EcoStruxure Building Management

System

Hardening Guide

04-20037-02-en
December 2021

Life Is On | Schneider Electric

Internal

Copyright © 2021 Schneider Electric. All rights reserved.

The Schneider Electric brand and any registered trademarks of Schneider Electric Industries SAS referred to in this guide are the sole property of Schneider Electric SA and its subsidiaries. They may not be used for any purpose without the owner's permission, given in writing. This guide and its content are protected, within the meaning of the French intellectual property code (Code de la propriété intellectuelle français, referred to hereafter as "the Code"), under the laws of copyright covering texts, drawings and models, as well as by trademark law. You agree not to reproduce, other than for your own personal, non-commercial use as defined in the Code, all or part of this guide on any medium whatsoever without Schneider Electric's permission, given in writing. You also agree not to establish any hypertext links to this guide or its content. Schneider Electric does not grant any right or license for the personal and non-commercial use of the guide or its content, except for a non-exclusive license to consult it on an "as is" basis, at your own risk. All other rights are reserved.

Trademarks and registered trademarks are the property of their respective owners.

Contents

1 EcoStruxure Building Operation

1.1 Overview

Ensuring the EcoStruxure Building Management integration is installed securely is key to the overall security envelope of the building. This chapter discusses integration security configurations that need to be consider ensuring the overall security meets “best practice” standards.

> NOTE: Hyperlinks in this document may point to topics in the online documentation that are not available without appropriate authorization. Ensure that you are logged on. If the content is still not available, find the corresponding information in the EcoStruxure Building Operation Technical Reference Guide.

1.2 Important Concept

When discussing any network-based installation, understanding the purpose and security capabilities of each component is key in achieving integration security.

There are two general classes of network devices commonly used in BMS integrations:

- Network protective devices (Firewalls, VPNs, routers, switches, etc.)
- BMS products

While BMS products generally have many of the same network security features found in network protective devices; for many reasons those BMS features are not to be used as substitutes for the equivalent network protective devices.

It is important to note that BMS products have been designed to provide building management functionality, not network management and security.

Network protective devices are specifically designed to provide network management and security features. They are generally located on the perimeter of the BMS network and control the dataflow into and out of that network.

The following “Requirements” are a MUST for all BMS network implementations:

1.3 BMS Equipment and Network Requirements

Requirement #1 – BMS networks MUST BE isolated from the Internet.
EcoStruxure BMS servers are NOT to be connected directly to the Internet. BMS system access to the Internet must be buffered by at least one, properly configured, router.

Requirement #2 – BMS components MUST BE connected to isolated network segments dedicated to BMS use.
All BMS network segments must be isolated from all other networks using at least one router configured to ensure only appropriate external systems can interact with the BMS network components.

Requirement #3 – Remote access MUST USE a VPN for connectivity to the BMS network segments.
It is common for maintenance operations to be performed remotely. The security of that connection is critical in ensuring maintenance is performed securely. The use of a VPN connection between the remote device and the BMS network is the only approved way to establish that connection. There are various architectural considerations associated with VPN connections; the Customer’s IT department can assist in the designing and implementing a solution that meets company policies.

Requirement #4 – BMS security patches MUST BE applied in a timely manner.
Cyber Security is a fast-moving field where new vulnerabilities are constantly being detected. While the network protective devices and isolated network segments provide the primary protection functions; eliminating unnecessary risks by regularly updating all BMS product security patches is REQUIRED to ensure availability of the latest security features.

Requirement #5 – BMS backups MUST BE routinely completed, validated and secured.
A robust backup practice is the best insurance available for handling unexpected security issues. From Disaster Recovery to recovering a failed device, up-to-date backups speed recovery efforts. Beyond simply performing periodic backups, there should be a practice that validates each backup and ensures it is possible to restore it. All backups should be encrypted and securely stored.

Requirement #6 – User accounts MUST BE regularly maintained.

A common security risk is failure to adequately maintain user accounts. EcoStruxure BMS servers provides connectivity with Active Directory to assist with account management. When Active Directory is not in use, a manual process will be needed. It is very important to periodically review all user accounts and to disable or remove all users who no longer have a valid reason for accessing the BMS products.

