HOW-TO GUIDE

HT0038 Rev 19

FLXeon, CBXi, ASPECT®, CB and UNITRON 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.

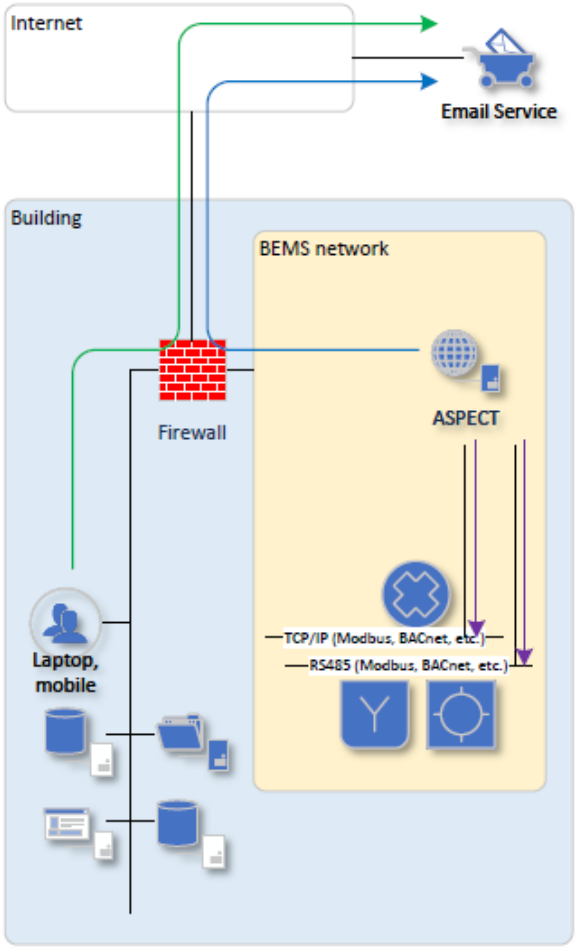
NETWORK SECURITY STRATEGY

ASPECT, FLXeon, CBXi, Unitron and CB-Line (CBR) 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.

Make sure that network devices and services intended for Building Automation are kept separate from devices and services intended for other purposes (e.g. office computers used for business operations, printers, entertainment systems, etc.).

All controllers and Supervisor stations must be secure.

OUTWARD COMMUNICATIONS

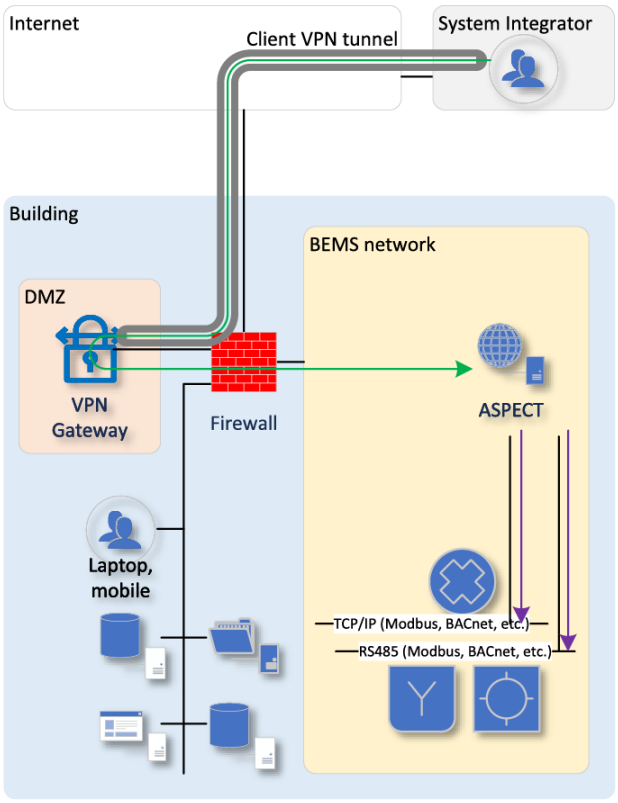


Disclaimer: The concept diagram does not reflect the actual implementation details, which must be covered in HLD/LLD documents.

The ASPECT, BACnet or Unitron application may access external resources such as mail service, information services, and others. The firewall must enable outbound connectivity to required services.

