparent modes.

Preserving ability to run previous configuration

New versions of Master Station code use updated configuration data models that are not backwards compatible with older releases. When a unit running a *previous* release is upgraded to this release, a snapshot of its configuration is made and stored on the unit called “Auto”. The unit’s configuration is automatically migrated to newer data model. The user can downgrade back to the *previous* firmware version only by choosing to revert to the legacy configuration snapshot as described here. Any firmware can be loaded that is greater than or equal to the Factory snapshot version, but may require a different firmware cert be loaded (See SPECIAL NOTICE FOR CUSTOMERS UPGRADING TO THIS VERSION section above).

To maintain ability to run previous firmware follow the procedure below.

1. Should it be determined that reverting to the *previous* firmware is necessary, perform the following command on the CLI to reboot to the old firmware, and restore the system using a configuration snapshot. The Auto or a user snapshot can be used if available, but the factory snapshot will always be available.

```
> request system recovery rollback which-image { inactive } snapshot Auto
```

2. You will be prompted to confirm this action:
The current system configuration will be erased and replaced with the snapshot. Proceed? [no,yes]
3. Type ‘yes’ and press enter, and the system will restart to the *previous* configuration
4. Note that the recovery operation *may* include restoration of a previous SHA1 FW certificate. If so, then it will be necessary to reinstall the new SHA256 FW certificate before newer software can be downloaded again.

Special Instructions: Booting to 3.x firmware in the inactive image (MPRS Only)

To switch between 3.x firmware and 4.x system firmware on an MPRS follow the procedure below.

1. **IMPORTANT:** Once you are running 4.x firmware or greater, be sure to not overwrite the 3.x firmware in the inactive firmware location, or you will not be able to revert back to that version. E.g. copying active firmware to inactive location, or installing a new version to the inactive firmware location.
2. Should it be determined that reverting to the old 3.x firmware is necessary, perform the steps from the “Preserving ability to run previous configuration” section above to load the inactive image with a previous snapshot.

Known Errata

Note: numbers in brackets [] represent internal issue tracking numbers.

- **MDS Master Station Platform (Common):**
 - If a remote syslog server is unreachable, syslog events logged during that time may not be sent upon reconnection. [651]
 - Managing an IKE/IPSec VPN via the web interface is not functional. The CLI must be used for managing IKE/IPSec VPN connections. [1070]
 - Syslog is not fully compliant with RFC5424. [1033]
 - In the initial setup wizard, the radius server authentication type may attempt to reset to CHAP. Review the summary and ensure the authentication type is correct. [1202]
 - Ping statistics may not be displayed after the ping command is interrupted by the escape key sequence. [1354]
 - A QoS modify policy will act like it is automatically applied to all interfaces. [1556]
 - When using QoS, undesired behavior will occur if a shaping policy is the next-policy of priority policy. [1555]
- **MDS Master Station with LN Radio Modules (MPRL):**
 - None
- **MDS Master Station with SD Radio Modules (MPRS):**
 - Multihost feature is not functional with more than one poller. [1842]
 - Changes may not be applied immediately when changing Data Device Mode to either DCE or CTS Key mode. They will be applied after a reboot or failover. [1377] [1267]

Operational Notes and Limitations

Note: numbers in brackets [] represent internal issue tracking numbers.

- **MDS Master Station Platform (Common):**
 - In the CLI, deleting a single entry in a leaf-list will delete the entire list. Do not use brackets in the command when deleting an element in the list. [1325]
 - While the MDS Master Station supports management and routing via IPv6, not all services have support for IPv6. [1254] [1342] [1781]
 - The HTTP Protocol is not supported for exporting files. Files can be sent through a browser but not directly uploaded to an http server. [875]
 - If running a serial port at 300 baud it is recommended that vtime be set to at least 35ms. [1184]
 - The Firewall (Access Control Wizard) may get into a state where the summary screen displays changes that were not made by the user. It is recommended to cancel and restart the Wizard. Verify accuracy of all changes on the summary screen before saving the configuration. [1180]
 - If the system event log is very full, attempting to search the event log via the event log table on the Web UI may result in the system becoming unresponsive for a period of time. [1002]