1.4 Server Platform Best Practices

The following “Best Practices” pertain to server equipment and operating systems used to support EcoStruxure applications. These are practices that MUST be implemented for all BMS network implementations:

Best Practice #1 – Disable unused services.
Fundamental to the security of all servers is ensuring unnecessary Windows sub-systems are not running. Refer to EcoStruxure System Requirements for assistance in determine what Windows functions need to be running

Best Practice #2 – Disable unused network ports.
Windows should be configured to close all network ports not needed by the EcoStruxure Building Operation component(s). Ports that are unused but available for access expose the system to attacks on those ports. Proper system hygiene requires those ports to be closed to minimize the risk associated with the services attached to those ports.

Best Practice #3 – Uninstall unnecessary applications.
Every application brings its own security issues. For servers, it is important to remove all applications not directly related to the function of the server. Engineering tools should be evaluated and removed if possible, since they generally provide access to functionality an attacker my leverage to compromise BMS systems.

Best Practice #4 – Maintain Windows system patches.
The number one reason for system compromise is that operating system patches have not been applied in a timely manner. Updating control system servers can be complicated, especially when updating requires server hardware to be reset or “down” for a period of time. While network protective devices and network segmentation provide the primary protection, it is important that periodic system outage are planned and that patches are applied at this time.

Best Practice #5 – Ensure all BMS Windows servers are backed up, validated and secured.
A robust backup practice is the best insurance available for handling unexpected security issues. From Disaster Recovery to recovering a

failed device, up-to-date backups speed recovery efforts. Beyond simply performing periodic backups, there should be a practice that validates each backup and ensures it is possible to restore it. All backups should be encrypted and securely stored.

Best Practice #6 – Ensure user passwords meet minimum requirements. The Customer's credential and/or password requirements must be adequately incorporated into the Windows environment. For EcoStruxure BMS servers using Active Directory, it is important to ensure all required Windows configurations have been completed in a secure manner.

Best Practice #7 – Disable unused Windows user access accounts.
A common security issues is a failure to maintain user accounts. An EcoStruxure BMS server requires credentials at two levels – one on the operating system level and another for the EcoStruxure Building Operation applications. For servers using Active Directory, it is important that the Active Directory administrator be made aware of personnel status changes. For systems relying upon Windows and EcoStruxure Building Operation credentialing only, it is essential that a periodic practice for the review and maintenance of all user accounts be implemented.

The following "Best Practices" pertain to server equipment and operating systems used to support EcoStruxure Building Operation applications. These are practices that SHOULD be considered for all BMS network implementations.

1.5 Server Platform Additional Considerations

Best Practice #1 – Investigate the use of antivirus and allowlisting solutions.
A common security practice is installing antivirus and other common host protection software onto each server. Customer policy will generally determine any requirements.

It is becoming more common for Customer policy to require allowlisting services. These services ensure that only approved applications can run. The Customer's IT department will be of assistance in the implementation of such services.

1.6 Security Capability

The cybersecurity features of the EcoStruxure Building Operation software are constantly being enhanced. The following cybersecurity features indicate the version of the EcoStruxure Building Operation software each feature was introduced in, where applicable.

Identification and Authentication

Internal

Admin logon password management (v1.3)
For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=4278

Imported User Accounts are disabled by default (v1.7)
For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=5833

Certificate functionality
The EcoStruxure Building Operation software supports certificates. Certificates are electronic credentials used to certify the identities of computers, and other entities on a network.

- Self-signed certificates
- Default certificates (v1.4)
- Certificate Authority certificates (v1.6)

For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=10326

Password policies can be enforced (v1.6)
You can increase the password security by configuring a password policy that defines how passwords must be created by the users. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=10336

SSH connection control (v1.6)
You can set a lockout time on the SSH Console to prevent brute-force attacks. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=5907

Disabled after failed logon attempts
For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=5332

SSH device fingerprint authentication (v1.9)
For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=11391

Password policies and default settings
You can increase the password security by configuring a password policy that defines how passwords must be created by the users. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=10336

Force Admin password change (v1.7)
Servers force a password change at first time administrator logon.

Password blocklist (v1.7):
You can block use of certain easy-to-guess passwords. ~~A~~ default list is loaded from the factory.

