

Information Technology System Planning Guide

EcoStruxure Building Management

Commitment to IT-friendly and secure solutions

Schneider Electric views the deployment, monitoring, and security of the devices and software that comprise a Building Management System as essential to the goal of achieving optimal efficiency for a building. As a result, Schneider Electric is committed to providing an IT-friendly and secure solution.

Scope

This guide is designed for IT professionals who need to review the system design and provide support for the system installation.

EcoStruxure Building Operation Cybersecurity Features

The cybersecurity features of the EcoStruxure Building Operation software are constantly being enhanced. The following list of cybersecurity features indicates the version of the EcoStruxure Building Operation software each feature was introduced in.

Identification and Authentication

Admin logon password management (v1.3) - For more information, see the *Administration Accounts in EcoStruxure BMS Server Local Domain* topic on WebHelp.

Imported User Accounts are disabled by default (v1.7) - For more information, see the *Import and Export of User Management Solutions* topic on WebHelp.

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 the *Certificates* topic on WebHelp.

Password policies and default settings (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 the *Password Policy* topic on WebHelp.



SSH connection control (v1.6) - You can set a lockout time on the SSH Console to prevent brute-force attacks. For more information, see the *Setting the SSH Console Lockout Time* topic on WebHelp.

Disabled after failed logon attempts - For more information, see the *Editing the Maximum Logon Attempts* topic on WebHelp.

SSH device fingerprint authentication (v1.9) - For more information, see the *SSH Public Key Validation for Automation Server* topic on WebHelp.

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 the *Windows Active Directory User Groups* topic on WebHelp.

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 the *Federated Authentication Workflow* topic on WebHelp.

Enterprise Server Run-As-Service selectable user account (v1.5) - For more information, see the *Installing the Enterprise Server* topic on WebHelp.

Secure flag for cookies in WebStation is enabled when using HTTPS (v2.0)

Information Technology System Planning Guide

EcoStruxure Building Management

Multi-factor authentication for EcoStruxure Building Operation user account groups (v7.0) - For more information, see the *Multi-factor Authentication* topic on WebHelp.

Authorization

Custom logon banners can be enabled to communicate usage policies to operators

- Non-SSH connections (v1.5)
- SSH connections (v1.6)

For more information, see the *Security Banner* topic on WebHelp.

Role-based access control (permissions) - For more information, see the *Software Permissions Management* topic on WebHelp.

Object and point level security - For more information, see the *Software Permissions* topic on WebHelp.

Confidentiality

Encrypted transmission of data

- HTTPS is the default server to server communication protocol (v6.0.1)
- HTTPS using TLS 1.3 enabled by default (v4.0.1)
WorkStation has no support for TLS 1.3 and can only use TLS 1.2 or earlier
- HTTPS using TLS 1.0 and TLS 1.1 disabled by default (v4.0.1)
- SFTP using SSH 2.0 (v3.0.4)
- EWS Encrypted Logon (v1.5)
- Disable use of MD5 configuration option (v1.6)
- SNMPv3 support, SNMPv1 and v2 removed (v1.5)
- Automation server: SSHv2, SSHv1 removed (v1.5)
- Redirect web clients to HTTPS configuration option (v1.6)

For more information, see the *Encrypted Communication* topic on WebHelp.

SMTPTS secure email notification support (v1.8) - For more information, see the *Selecting and Specifying an Email Server for Email Notifications* topic on WebHelp.

Clickjacking protection options (v1.9) - For more information, see the *Security Configuration in WebStation* topic on WebHelp.

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. Using WebStation, Active Directory authentication is limited to HTTPS.

Secure connection between Device Administrator and AS-P or AS-B server (v3.0) - For more information, see the *Device Administrator Certificate Workflow* topic on WebHelp.

BACnet Secure Connect, BACnet/SC (v4.0.3) - For more information, see the *BACnet/SC Overview* topic on WebHelp.

BACnet/SC support for MP and RP controllers and IP-IO modules (v6.0.1) - For more information, see the *BACnet/SC SpaceLogic Controllers Certificate Management Workflow Using the Certificate Configuration Tool* topic on WebHelp.

BACnet/SC support for FDP server (v7.1.1) - For more information, see the *BACnet/SC Overview* topic on WebHelp.

Enrollment over Secure Transport (EST) certificate management protocol support (v6.0.1) - Support only applies to third party Public Key Infrastructure (PKI) that is configured using:

- EST protocol
- Registration Authority (RA) mode
- Basic HTTP authentication

Device Administrator support of CA certificate management for FDP server (v7.1.1) - For more information, see the *CA Certificate Management* topic on WebHelp.

Integrity

Auto logoff (v1.5) - User inactivity for configurable time is supported. For more information, see the *Automatic Logoff* topic on WebHelp.

Audit log with system-wide synchronized timestamps

- Audit logs provide non-repudiation

Information Technology System Planning Guide

EcoStruxure Building Management

- 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 the *External Log Storage Overview* topic on WebHelp.

For more information, see the *Audit Trailing of User Activity* topic on WebHelp.

AS-P server Secure Boot is available to ensure the authenticity of Schneider Electric firmware. (v4.0)

SHA2-256 Hash algorithm support (v1.9)

WebStation: HTML5 Graphics and Trend viewing support, removal of Java (v1.7)

Basic protection against program and data at rest modification

- Optional support for single or dual authentication at change (v3.0) - For more information, see the *Change Control* topic on WebHelp.

Basic protection for input validation - All input in clients is validated according to the built-in rules. For more information, see the *EcoStruxure Building Operation Objects* topic on WebHelp.

Document policy (v1.8) - You can increase 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 the *Document Policy* topic on WebHelp.

Validating integrity of EcoStruxure BMS server backups (v6.0.1) - All backups include a checksum that is used to validate the integrity of the backup and detect any tampering when the backup is restored on the same server that created the backup. For more information, see the *Validation of Field Server Backups* topic on WebHelp.

Restricted data flow

Basic capabilities for network segmentation - Guidance on Implementing a Cybersecure BMS Architecture with EcoStruxure Building Operation on the Schneider Electric website.

Basic options for enabling/disabling ports

- Disable HTTP (HTTPS only) configuration option (v1.5) - For more information, see the *Encrypted Communication* topic on WebHelp.
- Disable AS-P and AS-B server USB ports configuration option (v2.0) - For more information, see the *Disabling the USB Port on an Automation Server* topic on WebHelp.
- Disable automation server SSH port 22 configuration option (v2.0) - For more information, see the *Disabling Port 22 on an Automation Server* topic on WebHelp.
- Disable AS-P server Ethernet 2 port (v1.8) - For more information, see the *Disabling the Ethernet 2 Port* topic on WebHelp.
- EcoStruxure Web Services server interface is disabled by default on EcoStruxure BMS servers (v2.0) - For more information, see the *EcoStruxure Web Service Server* topic on WebHelp.

Firewall (v1.6) - You can configure the devices that are allowed to communicate with the AS-P and AS-B server to help 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 the *Firewall* topic on WebHelp.

Connect Agent (v1.6) - To help prevent data transfer over the cloud server, you can disable the transfer of system information and crash information of Enterprise Central and Enterprise Server and its automation server. For more information, see the *Connect Agent Overview* topic on WebHelp.

Timely response to events

Audit log access

- SIEM support: Remote system logging option (v1.6) - For more information, see the *Field Server Remote System Logging* topic on WebHelp.
- Web server access logging configuration option (v1.6) - For more information, see the *Web Server Access Logging* topic on WebHelp.

Resource availability

System backup, recovery, and reconstitution - For more information, see the *Backup and Restore Overview* topic on WebHelp.

Information Technology System Planning Guide

EcoStruxure Building Management

Access to network and security configuration settings - For more information, see the *Software Permissions* topic on WebHelp.

IT Overview

Best practice LAN architecture

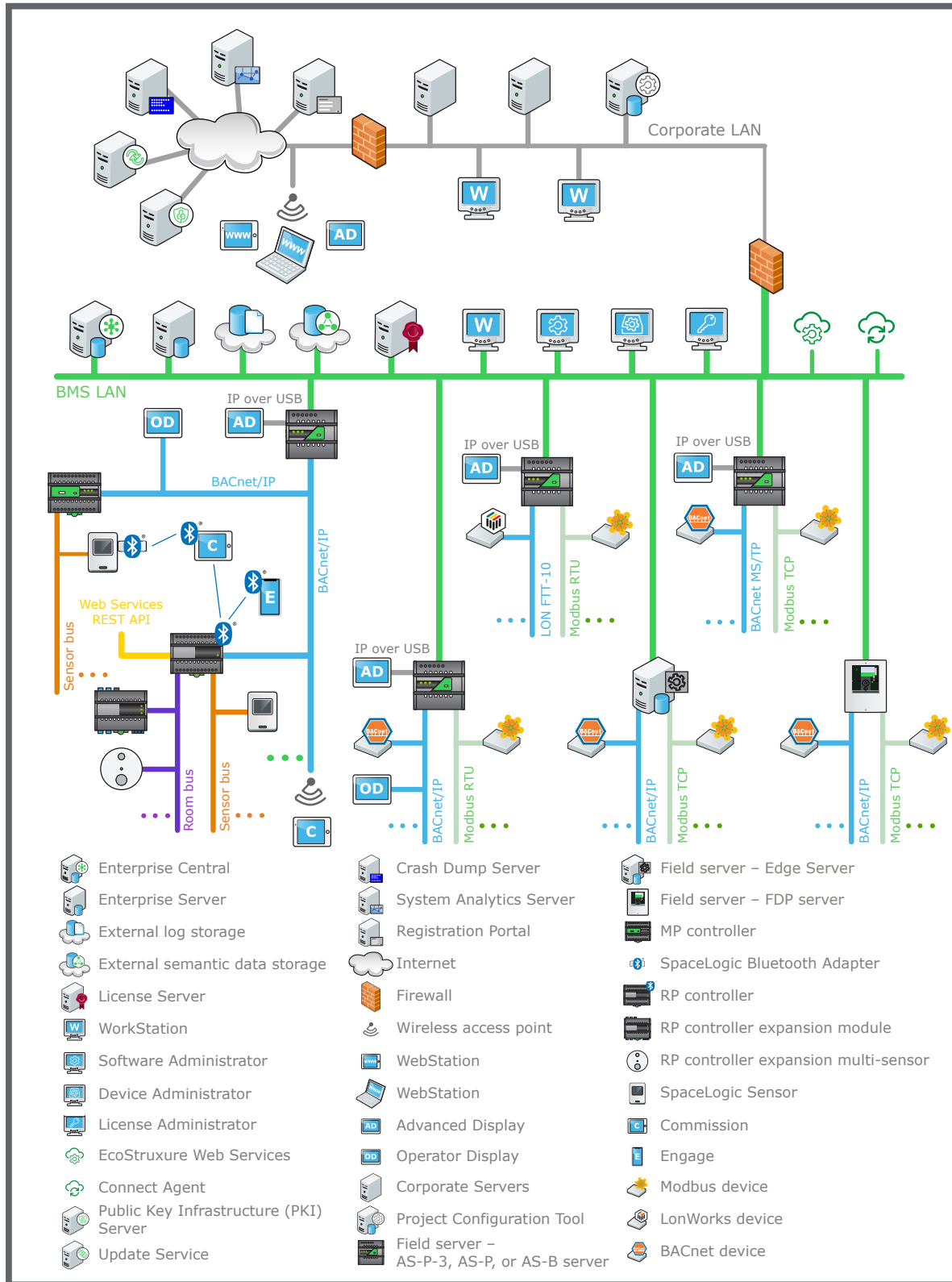
Servers should be protected against cybersecurity threats by using standard IT hardening methods, such as a firewall and port filtering. The servers in the EcoStruxure BMS have several internal cybersecurity

features. However, a defense-in-depth approach is recommended, particularly when Internet connectivity is required. Direct Internet connectivity is not supported.

