CYLON® TECHNICAL BULLETIN NO. 537
Issue Date: 07 August 2024

ASPECT® v3.08.02

Summary

The ASPECT® v3.08.02 release introduces comprehensive security upgrades aimed at fortifying the integrity of our software. In addition, several user-centric improvements are included to enhance eXplore tablet performance, streamline project deployment procedures, and introduce new editing features.

Detail

DON'T EXPOSE YOUR DEVICES ON THE INTERNET

Although a comprehensive discussion of network security is far beyond the scope of this document, the following items provide a starting point for creating a secure installation of equipment. Where available, users should always defer to the security policies of the hosting network organization.

1. Always ensure that the ABB Cylon BEMS (Building Energy Management System) solution is deployed on an isolated network specifically designated for BEMS controls only, with no connections to external networks.
2. Strictly prohibit the connection of ABB Cylon BEMS devices to networks that include security-critical IP devices, such as CCTV systems, any data-sensitive infrastructure or credit card terminals.
3. Under no circumstances should ABB Cylon BEMS solutions be exposed to the Internet. The exposure turns your system into a potential target accessible by every individual and machine globally.
4. Adopt a zero-exposure policy for ABB Cylon devices on the internet. Always prioritize security by limiting information exposure to the absolute minimum necessary for operational functionality.
5. Mandate the use of Secure Virtual Private Networks (VPNs) for all remote access requirements and always employ a Firewall for services requiring internet connectivity. VPNs ensure that devices remain off the public internet while providing a secure and encrypted path for authorized users to access system functions.

For more details see HT0038 ASPECT, FBXi and CBXi System Network Security Best Practice

INSTALLATION

Note: **ABB recommends that all unnecessary ports are closed on an ASPECT device.**
After upgrading, always review port configuration for any unnecessarily open ports and close accordingly.

In order to take advantage of product enhancements and resolutions in ASPECT v3.08.02, you must upgrade the firmware of your existing ASPECT target (MATRIX Series, NEXUS Series, ASPECT-Enterprise) using the System Update feature within the WebUI of the target.

Instructions on this process can be found in the ASPECT-Studio Online Help at any time. Once your target's firmware has been updated, you must then open your existing project using ASPECT-Studio v3.08.02. Perform a Clean and then deploy your project to the target. This process must be done to ensure your project files receive all enhancements and updated drivers included as part of this maintenance release.

SECURITY IMPROVEMENTS

In response to recent security assessments and internal reviews, we have implemented a series of updates to address vulnerabilities and improve the overall security of our product.

GENERAL IMPROVEMENTS

- An issue has been fixed whereby previous upgrades can potentially open previously closed ports.
- Float numbers are now correctly rounded when editing using an increment/decrement button in ngAdmin. i.e. Data Type is set to `Float`, with an Edit Step set to a number with decimals (e.g. `0.1`).
- Chrome browsers will now accept "generated" SSL certificates from an ASPECT target.
- An option has been added to the WebUI to tail `aspect1`/`aspect2`/`MIX` log files to aid in general debugging of various ASPECT issues – e.g. driver/communications, deployment etc...
- Valid SSL certificates are now negotiated automatically for outgoing connections for Calendar, SMTP, Business Analyzer and Pushover connections
- A `v3.08.01` issue has been resolved that did not allow Unitron formatted device IDs to be inputted into the Network device Device ID field. This bug was non-destructive, meaning that it did not destroy device IDs for Unitron networks.
- Alarm notifier has been modified to submit email requests to a queue in the event that the SMTP mail server is slow. This will allow timely reporting of alarms on systems when the mailer is slow and several alarms are triggered simultaneously.
- Tooltip information in ASPECT-Studio has been improved for the DeviceID field on a Network device to help mitigate communications configuration errors.
- Editing of graphics elements is now enabled when a customer is using kiosk "Green Screen" mode to display a graphic. This option is togglable from the Aspect Global Configuration Overrides page in an ASPECT target using allowKioskModeEdits=`true` flag.
- An option to set character encoding has been added to MySQL configuration, to support writing Chinese characters to Alarm and Audit tables in ASPECT targets.
- ASPECT points can now be bulk- edited from ngAdmin in the same way as Network points.
- Passwords of up to `64` characters are now allowed for LDAP authentication
- An option to toggle support for Web Sockets is now provided to allow data captures using the "Matrix" method
- Wording on SSL Configuration pages has been changed to reflect the modification that makes SSL configuration "general" for the product rather than for eMap driver configuration.
- Graphics display is now optimized when projects are accessed using ABB's eXplorer touchscreen devices. This feature is made available by toggling the allowGestures=`false` property in the ASPECT overrides.
- Single file deployment no longer fails intermittently if the ASPECT Control Engine was down or restarting during a deployment.
- A timing issue that led to single file deployment occasionally failing has now been resolved.

DEPRECATED FEATURES

The following features in ASPECT have been deprecated to enhance security and increase usability of the product.

- CalDAV / Biakal calendaring has been removed from ASPECT due to security considerations.
- vStat configuration has been removed from ASPECT - this option had already been deprecated from ASPECT, this update removes all configuration files from the product for security reasons.

Customer Impact

Note: **ABB recommends that all unnecessary ports are closed on an ASPECT device.**
After upgrading, always review port configuration for any unnecessarily open ports and close accordingly.

Users **must upgrade as soon as possible** to ensure their ASPECT targets are secure and to take advantage of the latest features and improvements.