Active Directory/Windows Logon support (v1.5)
For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=7605

Federated Authentication support (v4.0)
Authentication using SAML 2.0 is supported. SAML 2.0 authentication also enables multi-factor authentication when used with an Identity Provider that has that function enabled. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=14395

Enterprise Server Run-As-Service selectable user account (v1.5)
For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=5919

Authorization

Custom logon banner
For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=10125

Role-based access control (permissions)
For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=12215

Object and point level security
For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=7041

Confidentiality

Encrypted transmission of data.
For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=9485

SMTPS secure email notification support (v1.8)
For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=6920

Clickjacking protection options (v1.9)
For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=11679

Password data is obscured from view
Password input fields do not show passwords in clear text.

Passwords are stored and transmitted securely
Passwords are never sent or stored in clear text. Active Directory authentication is limited to HTTPS.

Secure connection between Device Administrator and AS-P/B (3.0)
For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=12672

Integrity

Auto logoff (v1.5)
User inactivity for configurable time is supported. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=8870

Audit log with system-wide synchronized timestamps
For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=4382

The system does not have any ordinary means to alter audit trail information.

The optional External Log Storage function requires that security measures are in place for the external database. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=12798

Secure boot
SpaceLogic server Secure Boot is available, to ensure the authenticity of Schneider Electric firmware. (v4.0)

SpaceLogic server Boot Loader U-Boot disabled (v1.5)

SpaceLogic server Boot restricted to a single boot location (v1.5)

Basic protection against program and data at rest modification.
Optional support for single or dual authentication at change. (v3.0) For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=13060

Basic protection for input validation
All input in clients is validated according to the built-in rules. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=6436

Document Policy
You can increase ~~the~~ security in your system by configuring the document policy. The document policy controls which file types a user can open, save, and import. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=10952&locale=en-US&productversion=nextrelease&prerelease=true&a=1

Restricted data flow

Basic capabilities for network segmentation

For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=9266

Basic options for enabling/disabling ports
Disable HTTP (HTTPS only) configuration option (v1.5). For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=9485

Disable SpaceLogic AS-P and AS-B server USB ports configuration option (v2.0). For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=12108

Disable SpaceLogic server SSH port 22 configuration option (v2.0). For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=10636

Disable SpaceLogic server Ethernet 2 Port. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=10918

EcoStruxure Web Services server interface is disabled by default on EcoStruxure BMS servers (v2.0). For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=9076

Firewall

You can configure the devices that are allowed to communicate with the SpaceLogic AS-P and AS-B server to prevent connection attempts from unauthorized devices. The IP addresses of the devices that are allowed to communicate are added to the allow list. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=10333

Connect Agent

To prevent data transfer over the cloud server, you can disable the transfer of system information and crash information of the Enterprise Central and the Enterprise Server and its SpaceLogic server. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=10310

Timely response to events

Audit log access
SIEM Support: Remote system logging option (v1.6). For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=10342

Web server access logging configuration option (v1.6). For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=10344

Resource availability

System backup, recovery and reconstitution
For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=7762

Access to network and security configuration settings
For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=11953 and https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=7041

1.7 Security Deployment

For more information, see https://www.se.com/us/en/download/document/AN_EBOCyberSecurity_EN/

For more information about requirements for software hosted on Microsoft Windows: https://download.schneider-electric.com/files?p_enDocType=White+Paper&p_File_Name=RecommendedCybersecurityBestPractices_7EN52-0390-03.pdf&p_Doc_Ref=7EN52-0390

An additional resource is the Center for Internet Security (CIS) Windows hardening guides. For more information, see https://www.cisecurity.org/benchmark/microsoft_windows_desktop/

For installations requiring that web browsers or password management do not automatically fill in credentials, ensure that the browser supports the Wordwide Web Consortium guideline for HTML directives for preventing this function. Many modern browsers do not yet comply with this guideline. In case such browsers are used, customers must ensure that the browser function is turned off and that password management software is blocked. For more information, see https://developer.mozilla.org/en-US/docs/Web/Security/Securing_your_site/Turning_off_form_autocompletion

For installations where email is used as a distribution mechanism for alarms and reports, ensure the email server is using adequate authentication and encryption.