The figure below shows the best practice architecture for the implementation of a Building Management System LAN connected to a Corporate LAN. The primary feature is the presence of the segregation firewall that effectively decouples the two networks.

Information Technology System Planning Guide

EcoStruxure Building Management



IT architecture implementation example

Information Technology System Planning Guide

EcoStruxure Building Management

On the Corporate LAN side, there may be many EcoStruxure Building Operation WorkStations. They are used to program and manage the Building Management System equipment.

Mobile and wireless devices are becoming as prevalent in the Building Management System world as they are in the corporate world. Building management professionals require secure and easy access to the Building Management System. The IT professional should plan on providing a pathway from the wireless system to the Building Management System firewall.

On the Building Management System side, a wide range of IP devices are operational 24/7/365:

- EcoStruxure Building Operation WorkStations
- EcoStruxure BMS servers that are EcoStruxure Building Operation software applications (Enterprise Central and Enterprise Server)
- Field servers – Building automation

Automation servers:

- AS-P-3, AS-P, and AS-B servers: These EcoStruxure BMS servers are hardware devices and use TCP/IP for their main communications and additionally support a wide array of open and proprietary serial bus protocols.
- Edge Server: This EcoStruxure BMS server corresponds to an AS-P server but is software only and uses only TCP/IP for communications (without support for serial communications).

- Field server – Fire detection
 - FDP server: This EcoStruxure BMS server is the core of a fire detection system. The FDP server is the software included in a Fire Detection Panel (FDP) hardware device and it uses TCP/IP for communications.
- SpaceLogic BACnet/IP devices:
 - RP controllers (RP-C and RP-V): These are IP-based field controllers, which are connected to an automation server or an Enterprise Server using various network topologies such as star, daisy-chain, or RSTP.
 - MP controllers (MP-C and MP-V): These are IP-based field controllers, which are connected to an automation server or an Enterprise Server using various network topologies such as star, daisy-chain, or RSTP.

- IP-IO modules: These are IP-based I/O extension modules, which are connected to an RP or MP controller, an automation server, or an Enterprise Server using various network topologies such as star, daisy-chain, or RSTP.

- External log storage for historical data can either be installed on the same PC as the Enterprise Central or Enterprise Server or on a separate PC.
- Graphical database for external storage of semantic information:
 - Enterprise Server and Enterprise Central for Windows: The semantic data storage is installed as part of the Enterprise Server or Enterprise Central installer.
 - Enterprise Server and Enterprise Central for Linux: The servers do not come with a prepackaged semantic data storage, but support the same semantic graph database as in the Windows case.
 - In both the Windows and Linux case: The semantic data storage can be installed either on the same computer as Enterprise Server or Enterprise Central, or on a separate computer. The EcoStruxure Building Operation software supports one semantic data storage per EcoStruxure BMS.

During normal operation, only a very limited amount of well-defined data needs to pass through the firewall, which ensures a simplified configuration of the segregation firewall.

Types of traffic

In general, communication passing through the segregation firewall is associated with the following functions:

- HTTPS: This protocol is used for Building Management System engineering and monitoring, reports, web services, and EcoStruxure Web Services.

EcoStruxure Web Services is a Schneider Electric web services standard used for integration between systems. In certain scenarios, the EcoStruxure Web Services traffic remains on the Building Management System LAN, and in other scenarios, the traffic could traverse public networks. As such, the firewall needs to be configured according to each use case.

Information Technology System Planning Guide

EcoStruxure Building Management

- SSH: This protocol is used for EcoStruxure Building Operation software upgrade operations on field servers.
- SNMPv3: This protocol is used to monitor servers within an EcoStruxure BMS using standard SNMP Managers supporting SNMP version 3 authentication. The protocol can also be used by the EcoStruxure BMS to send trap notifications to an SNMP management console.
- SMTPS: This protocol is used to send secure email messages.
- Simple XML Web Service communication
- SOAP Web Service communication
- MQTT communication
- Crash dump server communication (Connect Agent)
- PKI server communication using EST protocol

Proxy support

The EcoStruxure BMS supports the use of HTTP/HTTPS forward proxies for the following functions:

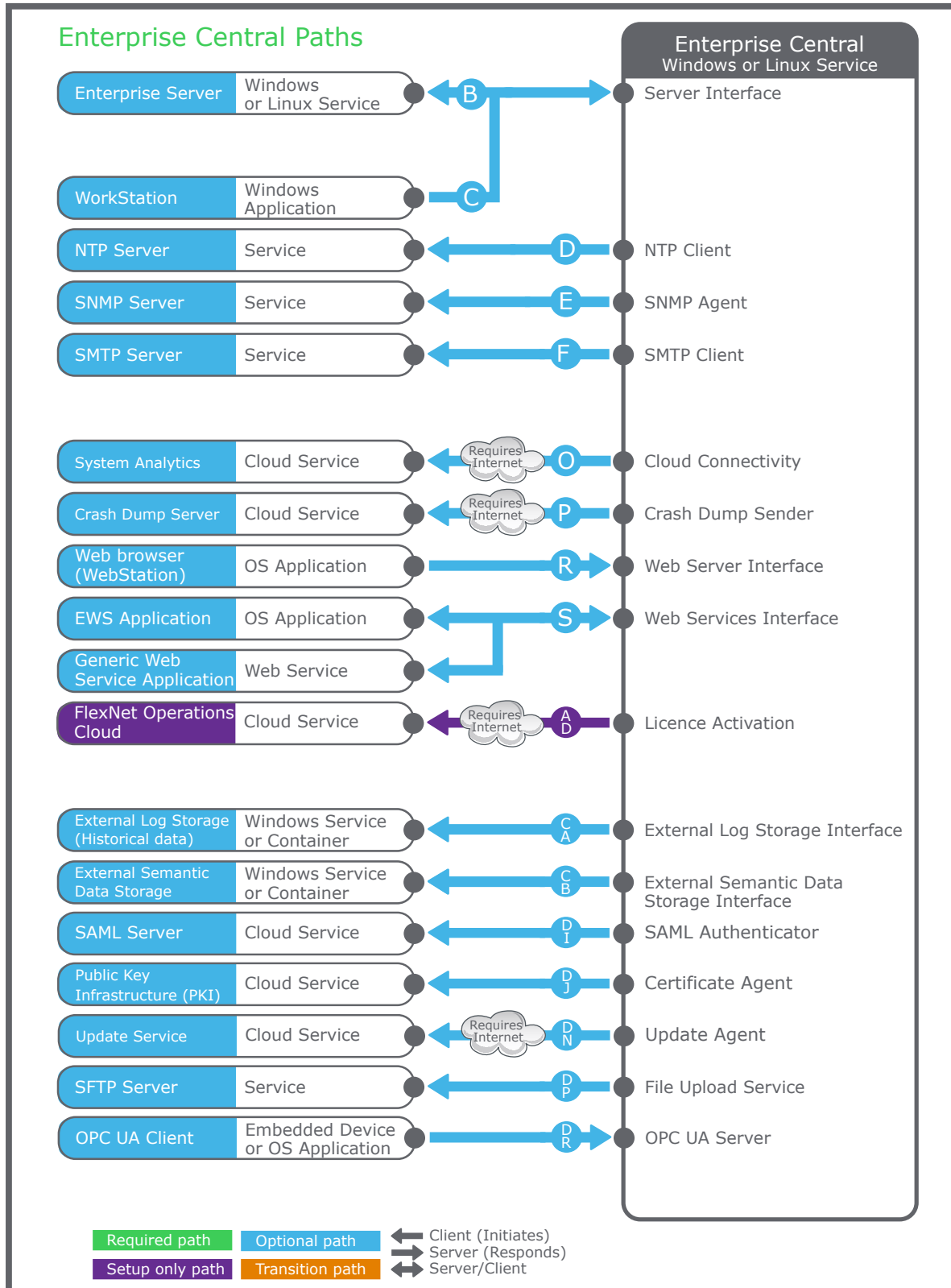
- Server-to-server communication
- Client-to-server communication

Open port on segregation firewall

The active communication paths should first be identified between network segments. Refer to the Communication Paths figure for the respective IP device to determine the paths that will be active to support the targeted system design. Then refer to the Network Ports table for the respective IP device to identify the network ports each path will require. All of the required ports should be configured for both inbound and outbound communication.

Information Technology System Planning Guide

EcoStruxure Building Management



Enterprise Central – Communication paths

Information Technology System Planning Guide

EcoStruxure Building Management

Enterprise Central – Network Ports

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
B ^a (option 1)	Server to server comm.	IT (IPv4/IPv6)	TCP (Config.)	4444 (TCP)	Yes	No	Persistent	-	-
B ^a (option 2)	Server to server comm.	IT (IPv4/IPv6)	HTTPS/WSS ^b (Config.)	443 (TCP)	Yes	No	Persistent	-	-
B ^a (option 3)	Server to server comm.	IT (IPv4/IPv6)	HTTP (Config.)	80 (TCP)	Yes	Yes	Persistent	-	-
C ^a (option 1)	Client to server comm.	IT (IPv4/IPv6)	HTTP (Config.)	80 (TCP)	Yes	Yes	On demand	-	-
C ^a (option 2)	Client to server comm.	IT (IPv4/IPv6)	HTTPS (Config.)	443 (TCP)	Yes	-	On demand	-	-
D	Time synch.	IT (IPv4)	NTP (Disabled)	123 (UDP)	-	Yes	Persistent	-	-
E	Network mgmt	IT (IPv4)	SNMPv3 (Disabled)	161/162 (UDP)	-	Yes	Persistent	-	-
F (option 1)	Email	IT (IPv4)	SMTP (Disabled)	25 (TCP)	-	Yes	Persistent	-	-
F (option 2)	Email	IT (IPv4)	SMTSPS (Disabled)	587 (TCP)	Yes	Yes	Persistent	-	-
O ^c	System analytics	IT (IPv4)	HTTPS (Enabled)	443 (TCP)	-	Yes	Persistent	Yes	-
P	Crash dumps	IT (IPv4)	SFTP (Enabled)	22 (TCP)	Yes	Yes	On demand	Yes	-
R (option 1)	Client to server comm.	IT (IPv4/IPv6)	HTTP (Enabled)	80 (TCP)	Yes	Yes ^d	On demand	-	Redirect to HTTPS
R (option 2)	Client to server comm.	IT (IPv4/IPv6)	HTTPS (Enabled)	443 (TCP)	Yes	Yes ^d	On demand	-	-
S (option 1)	Client to server comm.	IT (IPv4)	HTTP (Disabled)	80 (TCP)	Yes	Yes	On demand	-	Redirect to HTTPS
S (option 2)	Client to server comm.	IT (IPv4)	HTTPS (Disabled)	443 (TCP)	Yes	Yes	On demand	-	-
AD	License activation	Propriet. (IPv4)	HTTPS (Enabled)	443 (TCP)	-	-	Setup only	Yes ^e	-

Information Technology System Planning Guide

EcoStruxure Building Management

Continued

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
CA (option 1) ^f	External log storage	IT (IPv4)	TCP (Enabled)	5432 (TCP)	Yes	Yes ^g	Persistent	-	SSL
CA (option 2) ^h	External log storage	IT (IPv4)	TCP (Enabled)	1433 (TCP)	Yes	Yes ^g	Persistent	-	SSL
CA (option 3) ⁱ	External log storage	IT (IPv4)	HTTP (Enabled)	80 / 443 (TCP)	Yes	Yes ^g	Persistent	-	SSL
CB	Ext. semantic data storage	IT (IPv4)	HTTPS (Enabled)	7200 ^j (TCP)	Yes ^k	Yes ^g	Persistent	-	-
DI	SAML	IoT open protocol (IPv4)	HTTPS (Disabled)	443 (TCP)	Yes	Yes	On demand	-	-
DJ ^l	Certificate management	IT (IPv4)	HTTPS (Disabled)	443 (TCP)	Yes	Yes	On demand	-	-
DN ^m	Software updates	IT (IPv4)	HTTPS (Enabled)	443 (TCP)	-	Yes	On demand	Yes	-
DP ⁿ	File Upload	IT (IPv4)	SFTP (Disabled)	22 (TCP)	Yes	Yes	On demand	-	-
DR	OPC UA	BMS open protocol (IPv4/IPv6)	OPC UA (Disabled)	4840 (TCP)	Yes	Yes ^o	On demand	-	-

a) This communication path uses dynamic port assignment. The port assignment is controlled by the operating system (Windows). The allowable range for the port assignment is configurable from Windows. The default dynamic port range depends on the operating system. For the EcoStruxure Building Operation software supported Windows versions, the default port range is 49152 to 65535.

b) WebSocket Secure (WSS) is supported in EcoStruxure Building Operation version 6.0 and later.

c) This communication path applies both to Enterprise Central and the optionally installed cloud agent.

d) Not for WebStation.

e) Optional file-based activation.

f) TimescaleDB and PostgreSQL

g) The port can be disabled by stopping the Windows service for the database.

h) Microsoft SQL Server

i) AVEVA PI System

j) The communication between Enterprise Central and the semantic graph database is encrypted by default and the default port is 7200.

k) The port can be configured during installation. The port cannot be changed after installation.

l) This communication path applies both to the certificate agent installed with Enterprise Central and the optionally installed certificate agent. The optionally installed certificate agent differs in that the communication is enabled by default, the port is not configurable, and Internet connection is required.

