PRODUCT RELEASE NOTES Rev Z

RELEASE NOTE For: MDS ORBIT MCR/ECR Firmware Version 7.1.1
RELEASE DATE: January 31, 2019

©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/

MDS™ Orbit MCR/ECR

COVERING Firmware – REV 7.1.1

Overview
This section describes Software/Firmware updates for the MDS Orbit MCR/ECR platform, noting changes since REV 6.8.1.

Products: MDS Orbit MCR/ECR
Firmware Version: 7.1.1

SPECIAL 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 (6.8.1 or earlier) 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. Platform support for “4GY” Cell Modules with Dual SIM operation
2. Support for new LN hardware.
   - L4A (330-406MHz), 12.5KHz, 25.0KHz, 50.0KHz channels
   - L4C (450-520MHz), 12.5KHz, 25.0KHz, 50.0KHz channels
   - L9C (896-960MHz), 12.5KHz, 25.0KHz, 50.0KHz channels
3. 7FSK backward compatibility (MODEM 19200N, MODEM 19200E, MODEM 38400N)
4. LN MAC improvements
   - Support for RF-based QOS, “Fairness”, and improvements to adaptive modulation for serial networks
5. Extension of Virtual Radio Channels (VRC) to the U91 (NX, Unlicensed 900MHz) facilitating quick and simple configuration of serial networks
6. 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
7. Stateful Packet Inspection with UDP
8. Orbit Configuration support for Zero Touch Provisioning (requires a separate ZTP server)

Changes to Existing Features
1. Orbit now properly checks for serial port conflicts to prevent accidental reuse of the same COM port.
2. The Orbit LN interface now offers improved alarms and warnings for failure conditions.
3. 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).
4. Changing the user password now requires a user to enter retype the password for change verification.
5. To change a user password on the CLI, use the command “change-password user”.
6. Remote Management (via Web Proxy) has been optimized to load faster.
7. The Web UI now allows a user to extend a session prior to a web idle-timeout.
8. Clicking on the Firmware version listed on the top right of the Web UI redirects the user to the Firmware service.
9. Clicking on Web UI alarms in the event-log now provides an expanded log with more details.

Resolved Issues (Fixed)
1. WiFi now properly performs auto-recovery after entering a stuck condition.
2. IPSEC operation: IKE using AES and gcm/16 now works properly
3. General improvements made to cell connectivity robustness
4. General improvements made to web page robustness
5. General improvements made to NETMON based service recovery.
6. LN store-and-forward with assigned gateway ID now works properly.
7. When operating in 3FSK backward compatible mode, some over-the-air diagnostic operations (including switch-over to QAM mode) failed and caused a reboot.
8. The Firewall Wizard was previously limited to displaying no more than 10 entries.
9. UDP multipoint operation: “+++
   escape sequence to the CLI now works properly in cases where configuration was incomplete.
10. When attempting to reprogram, if a Firmware Certificate is missing, Orbit now displays a more descriptive message
11. Time is now updated properly when a timezone-location offset is deleted.
12. QoS: Use of IPv4 Custom Protocol = 0 is now properly prevented.
13. When updating firmware from LOCAL FILE, the browser timeout is now properly suspended.
14. SNMP configuration dump now works properly.
15. Clearing alarms on the system tamper detection page now works properly.
16. Static ARP entries are now properly preserved across a device reboot.
17. Passthrough mode using DNP3 Traffic with encryption now works properly
Kn
own Errata

1. Reprogramming using a local file may fail and get into a bad state. Reboot the device to regain local file reprogramming functionality.
2. The standard WiFi (W51) may experience interruptions in the presence of high RF interference. If a service interruption occurs, the ORBIT MCR will detect and reset the WiFi 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 Station Bridge may cause a service outage to other WiFi connected devices.
5. Monitoring a disconnected interface may cause a netmgr failure.
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.
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 will require a reboot to take effect.
10. In some cases, IPSec configurations will require a reboot to take effect.
11. Setting peer-endpoint to any in DMVPN will cause all traffic on all interfaces attempt to use the VPN.
12. Using the rollback command on the CLI may not restore the vlan-id to the interface.
13. When doing 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 reinitiate authentication.
14. Firefox versions 47-50 have a known issue preventing using the initial setup wizard.
15. VLAN priority is not preserved if passed from one VLAN trunk to another.
16. 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.
17. There may be occasions where alerts are erroneously displayed on the web interface.
18. When using RADIUS user authentication with multiple servers, incorrect routes will cause authentication to fail.
19. When in the IPSec Connections window and creating a new connection, the Remote Virtual Address field does not show up after selecting the host-to-net option. You must navigate away, then back for it to show up.
20. In the web there is an issue deleting the OSPF configuration; recommendation is to do this via the CLI.
21. If there are more than 50 routes in a radio’s routing table, the routes will not be correctly displayed via the CLI.
22. Carefully review the summary of changes at the end of the firewall wizard to ensure all the changes are expected.
23. There is a known issue in some versions of Firefox where the rollback to snapshot page is not rendered correctly. You must double click the snapshot field to have the options appear.
24. 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.
25. Entering control-C during ping may cause the display of overall ping statistics to be suppressed.
26. In rare cases, allowing a confirmed commit to timeout and rollback the configuration may cause the radio to reboot.
27. Instead of prioritizing on the DSCP field, it is recommended to prioritize with the TOS equivalent.
28. For Orbit LN using 7FSK modems, operation as a Store-and-Forward device is not recommended.
29. For Orbit LN using 7FSK modems, operation with system ID is not recommended.
30. For Orbit LN using 7FSK modems, operation with a repeater is not recommended.
31. When changing terminal server modes and you experience an error committing, refresh and review the settings.
32. When using Next Hop in Static Route leave Outgoing Interface Blank
Special Notes