Company employees or system integrators receive alerts through their respective email services.

REMOTE ACCESS



Disclaimer: The concept diagram does not reflect the actual implementation details, which must be covered in HLD/LLD documents.

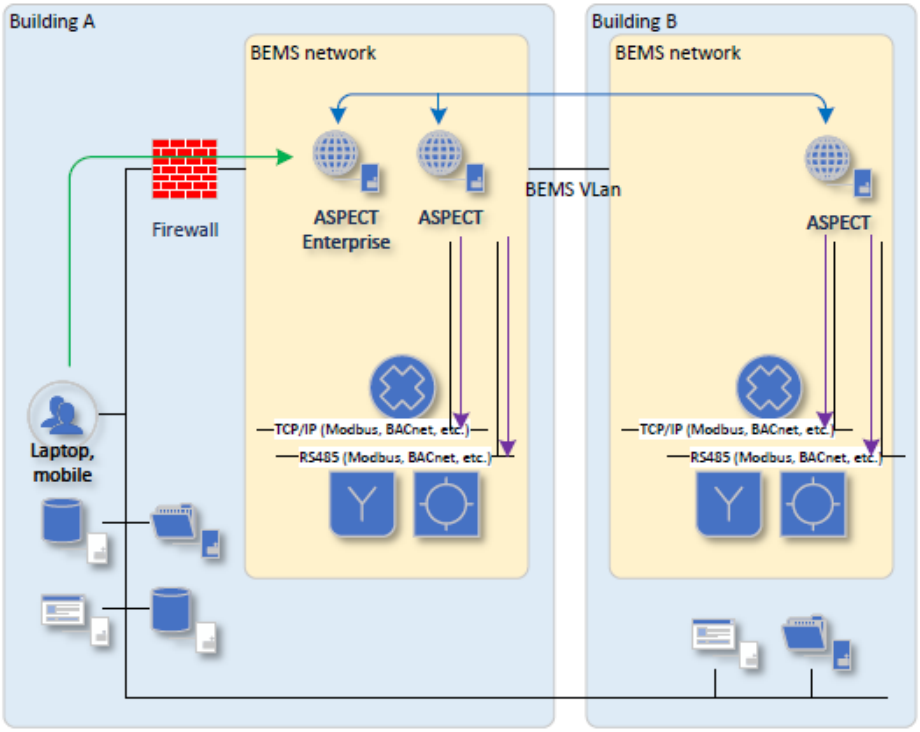
The ASPECT, BACnet or Unitron application can be accessed from outside the company network. The correct way to provide secure access is by using a VPN, which grants access to the ASPECT, BACnet or Unitron applications based on proper user authentication and authorization.

Both company employees and system integrator employees may use this communication channel.

The company may also use any other secure remote access system already in place, such as Zero Trust Network Access.

Note: An existing company VPN or a separated dedicated VPN device must be used to provide secure encrypted access to the BMS network.

SEGREGATION & MULTI-BUILDING CONNECTIVITY



Disclaimer: The concept diagram does not reflect the actual implementation details, which must be covered in HLD/LLD documents.

ABB ASPECT, BACnet and Unitron applications are not intended to be internet-facing.

Additionally, the application should be segregated from the company network, along with monitored devices.

Communication between ASPECT Enterprise and ASPECT servers must be facilitated between company buildings. In all cases, the BEMS VLAN should be extended to other buildings to maintain seamless connectivity.

Users of the ASPECT, BACnet or Unitron application can access it through a firewall with a properly defined firewall policy.

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:

- 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®, FLXeon 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.

Encryption 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.

Note: Because ASPECT, FLXeon, CBXi, Unitron and CB-Line Systems **must** be on private networks, it may be difficult to deploy Signed Certificates, in which case browsers may display warnings. Please contact an IT professional for more information on dealing with such warnings.

WARNING : If your system is dependent on an external weather service, and if that weather service is compromised or spoofed, any logic in your system that uses the temperature for heating, cooling or any other purpose may be harmed.

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.

ALWAYS FOLLOW DOCUMENTED BEST PRACTICES FOR SECURING YOUR DEVICES AND SYSTEMS

WARNING: Do not configure, use or allow access to the ports listed below unless there is a specific reason to do so.

