HOW-TO GUIDE

HT0038 Rev 12

FBXi, CBXi and ASPECT® SOLUTIONS

Network Security Best Practice

This document describes networking within the ABB Cylon Building Environment Management System (BEMS), in order to identify Security considerations and aid troubleshooting for Ethernet Networking on ABB Cylon systems.

CYBERSECURITY DISCLAIMER:
This product is designed to be connected to and to communicate information and data via a network interface. It is your sole responsibility to provide and continuously ensure a secure connection between the product and your network or any other network (as the case may be). You shall establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, secure VPNs, application of authentication measures, encryption of data, installation of anti-virus programs, etc.) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB Ltd and its affiliates are not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

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.

NETWORK SECURITY STRATEGY

ASPECT, FBXi and CBXi devices are designed for trusted network communication only. If Remote access over untrusted networks is required, then it must be implemented over VPN tunneling where the customer is responsible for ensuring that it complies with the latest security standards.

Do not mix secure platforms with platforms that are not secure on the same network. All controllers and Supervisor stations must be secure.

CHANGE "FACTORY DEFAULT" CREDENTIALS

Most important: **do not use default or weak passwords at any of the Internet access points!**

a) You should always change your passwords from the defaults shipped from the factory.

b) Change the passwords to all elements that are network enabled, whether you are implementing these features or not. For example, even if you are not utilizing the MySQL database, change its default passwords.

c) You should always use strong passwords for any accounts that have the authority to make any changes to the system. Strong passwords include all of the following: upper and lower-case letters, numbers, and punctuation. Example: `pR10r!tyh@ndl1nG`

PATCH YOUR SYSTEMS

Always upgrade your system to the latest software version. Install all patches and software updates.

- The latest versions of our software may be accessed at ABB Library - HVAC Software (login required).
- Release notes for HVAC software may be found at ABB Library - HVAC Technical Bulletins.

For further information contact the BHAS Global Competence Centre:

- North America only: us-sbs.support@abb.com
- Rest of World: global-sbs.support@abb.com

USE ENCRYPTED COMMUNICATIONS

Cyber criminals are crafty, but ASPECT®, FBXi and CBXi put some extremely effective barriers in their way. Integration with SSL and HTTPS takes security to a whole new level of fortification against hacking and unauthorized intrusions.

Only install browsers using a trusted installation program. The program you use installs third-party certificates from CAs, such as VeriSign and Thawte. These must be trustworthy certificates.

SELF-SIGNED CERTIFICATES VS SIGNED CERTIFICATES

It is common to create a local Certificate Authority and issue certificates from it. This is typically referred to as a Self-Signed Certificate. Self-Signed Certificates are cryptographically as strong as Signed Certificates obtained from a Trusted Certificate Authority but incur no cost. The key limitation to Self-Signed Certificates is that they will not be trusted by any modern web browser without additional per-client configuration. This is because the locally created Certificate Authority is not trusted by the browser by default, therefore do not use Self-Signed certifications on a public website.

SIGNED SSL CERTIFICATE LIMITATIONS

In order to obtain and install a certificate for any web server (including ASPECT® FBXi and CBXi Systems), the following items are required:

1. A valid DNS name.

   It is not possible to obtain an SSL certificate for an IP address. `https://aspect.customer.com` and `https://aspect.bms.customer.com` are considered two different hostnames, and typically a signed certificate only applies to a single hostname. Be careful if using Split-DNS for internal vs external access.

2. Authority to purchase a certificate on behalf of the domain in which the system will reside.

   There are varying levels of identity verification required to purchase an SSL certificate, ranging from simple "domain control" validation to phone calls, interviews and financial queries for higher certification levels. For domain control verification, it is typical to have to prove administrative control for a given domain name. This will generally consist of one or more of the following:

3. Ability to create a specific DNS TXT record with a specified value
   - Ability to place a specific document or tag into a file on a web server on the domain in question.
   - Receive and respond to emails issued to addresses historically reserved for DNS or Webmasters of a domain (`hostmaster@customer.com`, `webmaster@customer.com`)

4. Payment for certificate.

   Certificate costs vary greatly from issuer to issuer. As long as the issuer is trusted, there will be no difference in the security of the certificate issued by Certificate Authority A vs Certificate Authority B.

DON'T FORGET PHYSICAL SECURITY

The best security protection is to ensure that no Device is physically connected to any untrusted network, or even to keep BMS networks isolated from any other networks that might be compromised from untrusted networks or the internet.

Physical security is crucial. Secure all computer equipment in a locked room. Make sure that each station is only accessible by authorized users.

Physically protect wiring to prevent an unauthorized person from plugging in to your network.

DON'T FORGET ABOUT "PEOPLE"

The root cause for 30 percent of data breach incidents is human negligence, according to the Ponemon Institute *Cost of Data Breach Study*. Often this is due to the lack of expertise required to implement security controls, enforce policies or conduct incident response processes.

Training employees on risk-mitigation techniques including how to recognize common cyberthreats such as a spear-phishing attack, best practices around Internet and e-mail usage, and password management. Failure to enforce training and create a security-conscious work culture increases the chances of a security breach.