GE MDS

PRODUCT RELEASE NOTES Rev AG

v8.3.3

RELEASE NOTE For: MDS ORBIT MCR/ECR Firmware Version 8.3.3
RELEASE DATE: January, 29 2021

FIRMWARE

©2021 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

MDS™ Orbit MCR/ECR

COVERING FIRMWARE – REV 8.3.3

Overview

This section describes Software/Firmware updates for the MDS Orbit MCR/ECR platform, noting changes since REV 8.0.8.

Products:	MDS Orbit MCR/ECR
Firmware Version:	8.3.3

Orbit MCR/ECR Release Notes now includes some items associated with Master Station (MPR) operation. Separate MPR notes will be maintained for now.

SPECIAL NOTICE FOR CUSTOMERS UPGRADING TO THIS VERSION (from pre-7.0)

As part of an enhanced security posture this release uses a SHA256 firmware certificate. When upgrading from earlier firmware versions (before 7.0.0) 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.

New Features

1. Cellular Dual APN
   - Dual APN provides the ability for a cell device to have dual data sessions using a single wireless connection.
   - Operation is supported on the 4Gx, 4Gy, 4GA, and 4GB media types, for common GSM-based carriers including AT&T and Verizon.
   - Configuration is provided by way of the "extra-PDN" field in the cell management user interface

2. Automatic Firmware Over The Air (FOTA) updates.
   - New controllable option enables automatic Orbit device originated firmware upgrades
     - Option ships ON with related parameters preconfigured for FirstNet configured orders.
     - Option ships OFF for standard orders (must be manually turned on)
   - GE maintains a public server location with a "Manifest" file indicating which firmware version is current and where to get it.
   - Secure transfer is supported via HTTPS with a CA X.509 certificate on the device.
   - Default manifest file location can be changed by customer and a custom manifest can be created to support special deployments or specific enterprise needs.
   - Robust retry mechanisms ensure firmware will be maintained.

3. Support for MPRS – Master Station band 4A (350-400MHz)

Changes to Existing Features

1. The System / Firmware selection now includes configuration to control setting of Automatic Firmware Over The Air (FOTA) updates.

Resolved Issues (Fixed)

1. General CVE updates – security updates as reported through December 2020.
2. IPSEC VPN Tunnels could get torn down prematurely during start up. The device status check timeout has been increased to prevent this rare occurrence.
3. Unstable Tunnels with DMVPN using Cisco ASR/ISR routers as Hub Routers. This error did not necessarily prevent payload data from being sent, but it did generate lots of spurious cell link traffic. This is now resolved.
4. L1C minimum step size was incorrect. Now properly set to 1.25KHz
5. Tech user access role can now access spectrum analyzer
6. Clearing statistics on the LnRadio interface will no longer cause a temporary loss of traffic.
7. Changing parameters for the serial passthrough no longer causes an interruption to data passing.
8. Improvements to web interface.
9. LN radios now have improved co-channel performance preventing modem stalls.
10. Software robustness improvement for NIC module operation at -40C.
11. RSSI fix for 2G/3G operation.
12. Robustness fix for cell firmware downloads interacting with GPS.

Special Notes

1. IMPORTANT COMPATIBILITY NOTICES
   - For systems running in Advanced-Polling mode, it is critical to update the AP to version 8.0.7 or higher first, prior to running any remotes with version 8.0.7 or higher.

2. Reverting to earlier configurations
   - Orbit software releases include updated configuration data models that are not backwards compatible with older releases. When a unit running an older release is upgraded to this release, a snapshot of its configuration is made and stored on the unit. The unit's configuration is automatically migrated to newer data model. The user can downgrade back to the older firmware version only by choosing to revert to the legacy configuration snapshot.

3. Firewall Robustness
   - The Orbit Firewall is a powerful tool for restricting unintended traffic. As a protective measure, if the Orbit Firewall ever experiences an unexpected error, all traffic is dropped with the exception of HTTPS and SSH protocols. These protocols can be used to recover the device to a functional state.

