November 2018 AcquiSuite/AcquiLite Firmware changes

Version **v02.18.1117** for A7810, A8810, A8812, and A8814.

Users should be aware of these changes and how these may impact any custom applications that may have been developed. Although great care has been taken to maintain the previous feature set, users should test the firmware update prior to deploying this firmware on production equipment.

The firmware update will be provided at no cost.

***IMPORTANT**: After updating firmware, please **press CTRL-F5** in your browser window to cause the browser to reload any cached web files from the AcquiSuite/AcquiLite.*

Overview of Changes

- BACnet/IP is now part of the core firmware, and we've introduced BACnet/IP Logging.
  - **BACnet/IP Logging:** We've added logging of BACnet objects over the IP protocol, and both BACnet and Modbus data points may be used in Virtual Meters. Note that BACnet/MSTP is not supported at this time, however the AcquiSuite may log data from or share data to BACnet/MSTP devices through 3rd party BACnet/IP-to-MSTP gateways.
  - **BACnet/IP Server/Gateway** is off by default, unless you had previously installed our BACnet Server add-on module.
  - As a reminder, our BACnet/IP Server/Gateway features:
    - BBMD and FDR (server-side) support, to simplify spanning IP subnets.
    - Automatic sharing of Modbus, Modhopper-connector or Virtual meters via BACnet/IP.
    - See http://www.obvius.com/sites/obvius.com/files/BACnet_Users_Guide.pdf
- Improvements to **Template editor**.
- Improvements to help visualize **System RAM & Flash usage** and to handling of **"Flash-memory-full"** situations (see below for details).
- Security improvements.
- Various fixes to Meters, Sunspec, BACnet, and Templates.

Security-Related Changes in v02.18.1117 compared to previous release (v02.17.1003):

- **Security**: Update **thttpd** web server to 2.28 (latest version).
- **Security**: Update **dropbear SSH** to 2018.76 (latest version).
- **Security**: Improve **Cross-Site-Scripting (XSS) protection** by adding HTTP header X-XSS-Protection: 1; mode=block).
- **Security**: Improve **Cross-Site-Scripting protectio**n by not echo'ing URL in error pages for HTTP 403, 404 errors.
- **Security**: **Block listing of /images** (in fact, of all subdirs under web root) to prevent false positives from scanning tools.
- **Security**: Fixed several (potential) printf-format security issues (very unlikely to be exploitable; result of code reviews).

Major Changes and New Drivers in v02.18.1117 compared to previous release (v02.17.1003):

- **BACnet/IP Logging Feature Summary:**
  - Our existing BACnet Server/Gateway and new BACnet/IP Logging features have been integrated into the base AcquiSuite firmware. If the Obvius_BACnet add-on module is installed, it will be