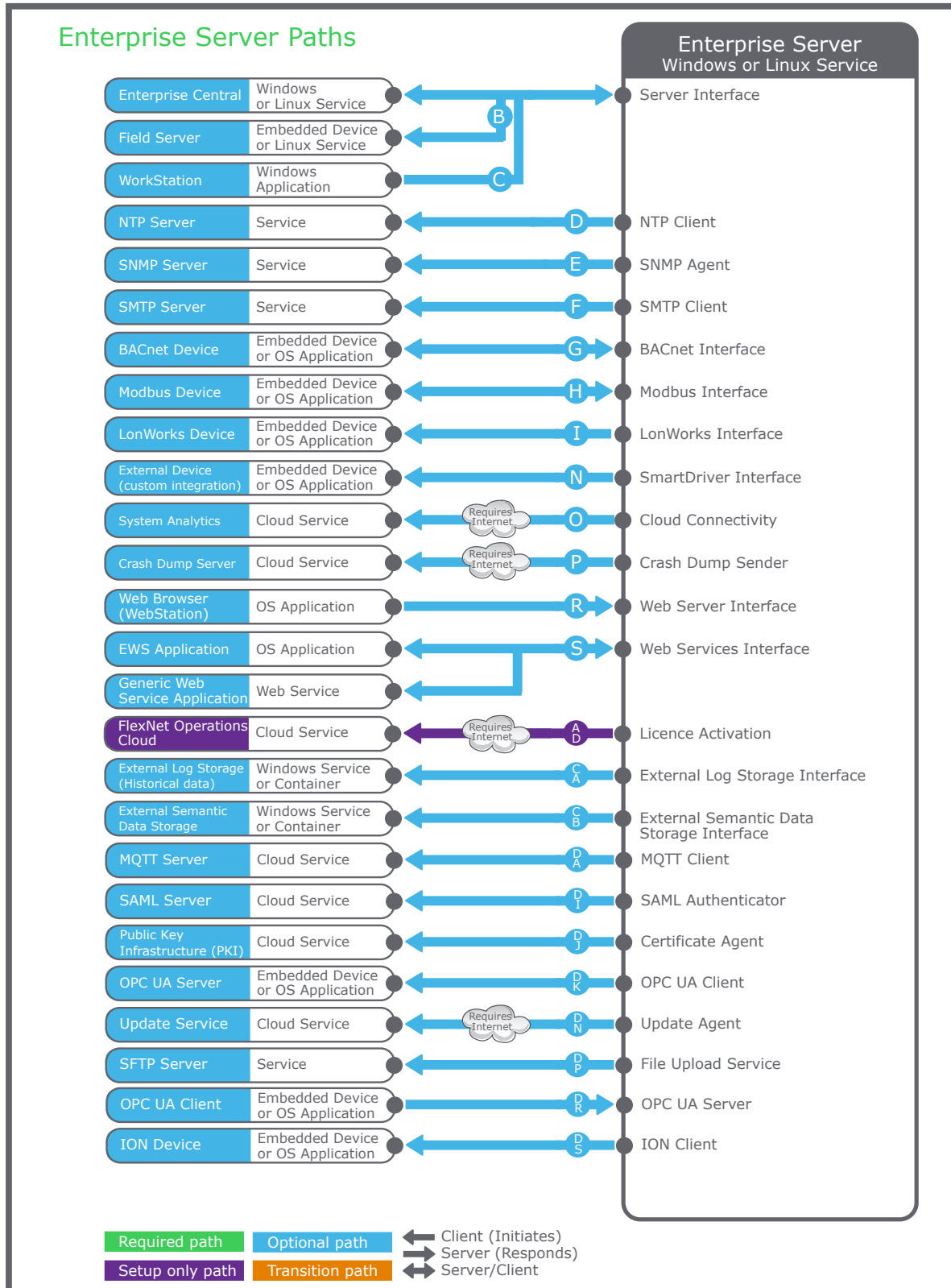
m) This communication path corresponds to the optionally installed update agent.

n) This communication path is supported in EcoStruxure Building Operation version 7.0.2 and later.

o) Ports are not active if all devices are disabled.

Information Technology System Planning Guide

EcoStruxure Building Management



Enterprise Server – Communication paths

Information Technology System Planning Guide

EcoStruxure Building Management

Enterprise Server – Network Ports

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
B ^a (option 1)	Server to server comm.	IT (IPv4/IPv6)	TCP (Config.)	4444 (TCP)	Yes	No	Persistent	-	-
B ^a (option 2)	Server to server comm.	IT (IPv4/IPv6)	HTTPS/WSS ^b (Config.)	443 (TCP)	Yes	No	Persistent	-	-
B ^a (option 3)	Server to server comm.	IT (IPv4/IPv6)	HTTP (Config.)	80 (TCP)	Yes	Yes	Persistent	-	-
C ^a (option 1)	Client to server comm.	IT (IPv4/IPv6)	HTTP (Config.)	80 (TCP)	Yes	Yes	On demand	-	-
C ^a (option 2)	Client to server comm.	IT (IPv4/IPv6)	HTTPS (Config.)	443 (TCP)	Yes	-	On demand	-	-
D	Time synch.	IT (IPv4)	NTP (Disabled)	123 (UDP)	-	Yes	Persistent	-	-
E	Network mgmt	IT (IPv4)	SNMPv3 (Disabled)	161/162 (UDP)	-	Yes	Persistent	-	-
F (option 1)	Email	IT (IPv4)	SMTP (Disabled)	25 (TCP)	-	Yes	Persistent	-	-
F (option 2)	Email	IT (IPv4)	SMTSPS (Disabled)	587 (TCP)	Yes	Yes	Persistent	-	-
G (option 1)	BACnet integr.	BMS open protocol (IPv4)	BACnet/IP (Disabled)	47808 / 33487 (UDP)	Yes	Yes	Persistent	-	-
G (option 2)	BACnet integr.	BMS open protocol (IPv4)	WebSocket Secure (WSS) ^c (Disabled)	-	Yes	Yes	Persistent	-	-
H	Modbus integr.	BMS open protocol (IPv6)	Modbus TCP (Disabled)	502 (TCP)	-	Yes	Persistent	-	-
I	LonWorks integr.	BMS open protocol (IPv4)	LonWorks IP (Disabled)	1628 (UDP)	-	Yes	Persistent	-	-
N	Integr.	Driver depend.	Driver depend. (Disabled)	Driver depend.	Driver depend.	Yes	Persistent	-	-

Information Technology System Planning Guide

EcoStruxure Building Management

Continued

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
O ^d	System analytics	IT (IPv4)	HTTPS (Enabled)	443 (TCP)	-	Yes	Persistent	Yes	-
P	Crash dumps	IT (IPv4)	SFTP (Enabled)	22 (TCP)	Yes	Yes	On demand	Yes	-
R (option 1)	Client to server comm.	IT (IPv4/IPv6)	HTTP (Enabled)	80 (TCP)	Yes	Yes ^e	On demand	-	Redirect to HTTPS
R (option 2)	Client to server comm.	IT (IPv4/IPv6)	HTTPS (Enabled)	443 (TCP)	Yes	Yes ^e	On demand	-	-
S (option 1)	Client to server comm.	IT (IPv4)	HTTP (Disabled)	80 (TCP)	Yes	Yes	On demand	-	Redirect to HTTPS
S (option 2)	Client to server comm.	IT (IPv4)	HTTPS (Disabled)	443 (TCP)	Yes	Yes	On demand	-	-
AD	License activation	Propriet. (IPv4)	HTTPS (Enabled)	443 (TCP)	-	-	Setup only	Yes ^f	-
CA (option 1) ^g	External log storage	IT (IPv4)	TCP (Enabled)	5432 (TCP)	Yes	Yes ^h	Persistent	-	SSL
CA (option 2) ⁱ	External log storage	IT (IPv4)	TCP (Enabled)	1433 (TCP)	Yes	Yes ^h	Persistent	-	SSL
CA (option 3) ^j	External log storage	IT (IPv4)	HTTP (Enabled)	80 / 443 (TCP)	Yes	Yes ^h	Persistent	-	SSL
CB	Ext. semantic data storage	IT (IPv4)	HTTPS (Enabled)	7200 ^k (TCP)	Yes ^l	Yes ^h	Persistent	-	-
DA (option 1)	MQTT	IoT open protocol (IPv4)	TLS (Enabled)	8883 (TCP)	Yes	Yes	Persistent	_m	-
DA (option 2)	MQTT	IoT open protocol (IPv4)	TCP (Disabled)	1883 (TCP)	Yes	Yes	Persistent	_m	-
DA (option 3)	MQTT	IoT open protocol (IPv4)	WebSocket Secure (WSS) (Disabled)	443 (TCP)	Yes	Yes	Persistent	_m	-
DA (option 4)	MQTT	IoT open protocol (IPv4)	WebSocket (WS) (Disabled)	80 (TCP)	Yes	Yes	Persistent	_m	-