- Configuring multiple Terminal Servers on the *same* TCP port generates a warning, but accepts the configuration although the configured Terminal Servers will not work correctly.
- A com port configured as Console mode only supports 8N1 formatting even though the serial settings can be set otherwise, operates correctly when in data mode. [1326]
- SCEP operations require certificate information to contain a Common Name, otherwise the operation will fail. No direct indication of failure is provided.
- On a Microsoft CA server, the SCEP template used should not include Extended Key Usage.
- In the Web UI, there are no preconfigured file servers. This facility is only accessible from the CLI.
- The USB port is currently intended for console access only.
 - Note: If the USB port is in use as a console OR Terminal Server and the system is rebooted (or connection interrupted) the USB cable may need to be disconnected and reconnected and the Terminal Session on the connected device may need to be restarted.
- Any member of a disabled bridge will be disabled. Members must first be removed from the bridge in order to regain access to the interface.
- Date/Time settings are expressed in GMT format.
- The “\” character is an escape character for the CLI. If you want to enter a “\” into a text field (such as a user password), you will need to use “\\”. [1234][876]
- STP is not functional over interfaces belonging to a VLAN.
- Tab completion is not available on the CLI when deleting list entries. The entry name must be manually entered using the name as displayed by the show command.
- Displaying the active routes will not show all configured routes when connectivity to an affected subnet cannot be established.
- In some versions of Firefox, the rollback to snapshot page is not rendered correctly. You must double click the snapshot field to have the options appear. [976]
- A user may not modify an already saved 'user snapshot'. Instead, delete and remake the snapshot with the necessary changes. [992]
- If attempting to ping an IPv6 link local addresses, you must also specify the outgoing interface. [1320]
- To clear the Remote Detection Service table, disable the service, then reenale.
- Error message boxes may appear in the Destination NAT, ACL, and Interface Setup wizards. [1590] [1589] [1588] [1583] [1567] [1566] [959]
- QoS traffic flows may not be prioritized properly if QoS settings are modified while it is in use. To prevent this, stop the traffic flows before changing QoS settings, and restart them after applying the new configuration. [1554]
- When using QoS, DSCP traffic and custom IPv4 protocol may not be prioritized correctly. [1550] [1547]
- Internal software warnings may be present in the event log after upgrading from firmware version 4.3.8. This does not affect operation. [1448]
- The Inms interface may receive a new DHCP address upon reboot when it is unbridged and operating as a DHCP client. [1440]
- An internal software error may be generated upon changing TCP terminal server configuration from streaming to polled. [1439]
- An internal software error may be generated when starting a remote reprogramming session. [1432]
- An internal software error may occur when changing serial port settings. Should this occur, reboot the device. [1428]
- When using Next Hop in Static Route leave Outgoing Interface Blank. [1598]
- If web page display seems to render incorrectly, try refreshing the page. [1783]
- When using Next Hop in Static Route leave Outgoing Interface Blank. [1598]
- A QoS modify policy will act like it is automatically applied to all interfaces. [1556]
- When making changes to QOS settings, changes will not occur after committing if traffic flow is already in progress. Reset the interface (or reboot the device) to ensure that changes will be in effect.
- When a firewall rule is changed such that certain traffic was previously explicitly allowed, but now would match the default drop rule, any previously allowed flows would still have access to the channel. For instance if a rule allowing SSH was removed, any ongoing SSH sessions would still be allowed. Either reboot the unit after such a change, or explicitly block that traffic.

- **MDS Master Station with LN Radio Modules (MPRL):**
 - If the modulation is forced to 64 QAM, it is recommended that FEC (forward error correction) is enabled. [1327]
 - NIC communications may take extra time to establish on the first boot following upgrade to firmware version 4.3.8 or higher. [1434]
 - When using the web proxy, connected remotes may be displayed incorrectly. [1431]
 - If operating an LN NIC in a simplex configuration using a single antenna port and no duplexer, simplex-mode must be enabled. When operating in simplex mode, the TX LED will be illuminated even when the transceiver is not actively transmitting. [1092]
 - Broadcast firmware push tries to keep pushing data until all data has been pushed, but if it takes too many errors it may have to be re-initiated. [1459]
 - Com2 console may become un-responsive, recover by using another interface to commit a change to COM2 and then revert back to the original setting. [1835]

- **MDS Master Station with SD Radio Modules (MPRS):**
 - Operating as a Repeater with local-data when using modem “none” may not work properly when using SDM9C or SDM9K Radio Modules. In this case, set the repeater mode to “repeater” instead of “repeater-with-local-data”. This does not apply when using SDM4B or SDM4C Radio Modules. For these modules, “repeater-with-local-data” should be used. [542]
 - If the operational mode of the radio is changed (e.g. from transparent to packet-with-mac), all mode specific parameters will assume their default values, even if previously set to a different value (e.g. MAC AP vs. Remote). [611]
 - An SD Radio Module configured as a DLINK root will not send local DLINK messages over the air if the radio is also configured for Repeater Mode “repeater”. An SD repeater that is also a DLINK root must be set to “repeater-with-local-data”. [750]
 - When using PulseNET or PulseNET Enterprise to monitor an MPRS in Packet w/ MAC mode, the Passive Collection Repeat Interval (in PulseNET) must be changed from the default 5000ms to a recommended value of 13000ms. This value must be changed for EACH MPRS being monitored in PulseNET. [1303, 1328]
 - An MPRS in transparent mode using ip-payload may require a reduction in the transparent-rx-timeout value, if the data streams are longer than 1480 continues bytes. [1215]
 - When operating in RTS keying mode, full-duplex operation is not supported. For full-duplex operation, continuous keying must be used. [324]
 - When operating as a DATAKEY Repeater with SDx/x710 radios as remote endpoints in 9600 modem, it is recommended that the following parameters be configured in the remotes for best polling performance. [762]
 - SDx/MPRS Polling Remote SCD: 8ms
 - x710/SDx Remote SCD: 12ms
 - SDx/MPRS Polling Remote and x710/SDx Remote PTT
 - For baud 96008N1: 0ms
 - For baud 96008E1: 4ms
 - When operating as a CKEY Repeater with SDx/x710 radios as remote endpoints in 9600 modem, it is recommended that the following parameters be configured in the remotes for best polling performance. [762]
 - SDx/MPRS Polling Remote SCD: 6ms
 - x710/SDx Remote SCD: 8ms
 - An underbaud condition may occur when operating in transparent mode in a network with SDs or x790 units, if the Master Station’s over-the-air data rate is greater than the serial port data rate. To avoid potential gaps in transmission, increase the SCD (soft carrier dekey) on x790 or data key hold time on the Master Station to at least 5. [1888]

- The unit may generate an alarm after committing initial configuration. [868]
- When operating as a repeater in x710 or transparent mode, using modem 9600 and baud rate 9600-8E1, the new repeater-tolerance parameter should be set to 'custom' to reduce errors. [758] [760]
- Due to a limitation of SD data compression when operating with certain modems, this feature is deprecated. Use is highly discouraged, but available for backward compatibility. [825]

For additional Information

MDS™ Master Station Learning and Development YouTube Channel



<http://goo.gl/isGFM2>