Digital Energy
MDS

PRODUCT RELEASE NOTE

RELEASE NOTE: EntraNET AP Firmware Version 5.0.8
RELEASE DATE: June 18, 2015

FIRMWARE

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

MDS EntraNET AP Firmware – Version 5.0.8

Overview

This section describes Software/Firmware for the MDS EntraNET AP products.

Products: MDS EntraNET 900 Access Point
MDS EntraNET 2400 Access Point

Package Elements: AP 5.0.8 OIB 3.0.12 TOR 2.3.3

Release Date: 18-JUN-2015

Important Notes

- **Updated build to resolve the Shellshock vulnerability**

New Features

1. Remote Serial Gateways have been enhanced to allow transmission to some remotes in addition to the ability to send directed traffic to a single remote or broadcast to all remotes. A group identifier has been added to remote serial gateway configuration on an EntraNET Access Point and this group identifier has also been added as an optional argument on either or both serial COM ports of an EntraNET Remote. A new Group Database has also been added to the Wireless Network menu of the EntraNET Access Point to allow users to view all remotes that belong to a particular group identifier. Valid group identifiers range from 0-15, the default group identifier of 0 indicates a remote is not assigned to a specific group.

   NOTE: This enhancement is not supported on EntraNET remotes running 2.x.x firmware.

2. Added Time-of-Day synchronization to the remote. This allows the remote to obtain the current date and time from the Access Point when the remote associates.

Changes to Existing Features

1. See the information about group identifier above.
2. Added a groupId parameter to the Remote Serial Gateway configuration scripts on the Access Point.
3. Added the ability to enable/disable endpoint logging via the web interface of the Access Point.
4. Added the ability to enable/disable auto key rotation via the web interface of the Access Point.
5. Added the ability to clear Remote Serial Gateway statistics via the web interface of the Access Point.

Defect Fixes

1. Updated build to resolve the Shellshock vulnerability.
2. Correctly load configuration scripts that were created in earlier software releases.
3. Remote Serial Gateway web interface no longer incorrectly terminates other RSG sessions.
4. Allow only the correct range of values, 0-1000, for Wireless Network menu item Max Remotes.

5. Prevent broadcast Remote Serial Gateway data forwarding out the Access Point's com1 console session.
6. Prevent EntraNET Access Point sporadically displaying the error message "TOR Firmware not programmed - No Tor Comms" during initial boot up.
7. Prevent EntraNET Access Point sporadically displaying the error message "TOR Needs Download" during initial boot up when, in fact, the TOR did not need to be downloaded.
8. Prevent EntraNET Access Point incorrect error message, "remMain_menu_draw: Could not read entries from the database." while using the "Manage Selected Remote Menu".
9. Properly handle downstream compressed multicast traffic to prevent IP to serial polling test failure.
10. Menu refresh was causing invalid input error message on the AP Group Database menu to be displayed but then immediately erased with the next dynamic menu display update.
11. Allow multicast remote serial gateway entries to be created when the Unit ID of the configuration was previously set to broadcast.
12. Prevent remote serial gateway data sessions terminating unexpectedly when other remote serial gateway entries are deleted.
13. Correct the group id default value for remote com2 port; it was incorrectly set to 4 rather than zero.
14. Initialize the group id for remote com2 port to 0 when first upgraded from 3.0.7 to the new firmware.
15. Properly handle multicast data to prevent IP to serial polling test failure.
16. EntraNET remote firmware changed for TOR reboot to more gracefully force the remote to disassociate from the Access Point then reassociate. Previously the code manually reset the connection address.
17. Prevent Access Point booting up in an alarmed state if IP Address Mode is dynamic and the unit was reset to factory defaults. (The unit properly obtains IP configuration from the DHCP Server but alarmed regardless.)
18. Prevent Send Event Log confirmation strings overwriting the send to host menu option.
19. EntraNET Access Point Endpoint Database display now includes the IP addresses of all endpoints.
20. EntraNET Access Point serial number is available via SNMP OID entraNetDCSerialNumber.
21. Prevent downloading the incorrect radio firmware to a 2.4 GHz radio on an EntraNET Access Point.
22. EntraNET Access Points using DHCP and Ethernet Bridging "All" or "IP/ARP Only" now acquire an IP address.

Known Errata

1. An EntraNET remote operating in DIRECT mode will erroneously show RADIO ASSOC= Remote radio associated to an AP.
2. Broadcast reprogramming will show "Some Remotes Failed Programming" when the remotes are a mix of either 1) units that do not support the 2MB expanded flash and units that do, or 2) EntraNET and NETio units.
3. If an EntraNET remote is rebooted while the Access Point is reprogramming it, the percent complete status indicator will remain unchanged until the Access Point is rebooted.
4. Selecting Image Verify at the console when a reprogramming process has been started from the web will show "Image copy in process" and the console may lockup. Power cycle the Access Point to recover.
5. An EntraNET Access Point using DHCP may erroneously report an "IP Address Invalid" alarm if the static IP Address is the default 192.168.1.1. Set the static IP Address to a different, valid address to resolve this.
6. An EntraNET 2.4 GHz FCC Standard Access Point may erroneously report an invalid radio output power range. Reboot the unit to clear this condition.
7. When downgrading remote firmware from 3.0.12 or higher, the remote may show incompatible log entries with the 'log show' command. These entries are not destructive and can be safely ignored or deleted.
8. Conflicting RSG configurations can occur when group broadcast configurations are created in 5.x and then more configurations are created in 3.x. When the Access Point is rebooted to 5.x, some group broadcast entries may be overwritten, while others reappear and could possibly be in conflict with those created in 3.x.

Operational Notes and Limitations

1. Using 7ms hop time may reduce IP throughput. Maximize system throughput with 14ms or 28ms hop time.