Information Technology System Planning Guide

EcoStruxure Building Management

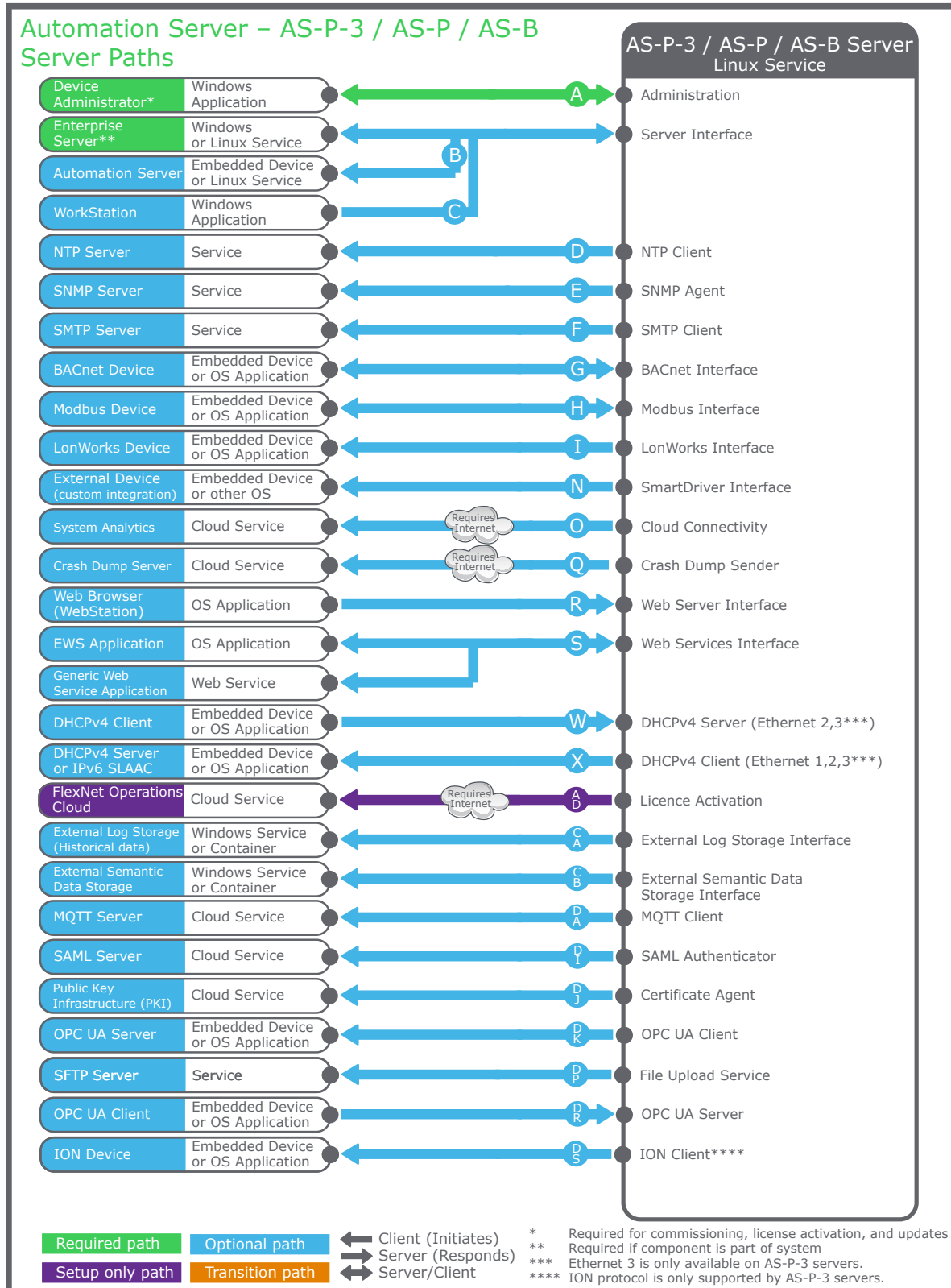
Continued

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
DI	SAML	IoT open protocol (IPv4)	HTTPS (Disabled)	443 (TCP)	Yes	Yes	On demand	-	-
DJ ⁿ	Certificate management	IT (IPv4)	HTTPS (Disabled)	443 (TCP)	Yes	Yes	On demand	-	-
DK	OPC UA	BMS open protocol (IPv4/IPv6)	OPC UA (Disabled)	- (TCP)	Yes	Yes ^o	On demand	-	-
DN ^p	Software updates	IT (IPv4)	HTTPS (Enabled)	443 (TCP)	-	Yes	On demand	Yes	-
DP ^q	File Upload	IT (IPv4)	SFTP (Disabled)	22 (TCP)	Yes	Yes	On demand	-	-
DR	OPC UA	BMS open protocol (IPv4/IPv6)	OPC UA (Disabled)	4840 (TCP)	Yes	Yes ^o	On demand	-	-
DS	ION integration	BMS propriet. (IPv4)	ION TCP (Enabled)	7700 (TCP)	Yes	Yes	Persistent	-	-

- a) This communication path uses dynamic port assignment. The port assignment is controlled by the operating system (Windows). The allowable range for the port assignment is configurable from Windows. The default dynamic port range depends on the operating system. For the EcoStruxure Building Operation software supported Windows versions, the default port range is 49152 to 65535.
- b) WebSocket Secure (WSS) is supported in EcoStruxure Building Operation version 6.0 and later.
- c) WebSocket Secure (WSS) is used for BACnet Secure Connect (BACnet/SC) applications.
- d) This communication path applies to both Enterprise Server and the optionally installed cloud agent.
- e) Not for WebStation.
- f) Optional file-based activation.
- g) TimescaleDB and PostgreSQL
- h) The port can be disabled by stopping the Windows service for the database.
- i) Microsoft SQL Server
- j) AVEVA PI System
- k) The communication between Enterprise Server and the semantic graph database is encrypted by default and the default port is 7200.
- l) The port can be configured during installation. The port cannot be changed after installation.
- m) An Internet connection is not needed when you run the cloud service on the same local network as Enterprise Server.
- n) This communication path applies both to the certificate agent installed with Enterprise Server and the optionally installed certificate agent. The optionally installed certificate agent differs in that the communication is enabled by default, the port is not configurable, and Internet connection is required.
- o) Ports are not active if all devices are disabled.
- p) This communication path corresponds to the optionally installed update agent.
- q) This communication path is supported in EcoStruxure Building Operation version 7.0.2 and later.

Information Technology System Planning Guide

EcoStruxure Building Management



Field server (automation server) – AS-P-3, AS-P, or AS-B server – Communication paths

Information Technology System Planning Guide

EcoStruxure Building Management

Field Server (Automation Server) – AS-P-3, AS-P, or AS-B Server – Network Ports

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
A	Administration	Propriet. (IPv4/IPv6)	SSH (Enabled)	22 (TCP)	Yes	Yes	Config. only	-	-
B ^a (option 1)	Server to server comm.	IT (IPv4/IPv6)	TCP (Config.)	4444 (TCP)	No	No	Persistent	-	-
B ^a (option 2)	Server to server comm.	IT (IPv4/IPv6)	HTTPS/WSS ^b (Config.)	443 (TCP)	Yes	No	Persistent	-	-
B ^a (option 3)	Server to server comm.	IT (IPv4/IPv6)	HTTP (Config.)	80 (TCP)	Yes	Yes	Persistent	-	-
C ^a (option 1)	Client to server comm.	IT (IPv4/IPv6)	HTTP (Config.)	80 (TCP)	Yes	Yes	On demand	-	-
C ^a (option 2)	Client to server comm.	IT (IPv4/IPv6)	HTTPS (Config.)	443 (TCP)	Yes	-	On demand	-	-
D	Time synch.	IT (IPv4)	NTP (Disabled)	123 (UDP)	-	Yes	Persistent	-	-
E	Network mgmt	IT (IPv4)	SNMPv3 (Disabled)	161/162 (UDP)	-	Yes	Persistent	-	-
F (option 1)	Email	IT (IPv4)	SMTP (Disabled)	25 (TCP)	-	Yes	Persistent	-	-
F (option 2)	Email	IT (IPv4)	SMTSPS (Disabled)	587 (TCP)	Yes	Yes	Persistent	-	-
G (option 1)	BACnet integr.	BMS open protocol (IPv4)	BACnet/IP (Disabled)	47808 / 33487 (UDP)	Yes	Yes	Persistent	-	-
G (option 2)	BACnet integr.	BMS open protocol (IPv4)	WebSocket Secure (WSS) ^c (Disabled)	-	Yes	Yes	Persistent	-	-
H	Modbus integr.	BMS open protocol (IPv6)	Modbus TCP (Disabled)	502 (TCP)	-	Yes	Persistent	-	-
I	LonWorks integr.	BMS open protocol (IPv4)	LonWorks IP (Disabled)	1628 (UDP)	-	Yes	Persistent	-	-

Information Technology System Planning Guide

EcoStruxure Building Management

Continued

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
N	Integr.	Driver depend.	Driver depend. (Disabled)	Driver depend.	Driver depend.	Yes	Persistent	-	-
O	System analytics	IT (IPv4)	HTTPS (Enabled)	443 (TCP)	-	Yes	Persistent	Yes	-
Q	Crash dumps	IT (IPv4)	HTTPS (Enabled)	443 (TCP)	Yes	Yes	On demand	Yes	-
R (option 1)	Client to server comm.	IT (IPv4/IPv6)	HTTP (Enabled)	80 (TCP)	Yes	Yes ^d	On demand	-	Redirect to HTTPS
R (option 2)	Client to server comm.	IT (IPv4/IPv6)	HTTPS (Enabled)	443 (TCP)	Yes	Yes ^d	On demand	-	-
S (option 1)	Client to server comm.	IT (IPv4)	HTTP (Disabled)	80 (TCP)	Yes	Yes	On demand	-	Redirect to HTTPS
S (option 2)	Client to server comm.	IT (IPv4)	HTTPS (Disabled)	443 (TCP)	Yes	Yes	On demand	-	-
W	DHCPv4	IT (IPv4)	DHCPv4 (Disabled)	67 (UDP)	-	Yes	Persistent	-	-
X	DHCPv4 or IPv6 SLAAC	IT (IPv4/IPv6)	DHCPv4 or IPv6 SLAAC (Enabled)	68 (UDP)	-	Yes	On demand	-	-
AD	License activation	Propriet. (IPv4)	HTTPS (Enabled)	443 (TCP)	-	-	Setup only	Yes ^e	-
CA (option 1) ^f	External log storage	IT (IPv4)	TCP (Enabled)	5432 (TCP)	Yes	Yes ^g	Persistent	-	SSL
CA (option 2) ^h	External log storage	IT (IPv4)	TCP (Enabled)	1433 (TCP)	Yes	Yes ^g	Persistent	-	SSL
CA (option 3) ⁱ	External log storage	IT (IPv4)	HTTP (Enabled)	80 / 443 (TCP)	Yes	Yes ^g	Persistent	-	SSL
CB	Ext. semantic data storage	IT (IPv4)	HTTPS (Enabled)	7200 ^j (TCP)	Yes ^k	Yes ^g	Persistent	-	-
DA (option 1)	MQTT	IoT open protocol (IPv4)	TLS (Enabled)	8883 (TCP)	Yes	Yes	Persistent	- ^l	-

Information Technology System Planning Guide

EcoStruxure Building Management

Continued

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
DA (option 2)	MQTT	IoT open protocol (IPv4)	TCP (Disabled)	1883 (TCP)	Yes	Yes	Persistent	↓	-
DA (option 3)	MQTT	IoT open protocol (IPv4)	WebSocket Secure (WSS) (Disabled)	443 (TCP)	Yes	Yes	Persistent	↓	-
DA (option 4)	MQTT	IoT open protocol (IPv4)	WebSocket (WS) (Disabled)	80 (TCP)	Yes	Yes	Persistent	↓	-
DI	SAML	IoT open protocol (IPv4)	HTTPS (Disabled)	443 (TCP)	Yes	Yes	On demand	-	-
DJ ^m	Certificate management	IT (IPv4)	HTTPS (Disabled)	443 (TCP)	Yes	Yes	On demand	-	-
DK	OPC UA	BMS open protocol (IPv4/IPv6)	OPC UA (Disabled)	- (TCP)	Yes	Yes ⁿ	On demand	-	-
DP ^o	File Upload	IT (IPv4)	SFTP (Disabled)	22 (TCP)	Yes	Yes	On demand	-	-
DR	OPC UA	BMS open protocol (IPv4/IPv6)	OPC UA (Disabled)	4840 (TCP)	Yes	Yes ⁿ	On demand	-	-
DS ^p	ION integration	BMS propriet. (IPv4)	ION TCP (Enabled)	7700 (TCP)	Yes	Yes	Persistent	-	-

a) This communication path uses dynamic port assignment. The port assignment is controlled by the operating system (Linux). The allowable range for the port assignment is not configurable. The default dynamic port range depends on the operating system. For automation servers (Linux), the default port range is 32768 to 61000.

b) WebSocket Secure (WSS) is supported in EcoStruxure Building Operation version 6.0 and later.

c) WebSocket Secure (WSS) is used for BACnet Secure Connect (BACnet/SC) applications.

d) Not for WebStation.

e) Optional file-based activation.

f) TimescaleDB and PostgreSQL

g) The port can be disabled by stopping the Windows service for the database.

h) Microsoft SQL Server

i) AVEVA PI System

j) The communication between the automation server and the SPARQL database is encrypted by default and the default port is 7200.

k) The port can be configured during installation. The port cannot be changed after installation.

l) An Internet connection is not needed when you run the cloud service on the same local network as the automation server.

m) Supported by AS-P and AS-B servers. Not supported by AS-P-3 servers.