1. Configuration compatibility
   - This release features 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.
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%
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. When using an Orbit on both sides of an IPSec tunnel there is an IKEv1 issue. IKEv2 is recommended regardless of this IKEv1 limitation.
6. 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.
7. To delete all IPv4 addresses from an interface use the following command: % delete interfaces interface myInterface ipv4
8. WiFi Station Bridging is not interoperable with other vendor’s WiFi devices.
9. When the WiFi interface is enabled with Dual SSIDs, Station Bridging operation is restricted to the first alphanumeric SSID.
10. SCEP operations require certificate information to contain a Common Name, otherwise the operation will fail. No direct indication of failure is provided.
11. On a Microsoft CA server, the SCEP template used should not include Extended Key Usage.
12. In WebUI, there are no preconfigured file servers. This facility is only accessible from the CLI.
13. 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.
14. 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.
15. Date/Time settings on ORBIT MCR are expressed in GMT format.
16. 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.
17. 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 “\".
18. STP is not functional over interfaces belonging to a VLAN.
19. Displaying the active routes will not show all configured routes, when connectivity to an affected subnet cannot be established.
20. When changing a WiFi Access point to put it into a VLAN, you may need to reboot the device for traffic to flow over the WiFi interface.
21. The configuration parameter to enable a specific WiFi Access Point, overrides the higher level configuration to enable the WiFi interface.
22. QoS may not affect the Ethernet interfaces or bridging of Ethernet traffic between a WiFi Access Point and a WiFi Station in a bridge.
23. When using a Public Dynamic IP Addressed SIM card, On-Demand IPsec Mode is not supported. Always-On mode must be used instead.
24. 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.
25. The user cannot proceed past the WiFi Setup page in the Interface Setup (Connectivity) Wizard when using the Enterprise Privacy Mode for a WiFi Access Point.
26. When configuring custom layer-2 protocol filters use Ox as a prefix when entering the value as Hex, otherwise enter the decimal value. Example for ARP: Enter 0x0806 or 2054.
27. An Orbit WiFi Access Point may not pass data to an Orbit WiFi Station-Bridge [after configuration changes are committed]. To ensure proper operation a reboot is recommended.

28. 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.

29. COM port attributes (data bits, parity, stop bits) are only applicable to data mode. When operating in Console COM ports will only supports 8N1.

30. Re-authentication is not supported on an established 802.1X Port based session.

31. Syslog is not fully compliant with RFC5424.

32. At the conclusion of remote over-the-air broadcast reprogramming, the System Manager may restart.

33. Nx NICs may need be configured with dwell times above 30ms if running at 125kbps.

34. When NX is in store and forward mode, continuous downlink saturation may cause some nodes to be starved and not given upstream time.

35. In a LN system, if the modulation is forced to 64 QAM, it is recommended that FEC (forward error correction) is enabled.

36. If running a COM port at 300 baud it is recommended that vtime be set to greater than 35 ms.

37. Preconfigured servers are not applicable to broadcast reprogramming.

38. When using QoS, you cannot have a shaping policy as the next-policy of priority policy.

39. When importing a configuration file that contains references to certificates, first ensure those certificates are loaded onto the unit.

40. In the web interface, certain configuration changes require a manual refresh of the web browser.

41. When operating Orbit LN in backward-compatible mode, degraded performance may sometimes occur in certain complex configurations that include MPRS.

42. When logged in using SSH, HTTPS, and the firewall rule is removed, reboot to ensure the proper level of security.

43. Configuring the orbit as an IPv6 DHCP server is not currently supported in the web. It must be done in the CLI.

44. Interfaces that user can name (bridges, vlans, etc.) should not have spaces in them.

45. 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.

46. 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.

47. 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.

48. Removing a QoS modify policy will require a reboot to take effect.

49. 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.

50. Web proxy (if enabled) will attempt to work with older code revisions (prior to 6.6.x) using a fallback method. MCR code before 6.0.0 will not render at all. This is a best effort system and may not render the web accurately. Firmware update of the network is recommended.

51. 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.

52. The configured power for WiFi radio may not be used, instead a lower capped value is used depending on regulatory constraints.

53. There may be issues managing a serial pass-through configuration in basic web mode if it was initially set up in advanced web, or the cli.

54. 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.

55. The new basic webui is only for units with a NX or LN radio, and optionally a WiFi module. Cell, WiFi, or Cell with WiFi, are not currently supported. Cell with NX or LN have limited configuration capability.
56. Timeout of MODBUS transactions can cause an dropped TCP connections. Potential fixes to increase poll rate or increase transaction timeout.
57. When the maximum number of user sessions is reached, login via the web is not available. An admin user can effect recovery by logging in via CLI and forcing off another session.
58. When moving from a terminal server config to a passthrough, it is recommended to use two separate commits.
59. When running VRRP on a Bridge interface, it is recommended to disable STP (spanning tree protocol).
60. When issuing a repeat command on the CLI, add the additional syntax "| nomore" (without quotes).
61. After modifying serial passthrough parameters (Simple Serial), you must wait 5 minutes for the unit to go into data mode.