# CYLON BUILDING ENERGY MANAGEMENT SYSTEM NETWORK SECURITY BEST PRACTICES

# ASPECT® SOLUTION

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

## 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. If possible, install the Cylon BEMS solution on a standalone network which is dedicated to BMS controls only. Do not mix with other IP devices such as CCTV or credit card terminals.
2. Remember, if something is exposed to the Internet and publicly available for access, it is accessible by every person and computer on the planet. Therefore: Be deliberate in your decision making about what truly needs to be exposed.
3. Be aware that every device on the Internet is constantly being probed and attacked. In the past, users may have had a successful history with Cylon solutions being open to the Internet, but due to today's widespread use of the Internet, all Internet-enabled technologies are experiencing new security challenges.
4. Expose the minimum information of a device necessary to accomplish a task. This is often referred to as "minimizing your surface area". Carefully evaluate whether something really needs public exposure or if other access methods are available (such as VPN). For example, a site may have multiple **MATRIX Series** Area Controllers and a single **ASPECT®-Enterprise** server. A suggested method of practice would be to only expose the **ASPECT®-Enterprise** server as a centralized point for external accessibility.
5. Use VPN (Virtual Private Network(s)) wherever possible. This allows authorized users within an organization to access a device without exposing it to the entire world. VPN access also provides an additional layer of user security credentials in order to gain access to a network.

## NETWORK SECURITY STRATEGY

The most secure approach is to expose nothing to the Internet, and to use VPN to access a corporate network. This is the preferred method of providing remote access and it delivers the most comfortable balance of convenience and security. 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.

## USE ENCRYPTED COMMUNICATIONS

Cyber criminals are crafty, but **ASPECT**® puts 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.

Physically protect the medium (usually a USB thumb drive) you use to back up and transport exported certificates.

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**® 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

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

Only expose what is **absolutely necessary**:

| Protocol | TCP/UDP | Ports | Function |
|---|---|---|---|
| ASPECT[1] | TCP | 7226 | This is the port where nearly all the action takes place and is typically the only port that should need to be exposed for user access without VPN. While a DoS (Denial of Service) attack is possible on this or any other random port one may designate, the rest of the common attack vectors are unavailable. Technicians can change default port `7226` without the assistance of a Network Administrator. |
| HTTP | TCP | 80 | Access to ASPECT web UI for configurations changes |
| MySQL[2] | TCP | 30144,3306 | **PhpMyAdmin** (which provides a UI for the **MySQL** database server for several **ASPECT®** targets) runs on port `30144`, so even if you forward the web UI on port `80` an attacker will not have access to the database administration subsystem. 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. |
| 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. |
| 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. |
| Cylon PUP Discovery | TCP/UDP | 4222 | Provides general network communications between **ASPECT®** Control Engine devices (PUP Discovery) |
| Cylon BACnet Discovery | TCP/UDP | 4224 | Provides general network communications between **ASPECT®** Control Engine devices (BACnet Discovery) |
| Cylon Aspect & SoloPro | UDP | 4225 | Provides PUP over IP network communications and SoloPro to access devices connected to an **ASPECT®** Control Engine device remotely. |

[1] If you want users to be able to access the deployed project without entering a port number, map the external port `80` to `7226` on the **ASPECT®** Control Engine box. This action will provide a good balance between ease of access and security for casual users.

[2] It is highly recommended that phpMyAdmin is not exposed to the Internet since it is a common attack target. If your application requires you to expose it, carefully review your **MySQL** installation and review all privileges.

[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.

**Weather Services**: Be warned. 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.