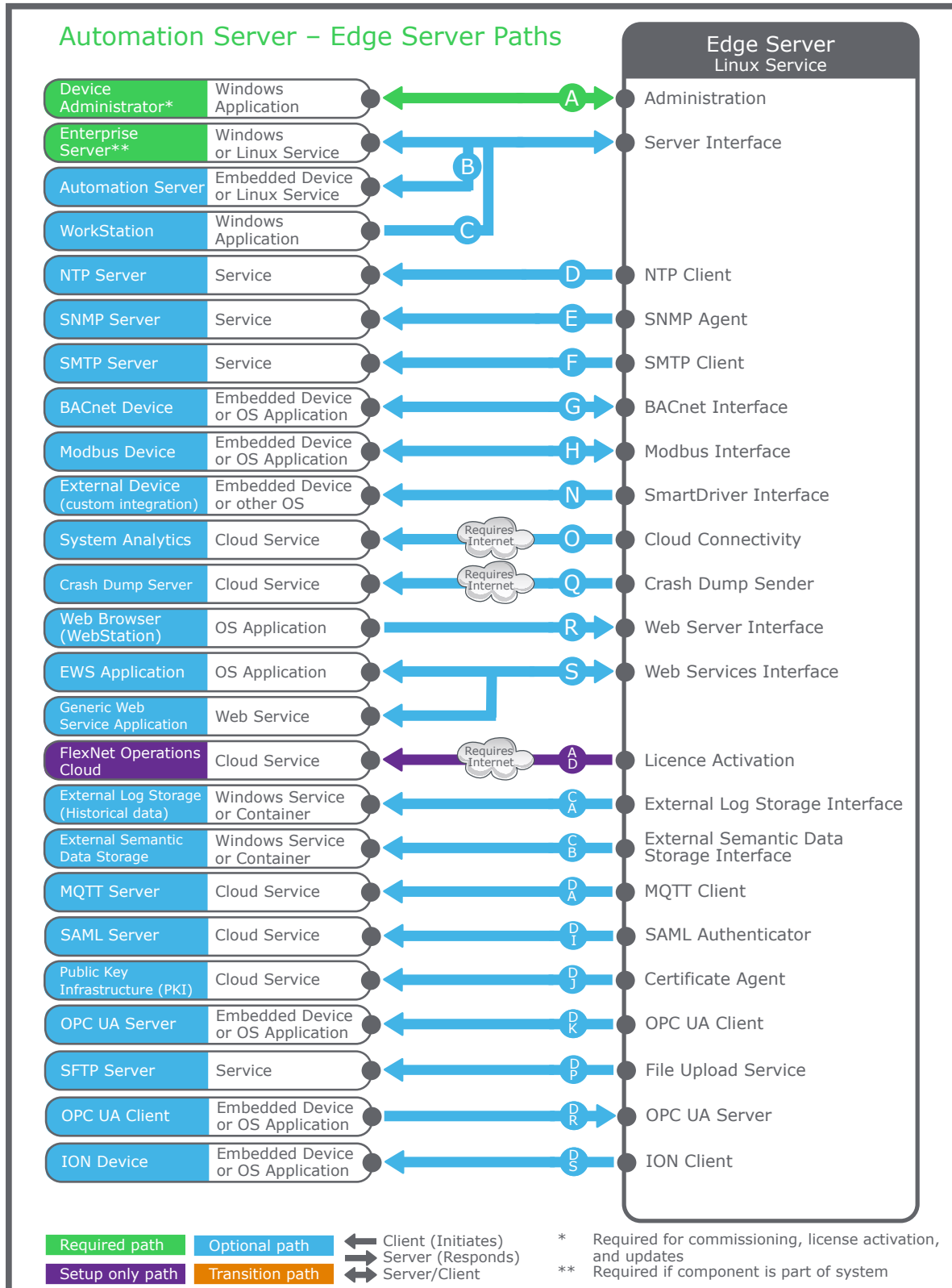
n) Ports are not active if all devices are disabled.

o) This communication path is supported in EcoStruxure Building Operation version 7.0.2 and later.

p) Supported by AS-P-3 servers. Not supported by AS-P and AS-B servers.

Information Technology System Planning Guide

EcoStruxure Building Management



Field server (automation server) – Edge Server – Communication paths

Information Technology System Planning Guide

EcoStruxure Building Management

Field Server (Automation Server) – Edge Server – Network Ports

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
A	Administration	Propriet. (IPv4/IPv6)	SSH (Enabled)	22 (TCP)	Yes	Yes	Config. only	-	-
B ^a (option 1)	Server to server comm.	IT (IPv4/IPv6)	TCP (Config.)	4444 (TCP)	Yes	No	Persistent	-	-
B ^a (option 2)	Server to server comm.	IT (IPv4/IPv6)	HTTPS/WSS ^b (Config.)	443 (TCP)	Yes	No	Persistent	-	-
B ^a (option 3)	Server to server comm.	IT (IPv4/IPv6)	HTTP (Config.)	80 (TCP)	Yes	Yes	Persistent	-	-
C ^a (option 1)	Client to server comm.	IT (IPv4/IPv6)	HTTP (Config.)	80 (TCP)	Yes	Yes	On demand	-	-
C ^a (option 2)	Client to server comm.	IT (IPv4/IPv6)	HTTPS (Config.)	443 (TCP)	Yes	-	On demand	-	-
D	Time synch.	IT (IPv4)	NTP (Disabled)	123 (UDP)	-	Yes	Persistent	-	-
E	Network mgmt	IT (IPv4)	SNMPv3 (Disabled)	161/162 (UDP)	-	Yes	Persistent	-	-
F (option 1)	Email	IT (IPv4)	SMTP (Disabled)	25 (TCP)	-	Yes	Persistent	-	-
F (option 2)	Email	IT (IPv4)	SMTPS (Disabled)	587 (TCP)	Yes	Yes	Persistent	-	-
G (option 1)	BACnet integr.	BMS open protocol (IPv4)	BACnet/IP (Disabled)	47808 / 33487 (UDP)	Yes	Yes	Persistent	-	-
G (option 2)	BACnet integr.	BMS open protocol (IPv4)	WebSocket Secure (WSS) ^c (Disabled)	-	Yes	Yes	Persistent	-	-
H	Modbus integr.	BMS open protocol (IPv6)	Modbus TCP (Disabled)	502 (TCP)	-	Yes	Persistent	-	-
N	Integr.	Driver depend.	Driver depend. (Disabled)	Driver depend.	Driver depend.	Yes	Persistent	-	-

Information Technology System Planning Guide

EcoStruxure Building Management

Continued

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
O	System analytics	IT (IPv4)	HTTPS (Enabled)	443 (TCP)	-	Yes	Persistent	Yes	-
Q	Crash dumps	IT (IPv4)	HTTPS (Enabled)	443 (TCP)	No	Yes	On demand	Yes	-
R (option 1)	Client to server comm.	IT (IPv4/IPv6)	HTTP (Enabled)	80 (TCP)	Yes	Yes ^d	On demand	-	Redirect to HTTPS
R (option 2)	Client to server comm.	IT (IPv4/IPv6)	HTTPS (Enabled)	443 (TCP)	Yes	Yes ^d	On demand	-	-
S (option 1)	Client to server comm.	IT (IPv4)	HTTP (Disabled)	80 (TCP)	Yes	Yes	On demand	-	Redirect to HTTPS
S (option 2)	Client to server comm.	IT (IPv4)	HTTPS (Disabled)	443 (TCP)	Yes	Yes	On demand	-	-
AD	License activation	Propriet. (IPv4)	HTTPS (Enabled)	443 (TCP)	-	-	Setup only	Yes ^e	-
CA (option 1) ^f	External log storage	IT (IPv4)	TCP (Enabled)	5432 (TCP)	Yes	Yes ^g	Persistent	-	SSL
CA (option 2) ^h	External log storage	IT (IPv4)	TCP (Enabled)	1433 (TCP)	Yes	Yes ^g	Persistent	-	SSL
CA (option 3) ⁱ	External log storage	IT (IPv4)	HTTP (Enabled)	80 / 443 (TCP)	Yes	Yes ^g	Persistent	-	SSL
CB	Ext. semantic data storage	IT (IPv4)	HTTPS (Enabled)	7200 ^j (TCP)	Yes ^k	Yes ^g	Persistent	-	-
DA (option 1)	MQTT	IoT open protocol (IPv4)	TLS (Enabled)	8883 (TCP)	Yes	Yes	Persistent	!	-
DA (option 2)	MQTT	IoT open protocol (IPv4)	TCP (Disabled)	1883 (TCP)	Yes	Yes	Persistent	!	-
DA (option 3)	MQTT	IoT open protocol (IPv4)	WebSocket Secure (WSS) (Disabled)	443 (TCP)	Yes	Yes	Persistent	!	-
DA (option 4)	MQTT	IoT open protocol (IPv4)	WebSocket (WS) (Disabled)	80 (TCP)	Yes	Yes	Persistent	!	-