1. Updating the firmware via web interface using a local file may fail and get into a bad state. The device will function properly, but updating firmware will fail until the device is rebooted.
2. The standard Wi-Fi (W51) may experience interruptions in the presence of high RF interference. If a service interruption occurs, the ORBIT MCR will detect and reset the Wi-Fi interface to restore service.
3. When a Commit is aborted the device may misrepresent the current configuration. It is recommended to confirm the configuration is correct and re-commit.
4. Rebooting a device functioning as a WiFi Station Bridge may cause a service outage to other WiFi connected devices. The other WiFi devices will resume connections on their own after a short time. (approx. 30 seconds)
5. Showing status on a disconnected interface may cause a netmgr failure. This internal failure will be logged as an event and the device will recover on its own.
6. Changing a WiFi interface from an enabled Station with an IP address and filters to a disabled, bridged, Access Point without an IP address and filter may cause a netmgr failure. This internal failure will be logged as an event and the device will recover on its own.
7. When a WiFi Station is in the bridge, the STP status information for the WiFi device is not available.
8. Attempting to send invalid firmware over broadcast reprogramming may cause a services manager failure.
9. In some cases, changes to the GRE interface configuration (VPN) will require a reboot to take effect. It is good practice to reboot the device after making changes to the VPN configuration.
10. In some cases, changes to IPSec configurations (VPN) will require a reboot to take effect. It is good practice to reboot the device after making changes to the VPN configuration.
11. Setting peer-endpoint to any in DMVPN will cause all traffic on all interfaces attempt to use the VPN.
12. When performing 802.1x port authentication, if the radius server is not reachable when the Ethernet cable is inserted, then it may need to be reinserted to re-initiate authentication.
13. VLAN priority is not preserved if passed from one VLAN trunk to another.
14. With multiple RADIUS servers configured for user authentication and none are reachable, it is possible that it will take a long time for the fallback authentication (if enabled) to be evaluated as each RADIUS server communication times out.
15. There may be occasions where alerts are erroneously displayed on the web interface.
16. When using RADIUS user authentication with multiple servers, incorrect routes will cause authentication to fail.
17. If there are more than 50 routes in a radio's routing table, the routes will not be correctly displayed via the CLI.
18. Carefully review the summary of changes at the end of the firewall wizard to ensure all the changes are expected.
19. 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.
20. Entering control-C during ping may cause the display of overall ping statistics to be suppressed.
21. For Orbit LN using 7FSK modems, operation with a repeater is not recommended.
22. In rare cases, allowing a confirmed commit to timeout (i.e. no user confirm) and rollback the configuration may cause the device to reboot. After the device reboots, it will be running the previous configuration.
23. QOS does not operate handle the DSCP field correctly. To ensure proper QOS priority use the TOS equivalent.
24. If running Mirrored Bits (TM) protocol on an NX network, we recommend using Orbit FW version 7.1.1 or earlier.
25. Operation as a Store-and-Forward device is not recommended in 7 level FSK modems. Operation with system ID is not recommended with 7 level FSK modems.
26. When changing terminal server modes and you experience an error committing, refresh and review the settings.
27. When configuring the Static Routes Next Hop parameter, leave the Outgoing Interface blank. Otherwise, the routing table will not be properly configured and data passing may stop.
28. Broadcast reprogramming of the firmware certificate may not correctly show the status at the broadcast sender.
29. Transporting Mirrored Bits (TM) protocol is only supported on NX interfaces.
30. The remote web proxy will not function if the device disables firmware push.
31. When using the broadcast reprogramming feature, we recommend use of an external file instead of pushing the internal firmware image.

32. When doing requests on the CLI with many arguments, ensure that the nested arguments (ones with {}) are provided last.
33. Alarm threshold parameters "rssi-upper-threshold" and "rssi-lower-threshold" in the ln-config, nx-config, and lw-config had inverted meaning in earlier code.

    If you upgrade to this version then return back to an earlier version, values may need to be manually adjusted.
34. While MDS Orbit supports management and routing via IPv6, not all services have support for IPv6.
35. The LNMS Retry Percentage alarm is non-functional.
36. If a pass-through configuration is initially set up via advanced web or the CLI, there may be problems managing the configuration in basic web mode. Revert to the original mode to allow proper configuration.
37. When changing between single LN configuration and LN profiles the error message "could not load config" may be displayed. This is a false error.