1.8 Security Hardening Guidelines

Identification and Authentication

Admin logon password management

- Ensure default admin account use is absolutely minimized. ~~A~~ll users should have a unique user account. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=4278

Certificate functionality

- Ensure trusted self-signed or Certification Authority certificates are used.
- Ensure there is a process in place for maintenance and renewal of certificates.

For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=10326

Password policies can be enforced

- Ensure password policies are configured according to customer needs. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=10336 .
  The following settings are recommended:
  - The minimum number of hours between password changes is 0.
  - A password expires after 90 days.
  - The password history is set to 6.
  - At least 3 characters are different in the new password.
  - A password contains at least 8 characters.
  - A password contains at least 1 lowercase character.
  - Uppercase characters are not required in a password.
  - A password contains at least 1 numeric character.

  - The numeric character can be the first or last character, such as “123password”.
  - A password contains at least 1 special character: !”#$%&’()*+,-./:;⇔?@[\]^_`{|}~´.
  - The special character can be the first or last character, such as “password!”.

- *Disabled after failed logon attempts*
  Ensure the setting for temporarily disabling users after failed logon attempts is configured as required by the customer. This limits the risk for Denial of Service situations and brute-force attacks. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=5332

- *Password blocklist*
  You can block the use of certain easy-to-guess passwords. A default list is loaded from the factory. For adding more passwords to the blocklist, contact Schneider Electric.

- *Enterprise Server Run-As-Service selectable user account*
  Ensure the EcoStruxure Building Operation service runs under a custom account with permissions designed to be as limited as possible. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=5919

- *Use of strong authentication hash algorithms*
  Ensure MD5 hashing is disabled. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=9485

Authorization

- *Custom logon banner*
  Ensure the security banner is enabled and convey any custom terms applicable for the users to access the system. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=10125

- *Role-based access control (permissions)*
  Ensure the access control scheme is carefully planned and implemented. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=12215

- Ensure processes are in place to regularly inspect the account management configuration. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=12215

Object and point level security

- Ensure the object, point and command level permissions are implemented to provide the least possible rights for the respective roles. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=7041
- Ensure processes are in place to regularly inspect the account management configuration. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=12215

Confidentiality

Encrypted transmission of data.

- Ensure HTTP is disabled, and that TLS 1.3 is used. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=9485

SMTPS secure email notification support

- Ensure email transmission uses secure options. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=6920

Clickjacking protection options

- Ensure that the embedding of 3rd party web sites is disabled and that the hosting of EcoStruxure Building Operation web pages within other pages is disabled. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=11679
- Ensure unsafe Javascript constructions are disabled. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=13001

Protection of data storage

- Ensure the EcoStruxure Building Operation installation ~~folders~~ and data storage folders on the host~~ing~~ Microsoft Windows operating system are protected from Windows user accounts that interactively log on to Windows. For more information, see operating system documentation.

External Log Storage

- Ensure the TimescaleDB/PostgreSQL installation ~~folders~~ and data storage folders are adequately protected and that the deployment is hardened appropriately. For more information, see https://www.enterprisedb.com/blog/how-to-secure-postgresql-security-hardening-best-practices-checklist-tips-encryption-authentication-vulnerabilities

- Ensure separate accounts are used for 3rd party access of the External Log Storage, In particular, you want to separate the account that EcoStruxure Building Operation is using to access the database.
- Ensure encrypted communication is used between EcoStruxure Building Operation servers and TimescaleDB/PostgreSQL. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=13446

Integrity

Auto logoff

- Ensure inactivity logoff is activated with a sufficiently low timeout. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=8870

Audit log with system-wide synchronized timestamps

- Ensure all servers have accurate configuration of NTP time synchronization. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=4382 and https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=6370

Clickjacking protection options

- Ensure that the embedding of 3rd party web sites is disabled and that the hosting of EcoStruxure Building Operation web pages within other pages is disabled. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=11679
- Ensure unsafe Javascript constructions are disabled. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=13001

Protection of data storage

- Ensure the EcoStruxure Building Operation installation folders and data storage folders on the host Microsoft Windows operating system are protected from Windows user accounts that interactively log on to Windows. For more information, see operating system documentation.