Information Technology System Planning Guide

EcoStruxure Building Management

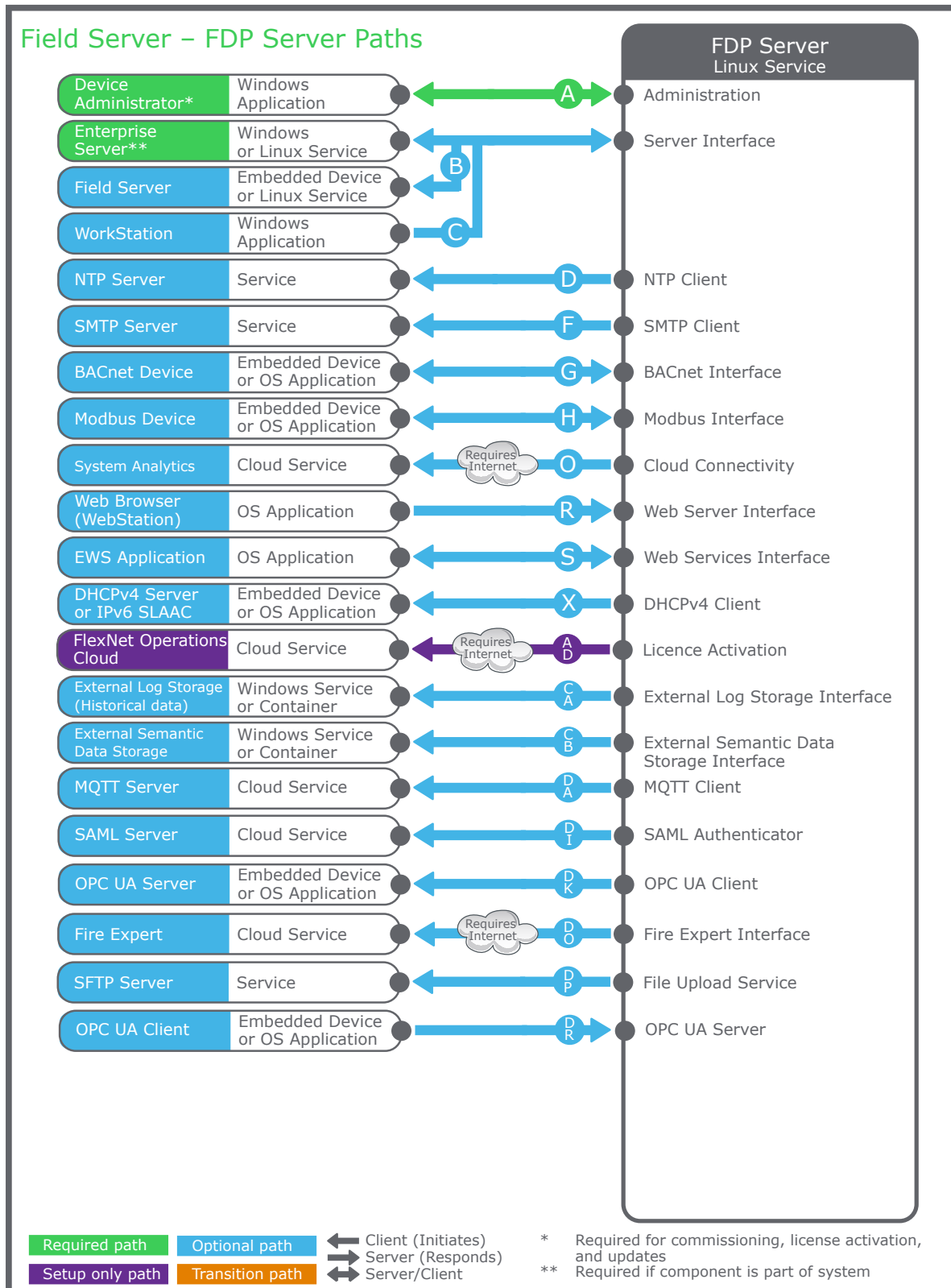
Continued

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
DI	SAML	IoT open protocol (IPv4)	HTTPS (Disabled)	443 (TCP)	Yes	Yes	On demand	-	-
DJ	Certificate management	IT (IPv4)	HTTPS (Disabled)	443 (TCP)	Yes	Yes	On demand	-	-
DK	OPC UA	BMS open protocol (IPv4/IPv6)	OPC UA (Disabled)	- (TCP)	Yes	Yes ^m	On demand	-	-
DP ⁿ	File Upload	IT (IPv4)	SFTP (Disabled)	22 (TCP)	Yes	Yes	On demand	-	-
DR	OPC UA	BMS open protocol (IPv4/IPv6)	OPC UA (Disabled)	4840 (TCP)	Yes	Yes ^m	On demand	-	-
DS	ION integration	BMS propriet. (IPv4)	ION TCP (Enabled)	7700 (TCP)	Yes	Yes	Persistent	-	-

- a) This communication path uses dynamic port assignment. The port assignment is controlled by the operating system (Linux). The allowable range for the port assignment is not configurable. The default dynamic port range depends on the operating system. For automation servers (Linux), the default port range is 32768 to 61000.
- b) WebSocket Secure (WSS) is supported in EcoStruxure Building Operation version 6.0 and later.
- c) WebSocket Secure (WSS) is used for BACnet Secure Connect (BACnet/SC) applications.
- d) Not for WebStation.
- e) Optional file-based activation.
- f) TimescaleDB and PostgreSQL
- g) The port can be disabled by stopping the Windows service for the database.
- h) Microsoft SQL Server
- i) AVEVA PI System
- j) The communication between the automation server and the SPARQL database is encrypted by default and the default port is 7200.
- k) The port can be configured during installation. The port cannot be changed after installation.
- l) An Internet connection is not needed when you run the cloud service on the same local network as the automation server.
- m) Ports are not active if all devices are disabled.
- n) This communication path is supported in EcoStruxure Building Operation version 7.0.2 and later.

Information Technology System Planning Guide

EcoStruxure Building Management



Field server (fire detection) – FDP server – Communication paths

Information Technology System Planning Guide

EcoStruxure Building Management

Field Server (Fire Detection) – FDP Server – Network Ports

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
A	Administration	Propriet. (IPv4/IPv6)	SSH (Enabled)	22 (TCP)	No	No	Upgrade only	-	-
B ^a (option 1)	Server to server comm.	IT (IPv4/IPv6)	TCP (Config.)	4444 (TCP)	No	No	Persistent	-	-
B ^a (option 2)	Server to server comm.	IT (IPv4/IPv6)	HTTPS/WSS ^b (Config.)	443 (TCP)	No	No	Persistent	-	-
B ^a (option 3)	Server to server comm.	IT (IPv4/IPv6)	HTTP (Config.)	80 (TCP)	No	Yes	Persistent	-	-
C ^a (option 1)	Client to server comm.	IT (IPv4/IPv6)	HTTP (Config.)	80 (TCP)	No	Yes	On demand	-	-
C ^a (option 2)	Client to server comm.	IT (IPv4/IPv6)	HTTPS (Config.)	443 (TCP)	No	-	On demand	-	-
D	Time synch.	IT (IPv4)	NTP (Disabled)	123 (UDP)	-	Yes	Persistent	-	-
F (option 1)	Email	IT (IPv4)	SMTP (Disabled)	25 (TCP)	-	Yes	Persistent	-	-
F (option 2)	Email	IT (IPv4)	SMTSPS (Disabled)	587 (TCP)	Yes	Yes	Persistent	-	-
G (option 1)	BACnet integr.	BMS open protocol (IPv4)	BACnet/IP (Disabled)	47808 (UDP)	No	Yes	Persistent	-	-
G (option 2)	BACnet integr.	BMS open protocol (IPv4)	WebSocket Secure (WSS) ^c (Disabled)	47824 (UDP)	No	Yes	Persistent	-	-
H	Modbus integr.	BMS open protocol (IPv6)	Modbus TCP (Disabled)	502 (TCP)	-	Yes	Persistent	-	-
O	System analytics	IT (IPv4)	HTTPS (Enabled)	443 (TCP)	-	Yes	Persistent	Yes	-
R (option 1)	Client to server comm.	IT (IPv4/IPv6)	HTTP (Enabled)	80 (TCP)	No	Yes ^d	On demand	-	Redirect to HTTPS
R (option 2)	Client to server comm.	IT (IPv4/IPv6)	HTTPS (Enabled)	443 (TCP)	No	Yes ^d	On demand	-	-

Information Technology System Planning Guide

EcoStruxure Building Management

Continued

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
S (option 1)	Client to server comm.	IT (IPv4)	HTTP (Disabled)	80 (TCP)	No	Yes	On demand	-	Redirect to HTTPS
S (option 2)	Client to server comm.	IT (IPv4)	HTTPS (Disabled)	443 (TCP)	No	Yes	On demand	-	-
X	DHCPv4 or IPv6 SLAAC	IT (IPv4/IPv6)	DHCPv4 or IPv6 SLAAC (Enabled)	68 (UDP)	-	Yes	On demand	-	-
AD	License activation	Propriet. (IPv4)	HTTPS (Enabled)	443 (TCP)	-	-	Setup only	Yes ^e	-
CA (option 1) ^f	External log storage	IT (IPv4)	TCP (Enabled)	5432 (TCP)	Yes	Yes ^g	Persistent	-	SSL
CA (option 2) ^h	External log storage	IT (IPv4)	TCP (Enabled)	1433 (TCP)	Yes	Yes ^g	Persistent	-	SSL
CA (option 3) ⁱ	External log storage	IT (IPv4)	HTTP (Enabled)	80 / 443 (TCP)	Yes	Yes ^g	Persistent	-	SSL
CB	Ext. semantic data storage	IT (IPv4)	HTTPS (Enabled)	7200 ^j (TCP)	Yes ^k	Yes ^g	Persistent	-	-
DA (option 1)	MQTT	IoT open protocol (IPv4)	TLS (Enabled)	8883 (TCP)	Yes	Yes	Persistent	↓	-
DA (option 2)	MQTT	IoT open protocol (IPv4)	TCP (Disabled)	1883 (TCP)	Yes	Yes	Persistent	↓	-
DA (option 3)	MQTT	IoT open protocol (IPv4)	WebSocket Secure (WSS) (Disabled)	443 (TCP)	Yes	Yes	Persistent	↓	-
DA (option 4)	MQTT	IoT open protocol (IPv4)	WebSocket (WS) (Disabled)	80 (TCP)	Yes	Yes	Persistent	↓	-
DI	SAML	IoT open protocol (IPv4)	HTTPS (Disabled)	443 (TCP)	Yes	Yes	On demand	-	-
DK	OPC UA	BMS open protocol (IPv4/IPv6)	OPC UA (Disabled)	- (TCP)	Yes	Yes ^m	On demand	-	-

Information Technology System Planning Guide

EcoStruxure Building Management

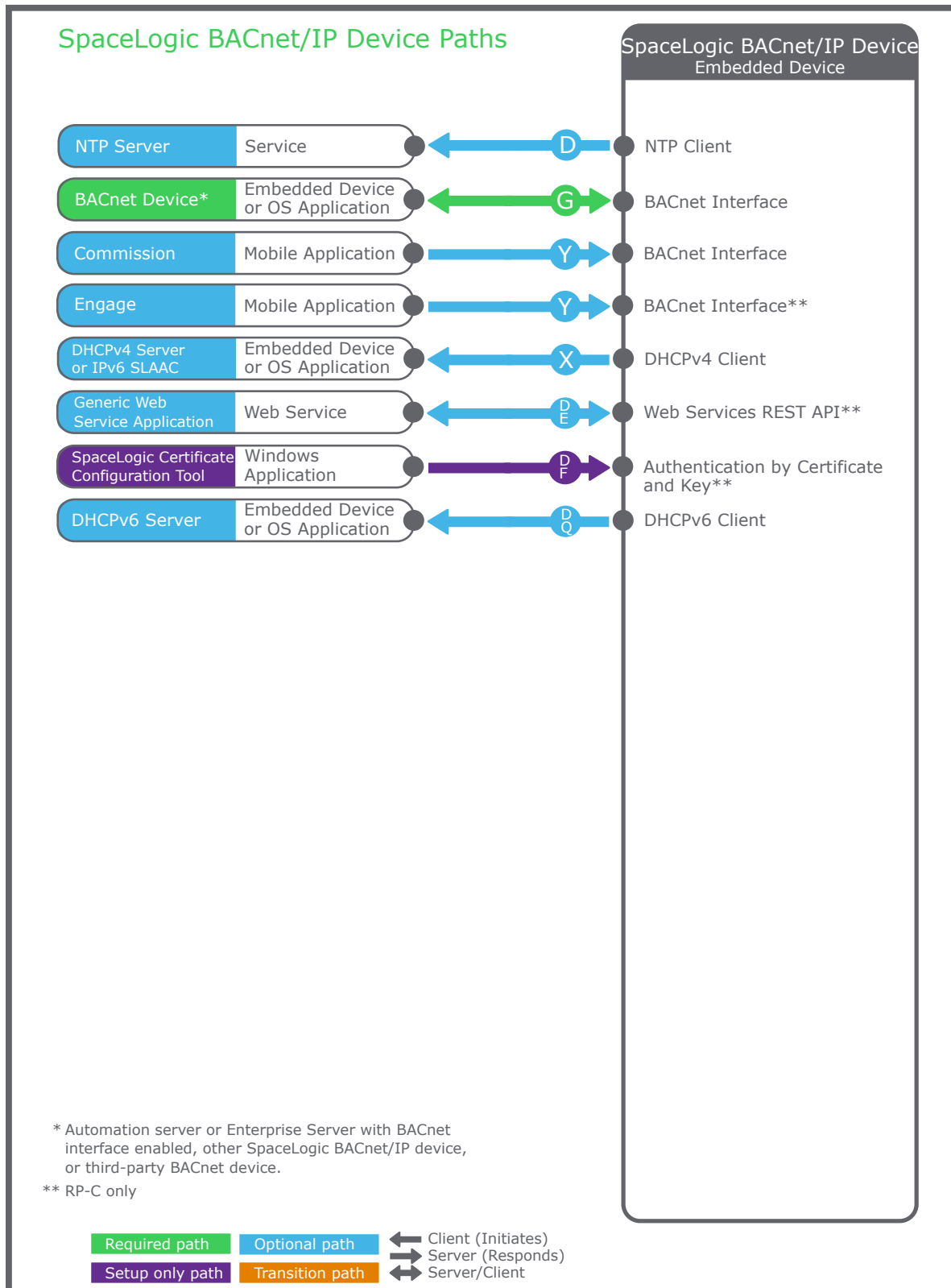
Continued

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
DO	Fire Expert	IT (IPv4)	HTTPS (Enabled)	443 (TCP)	No	Yes	On demand	Yes	-
DP ⁿ	File Upload	IT (IPv4)	SFTP (Disabled)	22 (TCP)	Yes	Yes	On demand	-	-
DR	OPC UA	BMS open protocol (IPv4/IPv6)	OPC UA (Disabled)	4840 (TCP)	No	Yes ^m	On demand	-	-