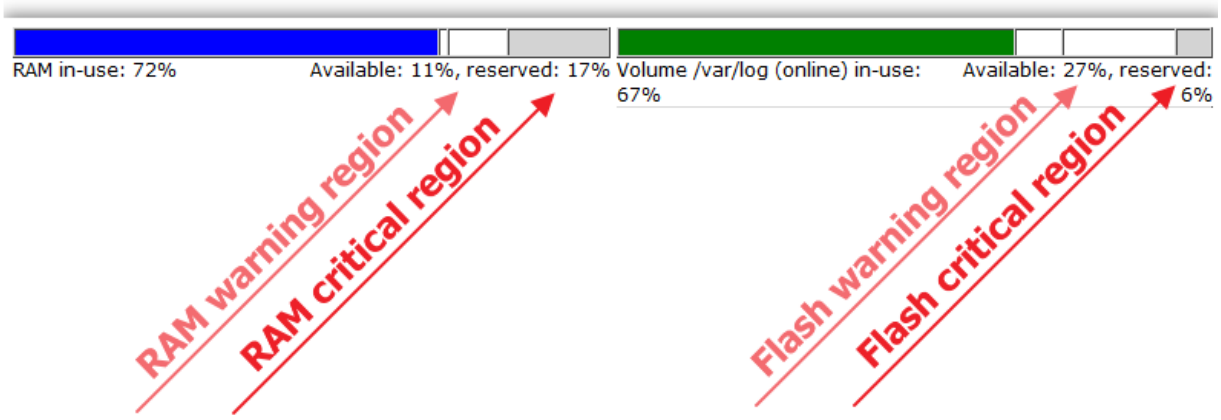
disabled (but not deleted) when upgrading to this firmware version, and the old module will be deleted to recover flash memory.
    - **Unified Device List** may contain BACnet, Modbus/RTU, Modbus/TCP or Virtual meters.
    - BACnet Logging is **compatible with all existing upload protocols** (e.g., BMO, FTP, etc), and should not require any changes to back-end server databases.
    - **BACnet Units** (e.g., kWh) are automatically mapped to the standard representation used by the AcquiSuite, and these also should not require any changes to back-end servers.
        - If Units cannot be automatically mapped or are incorrect, use the Template editor to manually adjust units.
        - Each BACnet point may also be Scaled and Offset (y = mx+b). This feature is used automatically to allow converting certain BACnet units where there is no 1-to-1 mapping.
    - **BACnet Object Types** supported for Logging:
        - Analog Input/Value/Output (AI/AV/AO)
        - Binary Input/Value/Output (BI/BV/BO)
        - Multi-State Input/Value/Output (MSI/MSV/MSO)
        - Accumulator
    - BACnet supported **BBIBs** for Logging:
        - DS-RPM-A with fallback to DS-RP-A.
        - Segmentation not supported.
    - BACnet meters may be added to the Device List in 2 ways:
        - **Via the BACnet > Discover** tool, to discover BACnet devices via Who-Is.
        - **Via Devices > Device List > Add**, and manually typing a BACnet Device Object ID.
    - When adding a BACnet device by either of the above methods, you may select to automatically detect the Objects to be logged. Several Object Filters are available:
        - **Auto-detect all Input Objects** (AI, BI, MSI, Accumulator)
        - **Auto-detect all Input and Value Objects** (above + AV, BV, MSV)
        - **Auto-detect all Support Object Types** (above + AO, BO, MSO)
    - Our Object Auto-Detection process generates a Template, which lists all the Objects that the AcquiSuite will log. **This Template may be edited at any time to change the Objects being logged.** Once customized, Templates may be re-used when adding additional devices of the same type to streamline the commissioning process. Templates may also be downloaded, backed up, and shared with other AcquiSuites.
    - Our BACnet Discover tool also **detects and warns about common configuration errors across the whole BACnet network,** such as duplicate Device Object IDs, and duplicate Virtual Network Numbers.
    - BACnet Error Handling:
        - When reading any Object, we query both its Present_Value and Status_Flags properties. If the Status_Flags property exists, we use this to determine if Present_Value is meaningful. If Status_Flags does not exist, we assume Present_Value is always meaningful for compatibility with older BACnet devices.
        - BACnet errors are mapped to AcquiSuite error codes (these codes appear in log files and are uploaded to servers). Thus, servers should require no changes to support BACnet devices.
        - BACnet “DEVICE_BUSY” error is transparently retried (per BTL's recommendation to BACnet gateways).
    - **Device > Device List**: Show icons in Device List to visually indicate device's endpoint-type (BACnet, Modbus, built-in, virtual-only, etc.)

- **BACnet/IP Server/Gateway Improvements:**
    - **BACnet: Allow BACnet/IP ports** from 0xB000 to 0xBABF to UI dropdown (total range: 0xB000 to 0xBFFF.) We recommend using ports in this range to avoid conflicts with other protocols or future features.
    - **BACnet: Gateway feature is now off by default** to avoid increasing RAM use in existing configurations or for customers who do not wish to use BACnet.

- **BACnet: Gateway may be enabled/disabled** via new option on BACnet >> Gateway page:
  - Meters shared via BACnet: {All, None}
  - Default value is None.
- **BACnet: Automatically enable the Gateway feature** if the Obvius_BACnet.asmodule.cramfs add-on was present on the system. Only reason to have installed Obvius_BACnet add-on was to use Gateway feature. This allows users of the Obvius_BACnet add-on to seamlessly upgrade.
- **BACnet: Delete the Obvius_BACnet.asmodule.cramfs**, if present, now that it's built-in. This lets users of our old BACnet module to seamlessly upgrade and automatically recover the flash used by the old module.

- **Template Improvements:**
  - **Templates**: Our Template editor now includes a "Delete Selected Points" feature, to allow deleting points in bulk. This is useful for customizing automatically-generated BACnet Templates, by removing unneeded points.
  - **Templates**: By default, we allow 256 points in a Template. The "Extended Number of Points" option now raises this limit to 1024 points (previously it raised it to 512) for customers who require a very large number of points per device.
  - **Templates**: Template editor now displays *all* points in the Template, even if greater than limits, rather than truncating what is displayed. BACnet's auto-detection process may generate Templates which greater than 1024 points. This change allows users to always be able to view or edit a Template, even if it contains more points than the system's Template driver is able to log.
  - **Template driver**: if NUMPOINTS= in Template are > 1024, we will now log from only the first 1024 points (rather than failing entirely). The expectation is that users will edit the Template.
  - **Template/Upload**: Remove Modbus-isms. Update for changed URLs of templateui.cgi, templateui.html.

