GE MDS **PRODUCT RELEASE NOTE**

RELEASE NOTE: iNET and iNET-II Firmware Version 8.3.1
RELEASE DATE: May 25, 2022

FIRMWARE

Phone +1 (585) 242-9600, FAX +1 (585) 242-9620, Web: www.gemds.com

MDS iNET and iNET-II FIRMWARE – Version 8.3.1

Overview

This section describes Software/Firmware updates for the MDS iNET and iNET-II products.

Products: MDS iNET 300 Access Point and Remote
MDS iNET 900 Access Point and Remote
MDS iNET-II 900 Access Point and Remote

Version: 8.3.1

Release Date: 25-MAY-2022

Important Notes:

- **This release note lists changes since production release 8.1.1.**
- **Release files SHA256 sum:**

inet-8_3_1.ipk	`aab4e597f3f4295721f8fb58a577c7fb12ce54f5563d826324ab718394d05208`
inet2-8_3_1.ipk	`a43ffa566235f89ca53d8f71928789577ab990958b11fbb968798a2c499dbb67`
inet300-8_3_1.ipk	`3af70407b77656c5b8eeafe838b7a36f7d93fa1b5dd7fb57fb7be17a63eb3c37`

New Features

1. Add support for SHA224, 256, 384, and 512 certificates with Device Auth Method 802.1X.
2. Add non-persistent Validate Cert Chain setting to the Manage Certificates UIs—the setting defaults to "enabled" at every power-on. Skip chain validation when the setting is disabled to support tiered PKI without storing the intermediate or issuing CA certs.
3. Add Display Certificates to the iNET-II Manage Certificates UIs.
4. Add Login Banner setting to the Device Security UIs, cfgscript, and SNMP. This provides a 500-character banner on serial, Telnet, and SSH login consoles. When the setting is empty, the banner defaults to the Device Name (if set) or the Model Number (if Device Name is blank)—see the Device Information UIs. Non-default values bring up an alert after login on the web UI.

Changes to Existing Features

1. Authorization key values may no longer be entered before logging in to the menu.
2. HTML response headers now include "X-Frame-Options: SAMEORIGIN" and "X-Content-Type-Options: nosniff".
3. Add SNMP OID inetNcBridgeStp to control whether the bridge uses Spanning Tree Protocol.
4. Support bundles will now include the OID for SNMP requests.

5. Prevent apparent failure of web event log view by closing any existing logWindow. Handle the view log request outside the header/footer block to avoid spurious 'HTML' line appearing onscreen during generation.
6. Prevent SNTP time assignment from breaking DHCP client timeouts by using monotonically increasing time.
7. Add confirmation prompt to Send Log and Send Support Bundle console menu items, matching the web.
8. Grey out the labels of unavailable channels on the Channel Configuration web page.
9. Add source of the alarm to "AP Ethernet Link Disconnected" event log entries.
10. Change cfgscript import parsing to remove the last instance of semicolon from an input line rather than the first. This allows string parameters to include semicolon as long as the line ends with the parameter help comment.
11. Provide status feedback on console while generating and sending an event log or support bundle.
12. Change menu help prompt for enumeration settings to include Backspace key.
13. Deprecate "HTTP Enable" from cfgscript export and import—it was deprecated for SNMP in iNET release 5.7.2.
14. Reset SNR and RSSI according to device mode so Performance Information UIs continue to show "AP" on Access Points rather than changing to "N/A".
15. Reduce SNTP validation interval to ensure "Date/Time from Server" is stored as quickly as possible.
16. Allow redundancy settings to be changed while redundancy is disabled.
17. Use the Performance Information, Wireless Network Status, Connection Detail field for detailed errors with Device Auth Method 802.1X.
18. Change "Unused Event" to "Resource Running Low" for event log memory monitor entries. Perform a "MemAllc" reboot to prevent iNET becoming unresponsive once free memory reaches a critical limit (N/A to iNET-II).
19. Tag FPGA+MAC reset counts in the event log with "MAC".
20. Remove "HopSMAC" MAC reset to prevent Remotes rebooting due to lengthy scanning durations.
21. iNET-II Remotes use 10% trimmed mean RSSI while mobility is disabled and beacon learning is on association.
22. Use alternate function if shutdown fails for factory default or SNMP or web device mode change.
23. Move Reprogramming UIs' minimum build warning above Current Firmware, to avoid console error feedback.
24. Add Support Bundle to the Maintenance web page.
25. Reduce DHCP client monitor interval to keep the restart delay as short as possible.
26. Reduce console monitor process acquisition retries to keep the restart delay as short as possible.

Defect Fixes

1. Restore factory test functionality by preventing single mode switch logic.
2. Update GoAhead webserver for Authentication Header Buffer Overflow.
3. Apply patch for GoAhead Webserver CVE-2017-17562.
4. Prevent the "Rebooting..." screen being overwritten when the user selects to reboot (Device Mode, RF Hopping Format, or Reboot Device).
5. Skip power control on Remotes when association state is Scanning. This prevents "RF Power Control Saturated Low" (EVENT_POWER_LOW) alarm when Remotes remain in Scanning for extended periods.
6. Add captions to Ethernet Link settings and separate H/W Watch from Poll Address group to clarify the settings.
7. Remove unconditional syslog call in print_hop_table().
8. Check the SNTP validation response to avoid setting the system time to an outlandish value.
9. Updated build to resolve the GHOST vulnerability.
10. Use separate buffers for settings requiring a reboot so the desired value isn't overwritten with the current value (Network Config, Device Mode).
11. Restore menu help for enumeration settings with a confirmation prompt: Network Config, Device Mode; Radio Config, Hop Format; Serial Config, Port Status; Device Info, Console Baud.
12. Correct Network Configuration web page so submitting a Device Mode change takes effect.
13. Prevent System Error with SHA1 certificates by forcing SSL retries to use separate thread instances.

