ABB CYLON® TECHNICAL BULLETIN NO. 551
Issue Date: 23 July 2025

ASPECT® v3.08.04-s01

Summary

The ASPECT `v3.08.04-s01` release includes General Usability and Security improvements. These improvements are the result of customer feedback and rigorous security assessments and represent a significant strengthening of ASPECT against potential threats.

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 equipment installation. Where available, users should always defer to the security policies of the hosting network organization.

1. Always ensure that the ABB Cylon® Building Energy Management System (BEMS) 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. ABB Cylon® BEMS solutions should never be exposed to the Internet. 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 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 closing all unnecessary ports on an ASPECT device.**
After upgrading, always review port configuration for any unnecessarily open ports and close them accordingly.

GENERAL USABILITY IMPROVEMENTS

ASP-7737 A configuration option has been added to control the "`Web Server Connection Lost`" message in `ngAdmin`.

SECURITY UPDATES

Note: **There will be a Vendor Security Advisory published for the vulnerabilities patched in this release. All ABB Product Advisories can be found here: ABB Cyber security alerts and notifications**

ASP-7746 Application Servlets have been hardened to prevent unauthorized access

Customer Impact

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

Note: ASPECT `v3.08.04-s01` is an irrevocable upgrade meaning if an ASPECT target has been upgraded to `v3.08.04-s01` it cannot be backed down to any pre-`v3.08.04` release.

Note: ASPECT is not designed to be an "internet-facing" server application. If you need to access the ASPECT device remotely, you should do so through a secure VPN (and not a publicly accessible internet domain).

Note: ABB recommends that all unnecessary ports are closed on an ASPECT device.
After upgrading, always review port configuration (WebUI > Communication Setup > IP Port Administration) for any unnecessarily open ports and close accordingly.

Note: It is recommended that `.aam` file checksums are verified against those published on the online ToolBox before a System Upgrade is performed.

Note: If you have any difficulty accessing ASPECT after upgrade, you may need to:

1. Clear your browsers history/cookies and restart the browser to clear out the older version/data (performing a hard refresh with Ctrl+F5 is an alternative option).
2. If login is still not working after clearing the cache, you may need to use the alternative WebUI login page at `https://192.168.0.1/altlogin.php` (replace the IP with your device's host/IP).