System Administrators and ASPECT System integrators must co-ordinate to ensure that the minimum access to these ports is configured, even on private internal networks.

For example: if your ASPECT instance makes use of BACnet then the local network should allow connections between ASPECT and the specific device or ASPECT instance using UDP port 47808 (or 47809) only.

Protocol	TCP/UDP	Ports	Function
ASPECT HTTP[1]	TCP	7226, 7227	These ports were used by older versions of ASPECT and provide unencrypted HTTP access to an ASPECT Control Engine. If possible, ASPECT should be accessed using a secure port - either on port 8226 or by changing the URL redirection to https://(your IP)/aspect1 so that port 443 is used.
ASPECT HTTPS[1]		8226, 8227	Ports used for direct https access to ASPECT Instance 1 and 2.
WebUI HTTPS		14443	Alternative Access: SSL access to the ASPECT Target and web
HTTP	TCP	80	Unencrypted access: It is highly recommended that this port is kept closed.
HTTPS	TCP	443	Encrypted access to FBXi, CBXi and ASPECT configuration web UI.
MySQL[2]	TCP	30144,3306	PhpMyAdmin/Adminer (which provides a UI for the MySQL database server for several ASPECT targets) runs on port 30144. Port 3306 may also be required on the local network for connectivity to a remote MySQL server for replication.
BACnet	UDP	47808,47809	Building Automation and Control Networks (BACnet) Port 47808 is required for local engineering of the system and communications to the field controllers. Sometimes this port is disabled by the network switches, they should be enabled on the local network. BACnet communication is over UDP/IP. BACnet Port 47809 is required for remote engineering of the system.
BACnet Web-based Configuration Interface	TCP	5480	BACnet Web-based Configuration Interface (Stubbed out for future use, no process is currently listening on this port)
Deployment Server	TCP	9966	Access to this port is localhost only. This port should never be opened.
Modbus®	TCP	502	Required for connectivity to Modbus TCP/IP devices such as electrical and gas meters.
SSH	TCP	22	Required for advanced configuration and troubleshoot the ASPECT system. This port should remain closed and the SSH service disabled unless the system is under maintenance.
Syslog	TCP	514	For remote syslog messages used to for example to log system diagnostic messages from one ASPECT target to another.
NTP [3]	UDP	123	Used for time synchronization
Simple Mail Transfer Protocol (SMTP)	TCP	25	ASPECT can use this port to send unauthenticated emails such as alarm notifications.
Gmail Authenticated SMTP over SSL	TCP	465	ASPECT can use this port to send authenticated emails such as alarm notifications.
Gmail Email Message Submission (Start TTLS)	TCP	587	ASPECT can use this port to send authenticated emails such as alarm notifications.
ABB Cylon PUP	TCP/UDP	4222	Provides general network communications between ASPECT® Control Engine devices (PUP Protocol Implementation)
Supervisor - localhost only	TCP	4223	Local watchdog service – Never expose this port
ABB Cylon BACnet Discovery	TCP/UDP	4224	Provides general network communications between ASPECT® Control Engine devices (BACnet Discovery)
ABB Cylon Aspect & SoloPro	TCP/UDP	4225	Provides PUP over IP network communications and SoloPro to access devices connected to an ASPECT® Control Engine device remotely.
BACnet Device Port	TCP/UDP	4226	BACnet Device Port (Stubbed out for future use, no process is currently listening on this port)
BACnet BVLS/BACnet Virtual Link States	TCP/UDP	4227	BACnet BVLS/BACnet Virtual Link States (Stubbed out for future use, no process is currently listening on this port)

[1] It is no longer necessary to use ports 80 or 7226 on the ASPECT Control Engine box. ASPECT can be accessed through port 443.

[2] PHPMyAdmin/Adminner is a common attack target and must not be exposed to the Internet.

[3] Network Time Protocol (NTP). Do not rely on an NTP server that you do not directly control. If your network depends on an external NTP server for the time of day, and that server is compromised or spoofed, your system may be harmed. For example, locks may be turned off, the alarm system disabled, etc. If you use an NTP server, it must be an internal server that is physically controlled by your trusted organization.