- a) This communication path uses dynamic port assignment. The port assignment is controlled by the operating system (Linux). The allowable range for the port assignment is not configurable. The default dynamic port range depends on the operating system. For field servers (Linux), the default port range is 32768 to 61000.
- b) WebSocket Secure (WSS) is supported in EcoStruxure Building Operation version 6.0 and later.
- c) WebSocket Secure (WSS) is used for BACnet Secure Connect (BACnet/SC) applications.
- d) Not for WebStation.
- e) Optional file-based activation.
- f) TimescaleDB and PostgreSQL
- g) The port can be disabled by stopping the Windows service for the database.
- h) Microsoft SQL Server
- i) AVEVA PI System
- j) The communication between the field server and the SPARQL database is encrypted by default and the default port is 7200.
- k) The port can be configured during installation. The port cannot be changed after installation.
- l) An Internet connection is not needed when you run the cloud service on the same local network as the field server.
- m) Ports are not active if all devices are disabled.
- n) This communication path is supported in EcoStruxure Building Operation version 7.0.2 and later.

Information Technology System Planning Guide

EcoStruxure Building Management



SpaceLogic BACnet/IP device – Communication paths

Information Technology System Planning Guide

EcoStruxure Building Management

SpaceLogic BACnet/IP Device – Network Ports

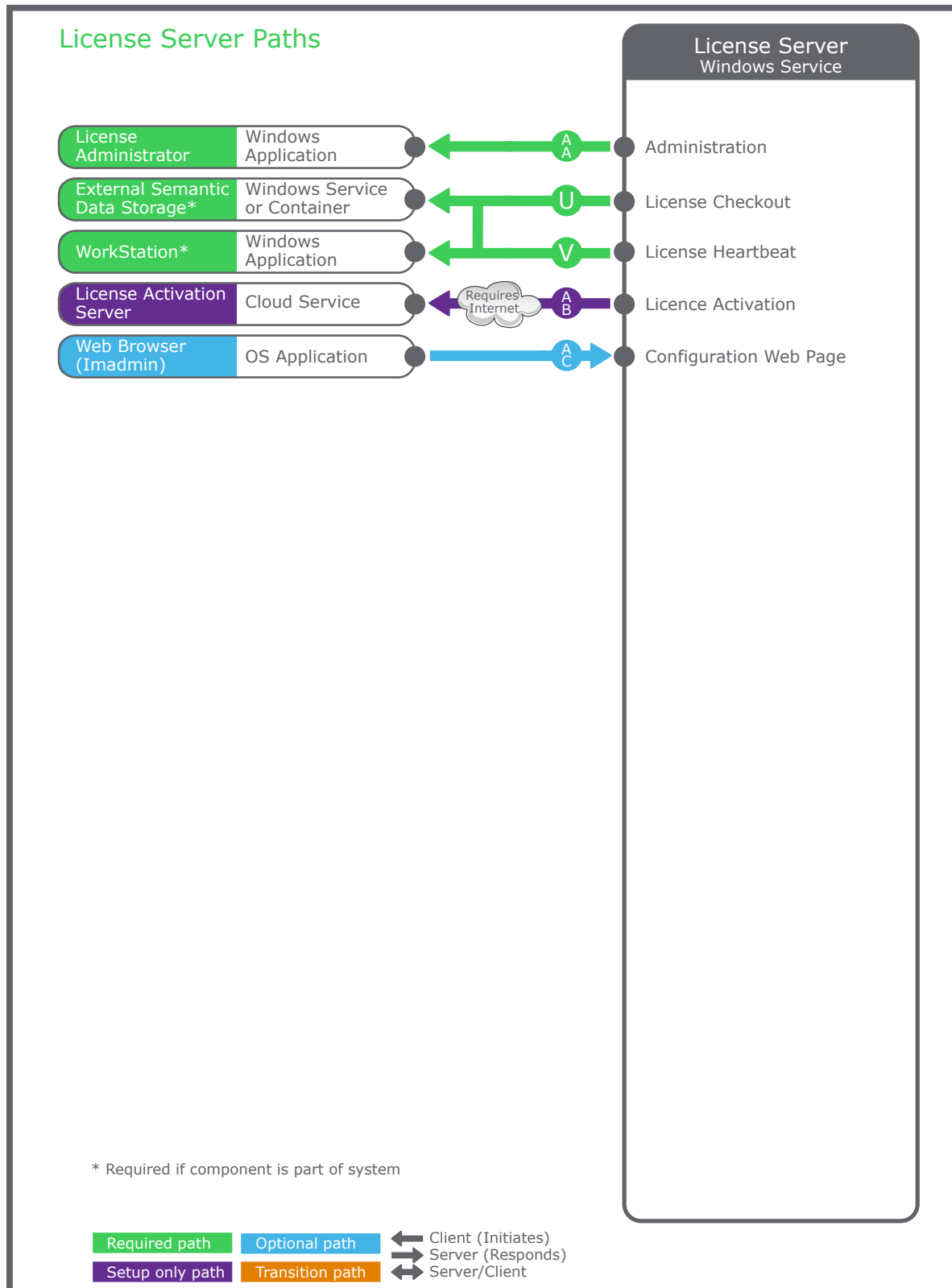
Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
D ^a	Time synchron.	IT (IPv4/IPv6)	NTP (Disabled)	123 (UDP)	-	Yes	Persistent	-	-
G (option 1)	BACnet integr.	BMS open protocol (IPv4/IPv6)	BACnet/IP (Enabled)	47808 / 33487 (UDP)	Yes	Yes	Persistent	-	-
G (option 2)	BACnet integr.	BMS open protocol (IPv4/IPv6)	WebSocket Secure (WSS) ^b (Disabled)	-	Yes	Yes	Persistent	-	-
Y	Client comm.	Bluetooth Low Energy	BACnet BLE/PPT	-	-	Yes	On demand	-	-
X	DHCPv4 or IPv6 SLAAC	IT (IPv4/IPv6)	DHCPv4 or IPv6 SLAAC (Enabled)	68 (UDP)	-	Yes	On demand	-	-
DE	Web services	IT (IPv4/IPv6)	HTTPS (Disabled)	443 (TCP)	Yes	Yes	On demand	-	-
DF	Certificate and key transfer	IT (IPv4/IPv6)	HTTPS (Disabled)	5000 (TCP)	Yes	Yes	Setup only	-	-
DQ ^a	DHCPv6	IT (IPv6)	DHCPv6 (Enabled)	546 (UDP)	-	Yes	On demand	-	-

a) This communication path is supported in EcoStruxure Building Operation version 7.0.3 and later.

b) WebSocket Secure (WSS) is used for BACnet Secure Connect (BACnet/SC) applications.

Information Technology System Planning Guide

EcoStruxure Building Management



License Server – Communication paths

Information Technology System Planning Guide

EcoStruxure Building Management

License Server – Network Ports

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
U	License checkout	Propriet. (IPv4/IPv6)	FLEXnet (Enabled)	27000-27009 (TCP)	Yes	-	Persistent	-	-
V	License heartbeat	Propriet. (IPv4/IPv6)	FLEXnet (Enabled)	Random (TCP) ^a	Yes	-	Persistent	-	-
AA	Administration	Propriet. (IPv4/IPv6)	FLEXnet (Enabled)	27000-27009 (TCP)	Yes	-	On demand	-	-
AB	License activation	Propriet. (IPv4)	HTTPS (Enabled)	443, 27000-27009 (TCP)	Yes	-	Setup only	Yes ^{b c}	-
AC (option 1)	Configuration	IT (IPv4)	HTTP (Enabled)	8888 ^d (TCP)	Yes ^e	-	On demand	- ^f	-
AC (option 2)	Configuration	IT (IPv4)	HTTPS (Disabled)	Not set (TCP)	Yes	Yes	On demand	- ^f	-

a) Flexera does not specify a port for the vendor daemon. If the port has not been specified, the port will be chosen at random by the operating system at runtime. It is completely random and depends upon what (non-restricted) ports are available at the time the operating system assigns it. This port may be configured manually to align with local policies and standard network management practices.

b) Optional file-based activation.

c) The destination address for the FlexNet Operations cloud server, <https://schneider-electric.flexnetoperations.com>, is required for firewall setup. TLS 1.2 is required on host OS.

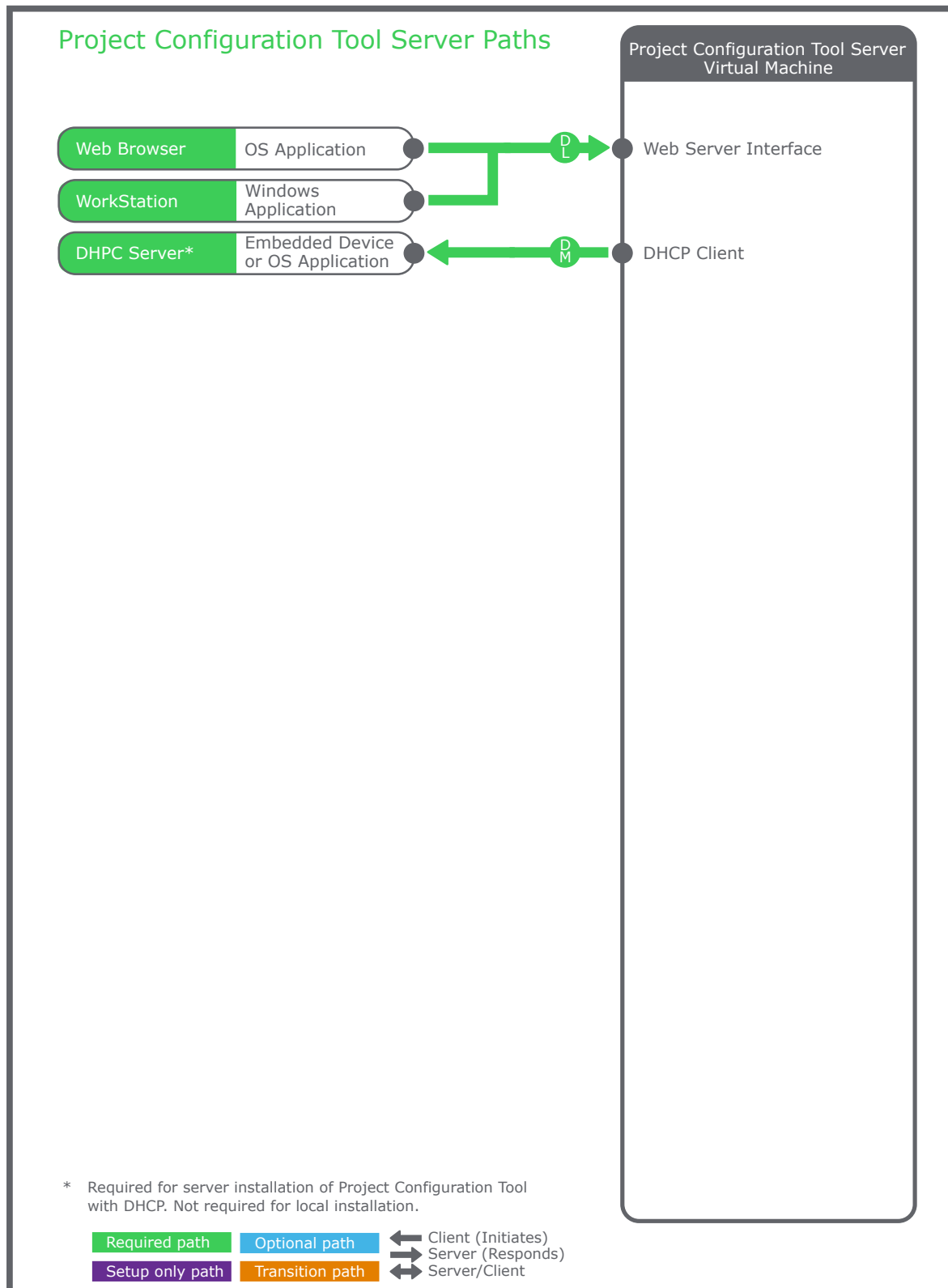
d) This is the port that a network scanner picks up when the Admin page starts up.