14. Prevent Maintenance, Support Bundle console menu returning to Event Log menu on exit if Current Alarms is viewed before entering Maintenance menu.
15. Stop concatenating EAP_TLS and EAP_INTERMEDIATE reason strings.
16. Re-enable periodic MAC timed out check for both AP and Remote.
17. Correct SNMP walk on Remotes by restricting update_sdb_cache to APs.
18. Correct SNMP inetChannelConfigTable walk.
19. Delay login prompt until radio has initialized to prevent iNET reboot at immediate login after power-on. Increase the window for core module initialization delay from 30 to 45 seconds.
20. Change console monitor logic to handle repeated logins/exits.
21. Use HTML entities so unknown IP addresses aren't blank in Remote and Endpoint Listing web UIs.
22. Ensure unknown IP addresses aren't hyperlinked in Remote Listing web UI.

Known Errata

1. RADIUS security changes should be followed by an AP reboot to ensure the changes are applied.
2. AP MAC parameter changes (e.g. RTS threshold) require a hop seed change to ensure the change is applied.
3. Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
4. Remotes may miss a change in auto-upgrade parameter when first enabled and remain associated, failing to start an auto-upgrade. Toggling the parameter with a nominal (~1 second) delay should correct the issue.
5. Remotes using dynamic IP address mode may not release an expired IP address. A power cycle will recover full DHCP client operability.
6. Remotes using dynamic IP address mode will not get configuration updates from an iNET-II DHCP server unless the server is restarted and the lease expires on the client.
7. Dynamic IP addressing (DHCP) is not supported when VLAN is enabled.
8. The DF1/EIP functionality can be accessed from either the Data or Mgmt VLAN subnets when VLAN is enabled.
9. Repeated terminations of telnet sessions may leave behind unrecovered resources, eventually leading to degraded performance. A power cycle will restore full operability.
10. Repeated enabling/disabling of auto key rotation can result in Remotes no longer associating with the AP.
11. Repeated cycling of Wireless Security, Device Auth Method from 'None' to 'IEEE 802.1X' may cause the airctl process to stop functioning and a "System Error Please Reboot" alarm to be logged. Reboot the unit to recover.
12. Changes to the console baud rate (COM1) may cause an interruption of data on the data port (COM2).
13. When operating in UDP serial data mode, the menu may improperly display the following stale message even after data is flowing correctly: "This 'IP ADDR' may be invalid for this network". If data is not flowing, disabling/ re-enabling the serial port or rebooting the device should fix the issue.
14. Loading an old config file with hop protocol = 1 to an AP will disable your network—no Remotes will re-associate. Load a hop protocol = 2 config file, change the AP's channels or reboot to recover.
15. Since iNET-II version 2.7.0 the 8ms dwell time is no longer supported. Units with 8ms dwell time will change to 16ms dwell time.

Operational Notes and Limitations

1. Functional compatibility
    - iNET and iNET-II units are not radio compatible. iNET APs cannot link with iNET-II Remotes or vice versa.
    - iNET units cannot be upgraded to iNET-II functionality.
2. Radio and data services to a unit performing reprogramming/upgrade should be avoided until the upgrade is complete. Communication may be unreliable during the upgrade.
3. Display Certificates UIs are omitted from iNET build variants due to image size constraints.
4. Networks with Wireless Security Encryption enabled may show Remotes associated in the Performance Information Remote Listing screens although data connectivity may not occur. Ensure all Remotes and the AP

have the identical Wireless Security Encryption Phrase to establish data connectivity. This should be confirmed before deployment.

5. iNET version 6.8.0 fixed an issue with reprogramming the FPGA region. Upgrading to version 6.8.0 prior to programming 6.9.1 reduces the risk of a programming issue due to Bad Image CRC by 50%. If version 6.9.1 is programmed into a unit not running version 6.8.0, multiple programming attempts may be required.
6. iNET-II version 2.5.0 fixed an issue with reprogramming the FPGA region. Upgrading to version 2.5.0 prior to programming 2.6.0 reduces the risk of a programming issue due to Bad Image CRC by 50%. If version 2.6.0 is programmed into a unit not running version 2.5.0, multiple programming attempts may be required.
7. Due to an important Access Point defect fix, GE MDS recommends that all iNET Access Points upgrade to firmware version 6.7.0 or higher. Similarly iNET-II Access Points should upgrade to version 2.4.0 or higher.
8. iNET hardware version 1.0.6 includes flash memory hardware that requires firmware version 6.7.0 or higher. iNETs with hardware version 1.0.6 will NOT function with firmware versions earlier than 6.7.0.
9. iNET-II firmware versions above 2.0.0 are not over-the-air compatible with earlier versions. All Remotes must upgrade to a version higher than 2.0.0 prior to upgrading APs above 2.0.0.