GE MDS

PRODUCT RELEASE NOTES Rev AM

V9.3.3

RELEASE NOTE For: MDS ORBIT MCR/ECR Firmware Version 9.3.3
RELEASE DATE: August 19, 2022

FIRMWARE

Phone +1 (585) 242-9600, FAX +1 (585) 242-9620
http://www.gegridsolutions.com/communications

MDS™ Orbit MCR/ECR

COVERING FIRMWARE – REV 9.3.3

Overview

This section describes Software/Firmware updates for the MDS Orbit MCR/ECR platform, noting changes since REV 9.2.2.

Products: MDS Orbit MCR/ECR
Firmware Version: 9.3.3

New Features

1. Added support for FlexVPN.
2. Added defer reset feature that allows a scheduled reboot of the system.
3. Added the concept of system ID to the LN radio. This allows better rejection of other LN radio systems.
4. Added the ability to trigger logged events, SNMP traps, or NETCONF notifications when a particular firewall rule was violated.

Changes to Existing Features

1. Added dead peer detection to Orbit VPN.

Resolved Issues (Fixed)

1. Fixed an issue exporting a support bundle in the web interface. [3096]
2. Fixed an issue Standard WiFi using station bridging can not support an MTU of 1500, the packets must be restricted to 1470 bytes. [5642]
3. Fixed spectrum analyzer for non-FCC NX units [5667].
4. Fixed an issue while using VLANs with new ECR hardware. [5682]

1. 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.

2. Upgrades from pre-7.0.0 Firmware
   - When upgrading from earlier firmware versions (before 7.0.0) it is necessary to overwrite the previous GE MDS firmware certificate with the SHA256 version before loading new the new firmware.
     - SHA256 certificates 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.

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.

- 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. [2260]
- 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. [2395]
- When a Commit operation is aborted the device may misrepresent the current configuration. We recommend confirming that the configuration is correct and reissuing the Commit. [2396]
- 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) [139]
- 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. [2397]
- 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. [1570]
- When a WiFi Station is in the bridge, the STP status information for the WiFi device is not available. [434]
- Attempting to send invalid firmware over broadcast reprogramming may cause a services manager failure. [2398]
- 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. [1481]
- 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. [1575]
- Setting peer-endpoint to any in DMVPN will cause all traffic on all interfaces attempt to use the VPN. [1574]
- 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. [1545]
- VLAN priority is not preserved if passed from one VLAN trunk to another. [1533]
- 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. [2399]
- There may be occasions where alerts are erroneously displayed on the web interface. [2400]
- When using RADIUS user authentication with multiple servers, incorrect routes will cause authentication to fail. [1377]
- If there are more than 50 routes in a radio's routing table, the routes will not be correctly displayed via the CLI. [1266]
- Carefully review the summary of changes at the end of the firewall wizard to ensure all the changes are expected. [2401]
- 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. [1876]
- Entering control-C during ping may cause the display of overall ping statistics to be suppressed. [1378]
- For Orbit LN using 7FSK modems, operation with a repeater is not recommended. [3182]
- 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. [1714]
- QOS does not operate handle the DSCP field correctly. To ensure proper QOS priority use the TOS equivalent. [2304]
- If running Mirrored Bits (TM) protocol on an NX network, we recommend using Orbit FW version 7.1.1 or earlier. [3132,3159]

- 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. [2361]
- When changing terminal server modes and you experience an error committing, refresh and review the settings. [2375]