Secure boot

- Ensure that you use Secure Boot versions of server hardware and edge servers.

Basic protection against program and data at rest modification.

- Ensure Compliance Pack is activated, change control is enabled and the appropriate settings are deployed in accordance with customer requirements. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=13060

Document Policy

- Ensure that only appropriate document types are enabled. Disable document types that are not needed. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=10952&locale=en-US&productversion=nextrelease&prerelease=true&a=1

Restricted data flow

Basic capabilities for network segmentation

- Ensure network design is planned and implemented according to current guidelines and best practices. For more information, see https://www.se.com/us/en/download/document/AN_EBOCyberSecurity_EN/

Basic options for enabling/disabling ports

- Ensure HTTP is disabled. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=9485
- Ensure USB ports are disabled. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=12108
- Ensure the SSH access is configured according to minimum needs. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=10636
- For SpaceLogic servers with no need for secondary Ethernet access, ensure Ethernet 2 Port is disabled. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=10918
- Ensure the EcoStruxure Web Services server interface is disabled. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=9076

Firewall

- Ensure the firewall in SpaceLogic servers and Enterprise servers is configured appropriately. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=10333 and Microsoft Windows documentation.

Timely response to events

Audit log access

- Ensure a SIEM system is in place and that remote logging is enabled. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=10342&locale=en-US&productversion=nextrelease&prerelease=true&a=1
- Ensure web server access logging is enabled and that there is an inspection process in place. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=10344

Resource availability

System backup, recovery and reconstitution

- Ensure backup functionality is properly configured and tested. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=7762
- Ensure processes are in place for continuous testing of recovery processes.

Access to network and security configuration settings

- Ensure that networking guidelines are followed. For more information, see https://www.se.com/us/en/download/document/AN_EBOCyberSecurity_EN/, https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=11953 and https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=7041

1.9 How To Securely Dispose Product

- Ensure you use the Uninstall program to remove EcoStruxure Building Operation binaries and configuration files. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=7094
- Ensure you inspect installation folders and database folders for left-over data files and manually delete them.
- Ensure you use a well-known data erasure product to remove information that may still reside on disks even after software uninstallation.

1.10 How To Securely Operate The Product

- Ensure you follow the operational instructions as documented in the “EcoStruxure Building Operation – WorkStation Operating Guide” or the “EcoStruxure Building Operation – WebStation Operating Guide”.

1.11 How To Manage Security Accounts

Role-based access control (permissions)

- Ensure the access control scheme is carefully planned and implemented. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=12215

- Ensure processes are in place to regularly inspect the account management configuration. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=12215

Object and point level security

- Ensure the object, point and command level permissions are implemented to provide the least possible rights for the respective roles. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=7041
- Ensure that processes are in place to regularly inspect the account management configuration. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=12215

1.12 In Summary

Maintaining the security of BMS integrations relies upon the proper use of various cybersecurity tools. From routers to VPNs to proper server hygiene, security is achieved through constant diligence to basics. This document provides common security hardening information. The reader is directed to contact cybersecurity professionals for more in-depth analysis and recommendations.

2 SpaceLogic BACnet/IP Controllers

2.1 Overview

Ensuring the EcoStruxure Building Management integration is installed securely is key to the overall security envelope of the building. This document discusses integration security configurations that need to be considered to ensure that overall security meets “best practice” standards.

2.2 Important Concept

When discussing any network-based installation, understanding the purpose and security capabilities of each component is essential to achieving integration security.

There are two general classes of network devices commonly used in BMS integrations:

- Network protective devices including the following:
  - Firewalls
  - VPNs
  - Routers
  - Switches

- BMS Products

Network protective devices are specifically designed to provide network management and security features. They are generally located on the perimeter of the BMS network and control the incoming and outgoing network dataflow.

While many BMS products are hosted on industry standard platforms (like Windows or Linux), the BACnet/IP controllers (MP-C, MP-V, RP-C and RP-V) are “pure BACnet” products. They use BACnet IP to talk to the AS controllers. A secure implementation of the BACnet IP protocol is currently available in EcoStruxure Building Operation. It is not currently available at the controller level, however. This means that required network protection must come from the proper use of network protective devices.