- **Improved Visualization of System RAM and Flash Usage, and Improved Handling of "full flash" Conditions:**
  - Historically, Obvius has given this simple guidance to customers: "Each AcquiSuite can support up to 32 devices in the Device List." As we add features and new meter drivers, this simple guidance is no longer sufficient. There is a significant difference in RAM use between a meter with 25 points and one with 1000 points, and certain features, such as BACnet Gateway or SSL consume significant RAM when enabled.
  - To help customers gauge the effect on system RAM and Flash of particular configuration changes, we've added RAM and Flash usage bar-graphs, shown at the bottom of each page of the Web UI, to help users *visualize* the effect of their choices and changes. For example:



  - **Each bar-graph will change to color red** when the resource enters the Warning or Critical region.
  - **To use the new bar-graphs,** simply *notice* the effect on RAM or Flash as you add Devices or enable Features, and stay out of the **red** regions.
  - The **Critical** regions of RAM and Flash usage (shown in gray on the bar-graphs as "**reserved: %**")

are the amount of RAM or Flash that *must* remain free to proper operation of the AcquiSuite in a minimal configuration. This is the only important limit.
    - The **Warning** region is just that – a *warning* that RAM or Flash are *approaching* the **Critical** limit. The Warning region is included as part of the "% available", because it is acceptable if the system occasionally enters the Warning region. For instance, this may happen when the system performs an upload cycle, because the tasks which only run during uploading consume ~10% additional RAM.
    - Finally, **note that actual RAM or Flash usage varies as the system runs** (for instance, if it is running an upload cycle, or if someone is using the Web UI). **RAM usage, in particular, varies quite a bit, nearly ~20%, which is the size of the "reserved" portion**. Customers should take into account this natural variation when judging RAM usage: Don't just look at RAM usage once, but rather look at RAM usage over time as they system runs, uploads, detects and dials out modems, etc.

    - **DevList**: **[devinfo]** tab now shows # of Points per Meter, to give the user a sense of system resources consumed by each device and to help with diagnosing out-of-RAM conditions.
    - **WebUI: System >> Status**: Don't show old-style memory usage; isn't very accurate.
    - **WebUI: System >> System Logs**: Don't show (redundant) flash usage bargraph. It's in footer now.
    - **System > Processes**: We now use the Processes > Advanced viewer as the default.
    - "Priv RSS" column has been renamed to "RAM".
    - **System > Processes**: Clicking column-headers now sorts by the column, DESCENDING, rather than ascending.

- **Improved handling of "Flash memory full" condition:**
    - "Flash memory full" means Flash usage approaching the 94% Critical/reserved, 6% free threshold (see bar-graphs above).
    - Full flash memory can make the AcquiSuite extremely sluggish to the point of being nearly unusable, resulting in "CGI timeouts", which in turn can make it difficult to fix the underlying cause.
    - In this release, we've improved our handling of Full flash memory conditions.
    - Full flash memory may happen for several reasons:
        - Persistent upload failures causing meter data to "pile up",
        - "Upload debug info level" set to "Full Debug with Trace", and especially with multiple Upload channels enabled. The debug log simply consumes a large amount of Flash.
        - Too many AcquiSuite Modules installed.
        - Too many total data points being logged, too frequently, which depends on the number of Devices in the Device List *times* the Number of Points of each Device *times* the data logging interval.
    - Changes to improve full flash handling:
        - "Upload debug info level" is ignored if flash is >= 75% full to avoid making a "full flash" problem worse. Logging level temporarily reverts to "Errors & Summary". "Full Debug", if selected, will resume when/if flash is < 75% full.
        - If flash is >= critical threshold (95%) full, we will purge files to reach warning threshold (75%). Previously, we purged files to *stay at* the 95% threshold, which didn't allow any space to actually debug or fix the problem.
        - ***NOTE 1**: This has no effect on the Maximum Offline Time; it is still based on the time to reach 95% full.*
        - ***NOTE 2**: Above our warning threshold (flash 75% full), we will first purge old sessions of all diagnostic log files to try to recover flash space, but we will keep current sessions to allow diagnosis & debugging of Upload or PPP problems. At our critical threshold (flash 95% full) we will purge all diagnostic log files, and then purge user-data files (oldest first).*
        - ***NOTE 3**: Customers who have implemented their own BMO-compatible Upload Server may remotely monitor flash usage to allow proactive response via the BMO Upload Protocol. % Flash In Use is reported as an HTTP Form Variable on every upload attempt to each server of each enabled Upload Channel. The AcquiSuite's "Weekly Health Monitor" upload choice*

allows using an Upload Channel to monitor system health without uploading data, as does our Selective Upload feature.