- 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. [2139]
- Broadcast reprogramming of the firmware certificate may not correctly show the status at the broadcast sender. [3281]
- Transporting Mirrored Bits (TM) protocol is only supported on NX interfaces. [3164]
- The remote web proxy will not function if the device disables firmware push. [2581]
- When doing requests on the CLI with many arguments, ensure that the nested arguments (ones with {}) are provided last. [727]
- 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. [3661]
- While MDS Orbit supports management and routing via IPv6, not all services have support for IPv6. [1672]
- The LNMS Retry Percentage alarm is non-functional. [3689]
- 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. [3756]
- The CLI must be used to switch between LN Operating modes Profile and Single Config. [3555]
- 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. [3681]
- Destination NAT is not currently supported for IPv6. [4196]
- In a very large LN network with multiple polling threads, it may be necessary to reduce the traffic entering the LN AP prior to initiating broadcast reprogramming. [4180]
- If polling an LN remote in backward compatible mode via DLINK, the timeout of the poller, must be longer than the timeout configured in the radio. [4356]
- When performing bulk changes to the SNMP service if the commit operations fails, it may be necessary to break the changes up into a set of smaller commits. You must discard current changes (or reboot) and enter the changes in smaller sets. [4520]
- On a Web-based file transfer (From Local File) through remote proxy, if the WebUI gets stuck in the file transfer state, performing the operation via CLI can restore operation. The CLI file transfer request need not be successful. [4395]
- If broadcast reprogramming does not complete, restart the transfer to continue reprogramming. [4283]
- If TACACS+ user authentication is used, and the server is routable, but not reachable, the system may lock up and reboot while attempting to authenticate a user. [4611]
- Exports of large serial captures might fail. Retry the operation capturing data for a smaller interval of time. [4198]
- For a system with LW radios, if degraded performance is observed immediately following a radio configuration change, effect recovery by disabling then re-enabling the LwRadio interface. [4712]

- When enabling tamper detection, the UI will become unresponsive for a few minutes. Reboot to effect faster recovery. [5030]
- VRF interface packet statistics may not match the member interfaces. Use the member interface statistics instead. [5034]
- When using OpenVPN server, if multiple clients connect with the same client certificate, the assigned IP address will be in conflict. Ensure unique certificates are used among all clients and restart the OpenVPN server. [5043]
- When using Orbit Wi-Fi AP, typically using CCMP, high data rate may cause temporary Wi-Fi disconnects. We do not recommend upgrading to code 9.0.3 or later if using as a Wi-Fi AP with the standard Wi-Fi module (W51) [5059]
- If using OpenVPN, verify that the clients are connecting properly, if you have an errant client it can prevent a valid client from connecting correctly. [5295]
- Binding the SSH, SNMP, or NETCONF service to an IPv4 or IPv6 address can cause boot errors if that address's interface is not up at the time of boot. This can happen if the unit is rebooted with the interface disabled or in the case of WiFi, if a connection is not made shortly after boot. To mitigate this issue, firewall can be set to control what traffic passes on each interface. [5289]
- Firewall filters that have a layer 2 rule can only be applied to a bridge or VLAN interface. They will not be displayed in the tab complete or pulldown menus for other types of interfaces. [5644]
- It is not recommended to bind any service to a radio interface. [5422]
- When using OpenVPN, if data is not able to pass over the VPN and the status page indicates that the service is in error, then the unit has to be rebooted to recover. [5857]
- For W51 WiFi, when changing device mode, make sure device is disabled first, then re-enable device in new mode [5850]
- When changing the TX power of the W53 Wi-Fi, the device needs to be either disabled and re-enabled, or the entire system rebooted for the change in power to take effect. [5803]
- On configuration change of the OpenVPN service, a reboot may be required. [5670]
- In some newer ECR devices, the ingress rate limiting user interface will not include an Ingress Burst value. Ingress Rate is also restricted to specific values (64-40000, 45000, 50000, 67000, and 75000kbps). [5847]
- If a One-Time Scheduled Reboot with a reboot interval of 0 is preempted by an active reprogramming session, the reboot will be rescheduled at an invalid time. The user will have to disable the schedules reboot manually. [5871]
- For DPD operation, the retransmit/tries parameter does not affect IKEv1 retransmit count for DPD probes (This remains at the default setting of 5). [5868]

- The W53 Wi-Fi module in 802.11g mode may experience low upstream throughput. [5827]

Operational Notes and Limitations

- 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. [1121,983]
- The HTTP Protocol is not supported for exporting files. [753]
- The Terminal Server may fail if polling with VMIN = 1. Disable then re-enable the Terminal Server to regain functionality. [2402]
- Internet Explorer version 8 is no longer supported. Please upgrade this application to version 11, or use Mozilla Firefox, Google Chrome, or Microsoft Edge. [2403]
- To delete all IPv4 addresses from an interface use the following command:

  % delete interfaces interface myInterface ipv4

  [2404]
- Wi-Fi Station Bridging is not interoperable with other vendor's Wi-Fi devices. [2405]
- When the Wi-Fi interface is enabled with Dual SSIDs, Station Bridging operation is restricted to the first alphanumeric SSID. [2407]
- SCEP operations require certificate information to contain a Common Name, otherwise the operation will fail. No direct indication of failure is provided. [2052,2408]
- On a Microsoft CA server, the SCEP template used should not include Extended Key Usage. [2053,2409]
- In WebUI, there are no preconfigured file servers. This facility is only accessible from the CLI. [2410]
- 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. [194]
- 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. [2411]
- Date/Time settings on ORBIT MCR are expressed in GMT format. [2412]
- 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. [2413]
- 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 "\\". [1437]
- STP is not functional over interfaces belonging to a VLAN. [3324]
- Displaying the active routes will not show all configured routes, when connectivity to an affected subnet cannot be established. [2414]
- 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. [146,442]
- The configuration parameter to enable a specific Wi-Fi Access Point, overrides the higher level configuration to enable the Wi-Fi interface. [2415]
- 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. [2416]
- When using a Public Dynamic IP Addressed SIM card, On-Demand IPsec Mode is not supported. Always-On mode must be used instead. [227]
- 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. [1246]

- 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. [2417]
- 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. [2418]
- COM port attributes (data bits, parity, stop bits) are only applicable to data mode. When operating in Console COM ports will only supports 8N1. [1238]
- Re-authentication is not supported on an established 802.1X Port based session. The service may require cycling upon a reboot to initiate port authentication. [1031]
- Syslog is not fully compliant with RFC5424. [1028,1033]
- Nx NICs may need be configured with dwell times above 30ms if running at 125kbps. [1584]
- When NX is in store and forward mode, continuous downlink saturation may cause some nodes to be starved and not given upstream time. [1585]
- In a LN system, if modulation is forced to 64 QAM we recommend enabling FEC (forward error correction). [1327,1405]
- When running a COM port at 300 baud we recommend that vtime be set to a value greater than 35 ms. [1367]
- Preconfigured servers are not applicable to broadcast reprogramming. [2420]
- When using QoS, you cannot have a shaping policy as the next-policy of priority policy. [1544]
- When importing a configuration file that contains references to certificates, first ensure those certificates are loaded onto the unit. [1527]
- When operating Orbit LN in backward-compatible mode, degraded performance may sometimes occur in certain complex configurations that include MPRS. [2421]
- 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. [2323]
- Interfaces that user can name (bridges, vlans, etc.) should not have spaces in them. [411]
- 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. [2422]
- 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. [1805]
- When configuring L7W (Licensed 700MHz Wide), do not set NIC-id. It is not supported in this release and will prevent link establishment. [3747]
- 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. [1806]
- A QoS modify policy is not tied to an interface and must be deleted to disable it. [1542]
- 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. [1783]
- 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. [2225]
- 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. [1756]
- For LN in transparent mode, if the over-the-air rate is greater than your serial port rate, we recommend increasing either SCD (soft carrier dekey) on x790 or data key hold time on MPRS to at least 5ms to eliminate potential gaps in the transmission. [1888]
- For Wi-Fi, in some cases the configured power may not be used; instead a lower capped value may be applied to ensure proper regulatory constraints. [1891]
- 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. [1988]

- Timeout of MODBUS transactions can cause dropped TCP connections. Workaround is to increase poll rate or increase transaction timeout. [2312]
- When changing COM port usage from terminal server to passthrough we recommend a 2-stage process. Remove the terminal server followed by its own commit first; then create the passthrough instance using a separate commit. [2341]
- 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. [93]
- When running VRRP on a Bridge interface we recommend disabling STP (spanning tree protocol). [2384]
- When issuing a repeat command on the CLI, add the additional syntax "| nomore" (without quotes). [2113]
- 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. [2589]
- Performing an ICMPv6 ping to a link local address requires one to specify the src-address of the outgoing interface. [1385]
- The tamper detect alarm is persistent across reboots. It requires an explicit clear from the tamper detect menu to not reassert next power cycle. [5300]