For the EcoStruxure Building Management line of products, the BACnet/IP controllers have been designed to connect to IP networks using the AS-P server. This device has been designed to provides the required isolation for IP based controllers on the BMS network segment.

The IP field network defined by the AS-P to the BACnet/IP controllers is normally implemented in a fully isolated mode. This limits each controller's attack surface to the IP Field Network to which it is connected. In such an architecture, additional network protective devices are not needed on the isolated subnet. If non-EBO IP controllers are introduced, additional network protective devices are used to limit the risk posed by these devices.

The following "Requirements" are a MUST for all IP Field Network implementations:

2.3 BMS Equipment and Network Requirements

Requirement #1 – The BACnet/IP controllers MUST BE isolated from the Internet.
The BACnet/IP controllers MUST NOT to be connected directly or indirectly to the Internet. Because these controllers are BACnet IP and have no inherent network protection, connecting them to the Internet brings unprecedented risks.

Requirement #2 – The BACnet/IP controllers MUST BE connected to isolated network segments dedicated to BMS use.
It is "best practice" for BACnet/IP controllers to be connected to the isolated second port of an AS-P server. In use cases where this is not possible, it is critical that network protective devices be installed and configured to ensure the confidentiality, integrity and availability of all communications to and from these devices.

Requirement #3 – Remote Access to BACnet/IP controllers is discouraged. If it is unavoidable,the connection MUST USE a VPN.
Remote connectivity to BACnet/IP controllers, if done at all, must be done securely. At a minimum, a VPN must be used, and an additional firewall and/or router may be needed to provide assurance that only authorized IP ports have access to the controller. Connecting other networks directly to an IP Field Network is strongly discouraged.

Requirement #4 – BACnet/IP controller security patches MUST BE applied in a timely manner.
Cyber Security is a fast-moving field where new vulnerabilities are constantly being detected. While network protective devices and isolated network segments provide the primary protection functions, eliminating unnecessary risks by regularly updating all BACnet/IP controller security patches is REQUIRED to ensure availability of the latest security features.

Requirement #5 – BACnet/IP controller backups MUST BE being routinely completed, validated and secured.
A robust backup practice is the best insurance available for handling unexpected security issues. From disaster recovery to recovering a failed device, up-to-date backups speed recovery efforts. Beyond simply performing periodic backups however, there needs to be a practice that validates each backup and ensures it is possible to restore it. All backups should be encrypted and securely stored.

2.4 BACnet/IP Controller Best Practices

The following "Best Practices" pertain to SpaceLogic controllers used to support EcoStruxure applications. These are practices that MUST be implemented for all BMS network implementations:

Best Practice #1 – Disable unused network ports.
When dual ports are available on a controller, when one port is not is use, ensure the configuration is configured to disables the unused port.

Best Practice #2 – Maintain controller firmware
Like servers, controllers have a large software base, needed to provide the controller's functionality. This software is often referred to as firmware. It is important to ensure all controller firmware is up-to-date.

Best Practice #3 – Ensure all controller are regularly backed up
A robust backup practice is the best insurance available for handling unexpected security issues. From Disaster Recovery to recovering a failed device, up-to-date backups speed recovery efforts. Beyond simply performing periodic backups, however, you should make a practice of validating each backup and ensuring it is possible to restore it. All backups should be encrypted and securely stored.

Best Practice #4 – Ensure user passwords meet minimum requirements.

Prior to the EcoStruxure Building Operation version 2022, the controllers had no users or passwords. With the advent of web services, connection to the controllers using web services is possible. It is essential that you place adequate security around those credentials.

Best Practice #5 – Ensure web services are disabled if not in use.
The RP controllers are shipped from the factory with web services disabled. They must be properly enabled and configured before use. It is important to ensure that RP controllers not using web services have

Internal

WebServices disabled. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=14417.

2.5 BACnet/IP Controller Additional Considerations

Best Practice #1 – Mitigate the risk of unencrypted BACnet/IP communications. At the current time, communication between the Automation Server and SpaceLogic controllers uses unencrypted IP technologies. Additional compensating controls may be required for highly sensitive installations. Be sure to evaluate the need for metal conduits for all IP cables and locked enclosures for the controllers.