    Validation will still be performed correctly following a commit.
38. The CLI must be used to switch between LN Operating modes Profile and Single Config.
39. When performing file transfers, if the status does not appear to update or looks inconsistent, a reboot of the system may be required to clear the failed state. When in the failed state the status icons in the upper left corner of the web UI will also be non-functional.
40. If a unit repeatedly fails to receive an over the air broadcast reprogram, connect to the unit and copy the active image over the inactive image to attempt to recover the state. Restart the broadcast reprogramming if it has stopped.
41. If problems occur when attempting to manage web-based SCEP renewal with existing client/key certifications, use the CLI instead.
42. The auto-update status is not accessible via SNMP.
43. If experiencing a problem in the redundancy wizard cancel out of the wizard and try again.
44. When applying VRRP to an interface, the interface also needs to have an IPv4 address configured.
45. Destination NAT is not currently supported for IPv6.
46. Using terminal server with MODBUS conversion will not show the correct format values with the serdump tool. All data passed is handled correctly, the display with serdump is incorrect. As a work around, one can look at the data with netdump to see the MODBUS traffic.
47. Webui currently can not provision SCEP configuration. While provisioning SCEP use CLI or SSH.
48. The 8.3.3 release added more strict handling of remote syslog configuration. If the configuration is invalid by referencing certificates that are not loaded, then it will reboot after several minutes. Delete remote syslog config or make sure syslog configuration references loaded certificates and keys.
49. In a large LN network with multiple polling threads, it may be necessary to reduce the traffic entering the LN AP to do broadcast reprogramming.

Operational Notes and Limitations

1. The Web UI rejects a password change with the backslash character if repeated two times in a row example: Y1 \ \ n%*". The CLI and SSH reject a password change with a single backslash character, example: Tech\123.
2. The HTTP Protocol is not supported for exporting files.
3. The Terminal Server may fail if polling with VMIN = 1. Disable then re-enable the Terminal Server to regain functionality.
4. Internet Explorer version 8 is no longer supported. Please upgrade this application to version 11, or use Mozilla Firefox, Google Chrome, or Microsoft Edge.
5. To delete all IPv4 addresses from an interface use the following command:

   % delete interfaces interface myInterface ipv4
6. Wi-Fi Station Bridging is not interoperable with other vendor's Wi-Fi devices.
7. When the Wi-Fi interface is enabled with Dual SSIDs, Station Bridging operation is restricted to the first alphanumeric SSID.
8. SCEP operations require certificate information to contain a Common Name, otherwise the operation will fail. No direct indication of failure is provided.
9. On a Microsoft CA server, the SCEP template used should not include Extended Key Usage.
10. In WebUI, there are no preconfigured file servers. This facility is only accessible from the CLI.
11. The USB port is currently intended for console access only

    · Note: If the USB port is in use as a Terminal Server and the ORBIT is rebooted (or connection interrupted) the USB cable must be disconnected and reconnected and the Terminal Session on the connected device must be restarted.
12. 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.
13. Date/Time settings on ORBIT MCR are expressed in GMT format.
14. Some CLI command sequences, particularly those involving device configuration or repeat status monitoring, may rarely cause an internal error known as a netmgr failure. The system will effect recovery, but to ensure proper operation a reboot is recommended.
15. The backslash 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 "\\".
16. STP is not functional over interfaces belonging to a VLAN.
17. Displaying the active routes will not show all configured routes, when connectivity to an affected subnet cannot be established.
18. When changing a Wi-Fi Access point to put it into a VLAN, you may need to reboot the device for traffic to flow over the Wi-Fi interface.
19. The configuration parameter to enable a specific Wi-Fi Access Point, overrides the higher level configuration to enable the Wi-Fi interface.
20. QoS may not affect the Ethernet interfaces or bridging of Ethernet traffic between a Wi-Fi Access Point and a Wi-Fi Station in a bridge.
21. When using a Public Dynamic IP Addressed SIM card, On-Demand IPsec Mode is not supported. Always-On mode must be used instead.
22. When configuring custom layer-2 protocol filters use 0x as a prefix when entering the value as Hex, otherwise enter the decimal value. Example for ARP: Enter 0x0806 or 2054.
23. An Orbit Wi-Fi Access Point may not pass data to an Orbit Wi-Fi Station-Bridge [after configuration changes are committed]. To ensure proper operation a reboot is recommended.
24. On the web interface, when pop up lists are used, entries cannot be deleted. To delete an entry simply highlight the text in the box and delete the text.
25. COM port attributes (data bits, parity, stop bits) are only applicable to data mode. When operating in Console COM ports will only supports 8N1.
26. Re-authentication is not supported on an established 802.1X Port based session.
27. Syslog is not fully compliant with RFC5424.
28. At the conclusion of remote over-the-air broadcast reprogramming, the System Manager may restart.
29. Nx NICs may need be configured with dwell times above 30ms if running at 125kbps.
30. When NX is in store and forward mode, continuous downlink saturation may cause some nodes to be starved and not given upstream time.