Other Fixes in v02.18.1117:

- **SunSpec Fixes:**
  - **Sunspec**: Improve discovery of SunSpec inverter models to prevent falsely loading a SunSpec inverter driver for some SunSpec model other than an inverter.
  - **SunSpec**: Added #defines for all of the SunSpec inverter models supported (101/102/103/111/112/113).

- **BACnet/IP Fixes:**
  - **BACnet/IP Gateway**: Startup faster by not waiting for devices which are in the middle of auto-detection.
  - **BACnet:** Fix phantom BACnet “Device 0” appearing in Discovery results.

- **Template Fixes:**
  - **WebUI menus**: Change "Device > Framework" terminology to "Device > Templates".
  - **Template/Curvescale Upload:** On upload, sanitize new Template (*.mbt) or Curvescale (*.cst) filenames by replacing meta-characters with underscore (“_”). Existing files are not affected. Recognize uppercase *.MBT, *.CST. Discard unrecognized file-types (*.pdf, *.doc, no extension, etc). Install only *after* sanity-checking files, set proper file permissions.
  - **Templates**: Fix Template sanity-check to allow BACnet, Virtual Only templates. Refactor Template code into lib.
  - **Template Editor:** Improve readability of Template picklist by showing only filename if device-type equals filename.
  - **Templates**: Fix UINT16 showing negative values if value has high bit set (e.g., >= 32768 before scaling).
  - **Templates**: Fix Template Point's data-type not being saved in Edit Point dialog. Previously, would always revert to UINT16.
  - **Device Readings**: Fix showing of Modbus slave ID number, and, if Template device, include "(edit)" link to Template editor.

- **A8814/graphics console**:
  - Fix warning: empty body in an if-statement in listmenu.c:341:ListMenu_RenderHeader, modbusdevice.c:260:MBDeviceMenu_RenderHeader.

- **Meter Fixes**:
  - Meter **WattsonMarkII** Fixed a typo in the Active Power units from kWh to kW.
  - Meters **E23**, **Sage**, **SMA3k5kTL, Veris CWLP**, **Ion**, **SharmMP200Y**, **Veris HWLP**, **Veris TWLP**: Fix array-out-of-bounds access. Results of code review. Never reported as a problem.
  - Meter **pm800**: Fix several cases of incorrect negative-number handling. Results of code review. Never reported as an problem.
  - Meter **pm800**: Fix conversion of negative values of 'True Power Factor, Total'. Never reported as problem. Results of code review.
  - Meter **e5600**: Fix undefined behavior in reading/converting S/N. Never reported as problem. Results of code review.
  - Meter **kv2**: Fix logical-op warning on modbus address in Advanced Config page. Never reported as problem. Results of code review.
  - **Dent PowerScout HD48:** Fix data-log timestamps always showing as 1969-Dec-31 23:59:59.
  - **SunSpec timestamps** – same as above.
  - **SunSpec Rainwise timestamps** – same as above.

- **Miscellaneous Fixes**:
  - Support for **Remote Assist 2.0.**
  - **A8810/A7810**: Fix blank LCD. Contrast not set properly.
  - **System > Backup**: Properly back up Template filenames containing spaces. Previously, a template *.mbt filename contains spaces would cause Backup to fail with a network error; a valid backup was not produced.
  - **WebUI Navigation Bar:** Fix layout to avoid ugly/useless scroll-bars, esp. in MSIE.
  - **WebUI Navigation Bar**: Improve browser's caching by using absolute references to '/image/...'
  - deviod_polled: Optimize ReadLoggerConfiguration() to only re-read if timestamp changed. ("deviod_polled" was previously "modbusloggerd").
  - **Modbus error reporting**: Give priority when reporting errors to _retryable_ errors (so we trigger retry behavior).
  - **Meter Units**: Add 'sec' and 'min' as alias units for 'seconds' and 'minutes'. Change szMIN_UNITS[] from "Min" to "min" for consistency and correctness (lowercase "min" is the more common abbreviation from "minutes").
  - **RAM optimization**: Allocate 4k 'GCB' buffer ONLY WHEN NEEDED rather than in every app on system.
  - **RAM optimization**: call malloc_trim() in modbusloggerd, bacnetdiscover to attempt to return RAM back to system.