2.6 Security Capability

The Cyber Security features of the EcoStruxure Building Operation software are constantly being enhanced. The following list of cybersecurity features for BACnet/IP and SpaceLogic controllers.

For the BACnet/IP controllers, units are shipped from the factory in a “low security” mode that supports the configuration and commissioning of the devices. Once the device is “hosted” by the Automation Server, it automatically switches to a more secure, or secure-by-default state. See the individual items below to determine which features follow this security strategy.

Identification and Authentication

Certificate functionality

The SpaceLogic web services functionality requires the installation of HTTPS certificates. For more information, see https://docs.microsoft.com/en-us/azure/rtos/netx-duo/netx-duo-web-http/chapter1.

Additional Controller Security Features for BACnet/IP

The following configuration features are available on SpaceLogic controllers to provide additional Cyber Security for BACnet/IP connections.

- Allowlisting -- An IP-based allowlist that restricts communications to only the IP addresses is available. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=11996

- B-OWS Restrictions -- This restriction comes into force automatically when the MP or RP controller is hosted. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=12529

- Disable Bluetooth Access via SpaceLogic Sensor -- Wireless Bluetooth access to the MP/RP controller from the Commission Mobile Application may be achieved via the SpaceLogic Sensor (LSS). For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=12553.

- Disable or Control Bluetooth Access via Onboard Feature (RP only) -- Wireless Bluetooth access to the RP controller from the Commission Mobile Application may also be achieved via the onboard Bluetooth feature.   For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=12704.

- BLE PIN code -- There is a user configurable PIN code included in the secure pairing process. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=12705.

- BLE Secure on Hosting – when the controller is hosted by an EBO server, the Commission Mobile Application is disabled and the Engage Occupant App BLE filter may be enabled. For more information, see: https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=13326.

- Ethernet Port 2 Disable – When not needed, disabling the Port 2 Ethernet connection is recommended. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=11992

- Serial Bus Disable (Port reference) – Serial bus ports on the MP & RP controllers may be disabled by removing the port reference on any consuming resource.

Authorization

The web services feature is the only controller feature that allows a level of authorization. For more information, see https://exchange.se.com/ and search for the document “SpaceLogic Web Service API".

Confidentiality

Since BACnet/IP has no confidentiality, if field networks require it, additional compensating controls are needed.

Web services provide a secure, always on, HTTPS connection. For more information, see https://exchange.se.com/ and search for the document "SpaceLogic Web Service API".

Integrity

BACnet/IP provides a level of integrity checking at the protocol level, while IP provides a level of integrity checking at the network level. For web services, the HTTPS provides a level of integrity checking.

Restricted data flow

Basic capabilities for network segmentation
For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=9266

Resource availability

System backup, recovery and reconstitution
For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=7762

2.7 Security Deployment

For more information, see https://www.se.com/us/en/download/document/AN_EBOCyberSecurity_EN/

2.8 Security Hardening Guidelines

Identification and Authentication

Web Services Identification and Authentication functionality
Before web services can be enabled, you need to install a server certificate and key securely using SpaceLogic Certificate Configuration Tool. For more information, see https://exchange.se.com/ and search for the document "SpaceLogic Web Service API".

The RPC web service must be enabled and can be disabled on demand. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=14417.

The RPC web service also supports client certificate authentication as an option. To increase security, client certificate validation may be enabled. For more information, see https://exchange.se.com/ and search for the document "SpaceLogic Web Service API".

Certificate functionality

- Ensure to use of trusted self-signed or Certification Authority certificates.
- Ensure a process is in place for maintenance and renewal of certificates.

For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=10326

Web Services Password Policies

Web services have their own password policy and enforcement system which is separate from other EcoStruxure BMS functionality. For more information, see https://exchange.se.com/ and search for the document "SpaceLogic Web Service API".

Authorization

Only the web service provides an authorization capability. For more information, see https://exchange.se.com/ and search for the document "SpaceLogic Web Service API".

Confidentiality

Standard BACnet/IP does not provide any level of confidentiality. For systems requiring additional "on the wire" security, using sealed metal conduits may be an option.