31. In a LN system, if the modulation is forced to 64 QAM, it is recommended that FEC (forward error correction) is enabled.
32. If running a COM port at 300 baud it is recommended that vtime be set to greater than 35 ms.
33. Preconfigured servers are not applicable to broadcast reprogramming.
34. When using QoS, you cannot have a shaping policy as the next-policy of priority policy.
35. When importing a configuration file that contains references to certificates, first ensure those certificates are loaded onto the unit.
36. When operating Orbit LN in backward-compatible mode, degraded performance may sometimes occur in certain complex configurations that include MPRS.
37. If using the Orbit as a DHCPv6 server with IPv6 subnet constructed from the interface specified in constructor-interface parameter, one must specify the v6subnet prefix as ::/0.
38. Interfaces that user can name (bridges, vlans, etc.) should not have spaces in them.
39. To limit the possibility of a cell connected unit not being accessible after a factory reset, we explicitly no longer block HTTPs and SSH ports from being initiated from over the cell link. As a part of provisioning, these ports should be disabled by modifying the IN_UNTRUSTED rules if they are not required.
40. Station bridged WiFi clients behave differently from normal (i.e., non-bridged) clients. Station bridged clients can communicate directly to each other, while normal clients are isolated and IP traffic will not pass between them.
41. When configuring L7W (Licensed 700MHz Wide), do not set NIC-id. It is not supported in this release and will prevent link establishment.
42. In rare cases where an NX or LN access point does not associate new remotes, disabling and then reenabling the access point may resolve the issue.
43. A QoS modify policy is not tied to an interface and must be deleted to disable it.
44. If using terminal server in TCP polled mode, it must be configured with the serial ports vmin to be greater than the largest possible response in bytes.
45. If you are experiencing unexpected fragmentation of data on your LN virtual radio channel or transparent serial, try increasing the vmin and vtime on the virtual serial port.
46. For LN in transparent mode, if your over the air rate is greater than your serial port rate, it is recommended that you increase your SCD (soft carrier dekey) on x790 or data key hold time on your MPRS to at least 5 to eliminate potential gaps in the transmission.
47. The configured power for Wi-Fi radio may not be used, instead a lower caped value is used depending on regulatory constraints.
48. The broadcast reprogramming feature is meant to make minimal impact to the current operation of the network. As such the time for reprogramming is highly dependent on the throughput of the link and how much it is loaded.
49. Basic webui only supports units with an NX, LN, or LW radio (with an optional Wi-Fi module). Standalone Wi-Fi, Cell, and Cell with Wi-Fi are not currently supported.
50. Timeout of MODBUS transactions can cause dropped TCP connections. Workaround is to increase poll rate or increase transaction timeout.
51. When changing COM port usage from a terminal server to a passthrough it is recommended to remove a terminal server with a commit first and then create the passthrough instance on a separate commit.
52. In the CLI, deleting a single entry in a leaf-list with bracket notation will delete the entire list. Do not use brackets in the command when deleting an element in the list.
53. When running VRRP on a Bridge interface, it is recommended to disable STP (spanning tree protocol).
54. Transparent serial system using repeaters, may need to mute portions of the echo repeater response. If polling remote is MPRS use the rx-mute to at least 5. An LN polling remote use data-key-hold-timeout of at least 8.
55. When issuing a repeat command on the CLI, add the additional syntax "| nomore" (without quotes).
56. MTU settings on the Cell interface have the following restrictions:

    -When IPv4 MTU is NOT configured explicitly by the user, the IPv4 MTU provided by the cellular network (during LTE attach) is configured on the cellular interface. This is the expected behaviour for cellular devices and ensures that traffic sent to the network from the device conforms to the MTU value expected by the network.

    - When IPv4 MTU is configured explicitly by the user AND the configured MTU is LOWER than currently active MTU value, then new IPv4 MTU value is applied to the cellular interface. NOTE: The user should never configure MTU value higher than one supported by the cellular network.

    - When IPv4 MTU is configured explicitly by the user AND the configured MTU is GREATER than currently active

MTU value, then new IPv4 MTU value is NOT applied to the cellular interface. In this case, the user must disable and re-enable cellular interface.