New Drivers and Major Features in v02.17.1003:

- **SunSpec Inverter Driver:** This driver supports the following SunSpec models; 101, 102, 103, 111, 112, 113 and a large portion of the "Immediate Controls" model 123.
  - Models 101, 102 and 103 are single, dual and three phase models based on 16 bit Modbus registers.
  - Models 111, 112, and 113 are single, dual and three phase models based on floating point Modbus registers.
  - SunSpec also supports three base register offsets from Modbus Register 40001. These offsets are the following; 0, 40000 and 50000.
  - SunSpec Immediate Controls model 123 is partially supported by allowing adjustments of the following controls (with respect to the inverter nameplate rated power production):
    - Power Output Percent
    - Power Factor (Cosine of Angle)
    - Var Output Percent (Reactive Power)
  - This driver supports both RS-485 and Modbus/TCP connections.
  - This driver requires at least one of the following 101,102, 103, 111, 112, 113 data measurement models.
  - This driver supports an Immediate Control model if it is supported by the inverter where an optional section appears on the Advanced Configuration page.
  - Other SunSpec non-inverter devices are not supported.
- **Miratron**: Added an "Advanced" button option on the lower right-hand corner of the 'Configuration" page.
- **Leviton Slave Id's:** support for A7810, A8810 branding as well as A8832, A8911, R-9120 Modbus
- peripherals.
- **A7810**: Fix device 250 showing incorrect input modes (actual fix was to Hw Revision Modbus Read Reg #41014).

New Drivers and Major Features in v02.16.0919:

- **Bundle several common AcquiSuite Modules on factory-fresh units:** "Obvius_SSLUpload", "Obvius_Xmem" and "AcquiSuite_RootCerts" are now bundled from the factory. They may be removed or upgraded by the user. Customers upgrading firmware may choose to add these Modules via System

>> Firmware Version. They are available free-of-charge.

- **LevitonBMO 3.0**: Add upload-protocol choice for Leviton BMO 3.0 (http://promo.leviton.com).
  - *Note: LevitonBMO 3.0 with SSL/TLS security requires the Obvius_SSLUpload module be installed.*
- **Reset-to-factory-defaults**: Fix: Some files not being deleted by reset-to-factory-defaults. We now perform the reset at runleve 1 (single user) so that all application daemons are stopped.
  - *Background: Reset-to-factory-defaults is selected from the LCD's Advanced menu.*
- **Auto-updates**: Increase the extra free space we create from 8kB to 200kB when trying to download firmware if flash is nearly full.
  - *Background: If flash is > 92% full [900kB free] when we try to install firmware over the web, either manually or automatically, we purge the oldest logs to try to free enough space for the upgrade; we now 'pad' this with an extra 200kB, to allow for the fact that flash will fill up [due to logging] while we download the firmware, especially over slow modems! So, if we're installed asarm.cramfs which is ~2 MB, we'd try to free 2.2MB. We only do this if we're at the point of discarding logs anyway because flash is nearly full.*
- **Remote Access (RA)**: Fix: Detect and report dead connections within 30 sec instead of 5 min by enabling SSH keepalives.
- **RA**: Fix: LoginLimit should allow web login as “admin” via RA even if “admin” password hasn't been changed.
  - *Background: Even if Telnet, FTP or SSH are enabled, if the “admin” password hasn't been changed from the default, login is blocked from “public” IP addresses as a security measure.*
- **RA**: Fix: Change LCD message from "Check firewall" to "Check router/fw".
- **RA**: Fix: Eliminate 5 minute delay before RA tries to connect when enabling RA from LCD immediately after a factory-reset.
- **SSH**: Fix: Service should be disabled (No/TCP Port Closed) if SSHLOGINENABLED= is not present in loggerconfig.ini, so that upgrading customers aren't alarmed by port 22 being open.
  - *Background: Factory-fresh units will have Telnet, FTP and SSH all set to "No (TCP Port Closed)". Users upgrading firmware will have SSH set to "No (TCP Port Closed)".*
- **SSH**: Fix: With SSH now defaulting to "No (TCP Port Closed)", it cannot be enabled.
- **Backup/Restore**: Fix: Missing printf() format: printf(szBuffer) --> printf("%s", szBuffer).
- **Modbus Custom Processing**: Increased the response buffer to avoid truncating long responses.
- **Modbus Custom Processing**: Changed response field to multi-line text box.
- **System >> Setup**: Fix spurious error msg about minipnpd if Enet is unplugged when Apply is clicked.