Web services provides confidentiality at the HTTPS protocol level. For more information, see https://exchange.se.com/ and search for the document "SpaceLogic Web Service API".

Encrypted transmission of data

Standard BACnet/IP does not provide encrypted data transmission. For systems requiring additional “on the wire” security, using sealed metal conduits may provide similar protection.

Web services provides data encryption at the HTTPS protocol level. For more information, see https://exchange.se.com/ and search for the document “SpaceLogic Web Service API".

Integrity

Standard BACnet/IP provides a level of data integrity checking at the protocol level. The IP protocol provides and additional level of integrity protection.

WebServices provides integrity checking at the HTTPS protocol level. For more information, https://docs.microsoft.com/en-us/azure/rtos/netx-duo/netx-duo-web-http/chapter1.

Restricted data flow

Basic capabilities for network segmentation

> Ensure the IP field network design is planned and implemented according to current guidelines and best practices. For more information, see https://www.se.com/us/en/download/document/AN_EBOCyberSecurity_EN/

Basic options for enabling/disabling ports

- Ensure USB ports are disabled. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=12108.
- For BACnet/IP controllers with no needed use of the secondary Ethernet port, ensure Ethernet 2 Port is disabled. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=10918.
- Ensure the EcoStruxure web services server interface is disabled. For more information, see https://ecostruxure-building-help.se.com/bms/topics/show.castle?id=14417.

Timely response to events

Audit log access

- Ensure a SIEM system is in place and that remote logging is enabled. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=11873

Resource availability

System backup, recovery and reconstitution

- Ensure backup functionality is properly configured and tested. For more information, see https://ecostruxure-building-help.se.com/bms/Topics/show.castle?id=7762
- Ensure processes are in place for continuous testing of recovery processes.

Access to network and security configuration settings

- Ensure that networking guidelines are followed For more information, see https://www.se.com/us/en/download/document/AN_EBOCyberSecurity_EN/.

2.9 How To Securely Dispose Product

Each of the BACnet/IP controllers may have a different secure disposal requirements. The following provides guidance for each controller.

- The MP controllers use Flash technologies for non-volatile storage. There is currently no effective way to securely erase Flash devices. The MP controllers do not store sensitive information, but if secure disposal is a requirement, the only way to do so is to physically destroy the MP controller.
- The RP controllers use Flash technologies for non-volatile storage. There is currently no effective way to securely erase Flash devices. The RP controllers do not store sensitive information, but if secure disposal is a requirement, the only way to do so is to physically destroy the RP controller.
- The CRS modules use Flash technologies for non-volatile storage. There is currently no effective way to securely erase Flash devices. The CRS modules do not store sensitive information, but if secure disposal is a requirement, the only way to do so is to physically destroy the CRM module.

2.10 How To Securely Operate Product

Since the controllers are BACnet/IP devices, the concept of "Secure Operation" is limited. For more information on each controller type:

The MP controllers have no security features. If additional security is required, external compensating controls will need to be planned into the system architecture.

The RP controllers have no security features. If additional security is required, external compensating controls will need to be planned into the system architecture. The exception to this statement is the fact that RP web services are designed to be secure by default. For more information on web services, see https://exchange.se.com/ and search for the document "SpaceLogic Web Service API".

The CRS modules rely upon their hosting device for all available security. As such, secure operation of a CRS module relies upon the security associated with controller it is connected to and the security of the larger integration.

2.11 How To Manage Security Accounts

In the BACnet/IP controller family, only the web services feature provides a manageable account functionality. Specific information on each controller type follows.

The MP controllers have no user account system and thus there are no security accounts to manage.

The RP controllers, at the BACnet/IP level, have no user account system and thus there are no security accounts to manage. The exception to this statement is the fact that RP web services are designed to be secure by default and have additional account settings. For more information on web services, see https://exchange.se.com/ and search for the document "SpaceLogic Web Service API".

The CRS module has no user account system and thus there are no security accounts to manage.

2.12 In Summary

Maintaining the security of BMS integrations relies upon the proper use of various Cyber Security tools. From routers to VPNs to software server hygiene, security is achieved through constant diligence to the basics. This document provides common security hardening information. The reader is directed to contact Cyber Security professionals for more in-depth analysis and recommendations.