e) Can be redirected to HTTPS.

f) An Internet connection is not needed when you run the license server web application on the same computer as the licenser server.

Information Technology System Planning Guide

EcoStruxure Building Management



Project Configuration Tool (Version 2) server – Communication paths

Information Technology System Planning Guide

EcoStruxure Building Management

Project Configuration Tool (Version 2) Server – Network Ports

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
DL	Client to server comm.	IT (IPv4)	HTTPS (Config.)	443 (TCP)	No	Yes ^a	On demand	-	-
DM	DHCP ^b	IT (IPv4)	DHCP (Enabled)	68 (UDP)	No	Yes ^c	On demand	-	-

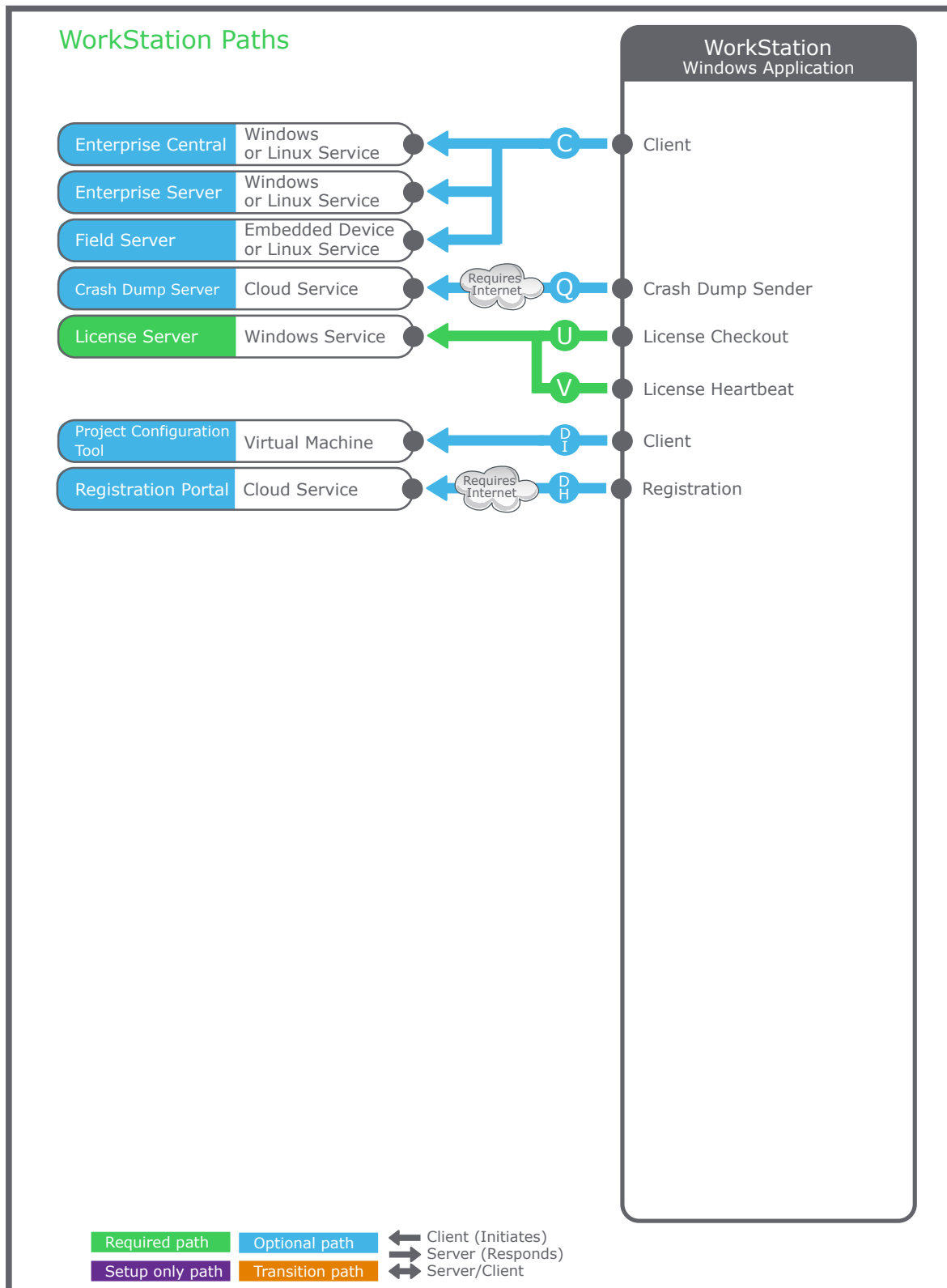
a) The virtual switch for external access to the virtual machine can be removed to make it work like a local installation of Project Configuration Tool.

b) This communication path applies only to a server installation, not a local installation of Project Configuration Tool. The virtual machine asks the DHCP server for an IP address to the virtual machine where Project Configuration Tool is running.

c) DHCP is disabled if the virtual switch for external access is removed.

Information Technology System Planning Guide

EcoStruxure Building Management



WorkStation – Communication paths

Information Technology System Planning Guide

EcoStruxure Building Management

WorkStation – Network Ports

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
C ^a (option 1)	Client to server comm.	IT (IPv4/IPv6)	HTTP (Config.)	80 (TCP)	Yes	Yes	On demand	-	-
C ^a (option 2)	Client to server comm.	IT (IPv4/IPv6)	HTTPS (Config.)	443 (TCP)	Yes	-	On demand	-	-
Q	Crash dumps	IT (IPv4)	HTTPS (Enabled)	443 (TCP)	No	Yes	On demand	Yes	-
U	License checkout	Propriet. (IPv4/IPv6)	FLEXnet (Enabled)	27000-27009 (TCP)	Yes	-	Persistent	-	-
V	License heartbeat	Propriet. (IPv4/IPv6)	FLEXnet (Enabled)	Random (TCP) ^b	Yes	-	Persistent	-	-
DI	Client to server comm.	IT (IPv4)	HTTPS (Config.)	443 (TCP)	No	Yes	On demand	-	-
DH	Registration	IT (IPv4)	HTTPS (Enabled)	443 (TCP)	No	No	On demand	Yes ^c	-

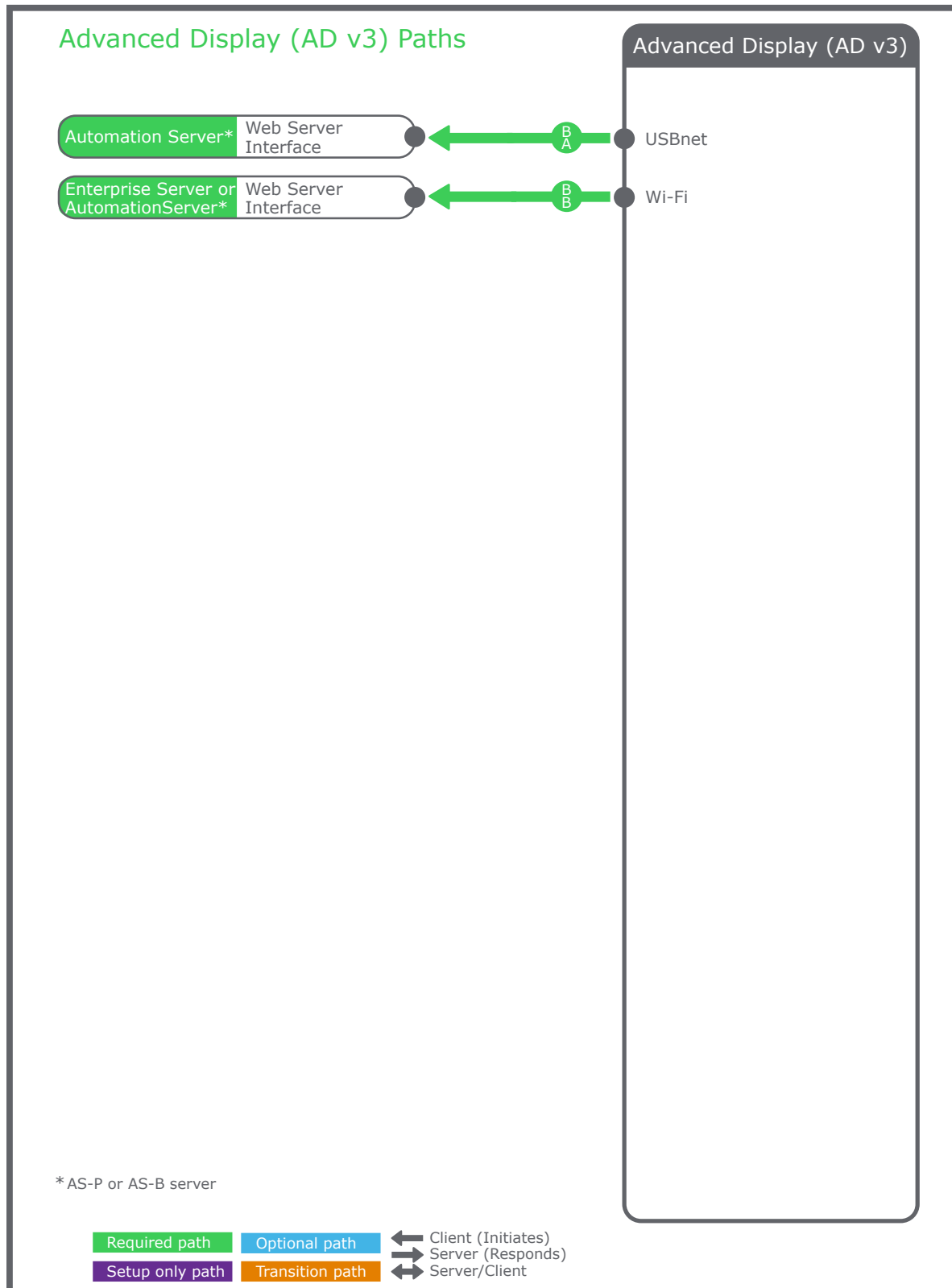
a) This communication path uses dynamic port assignment. The port assignment is controlled by the operating system (Windows). The allowable range for the port assignment is configurable from Windows. The default dynamic port range depends on the operating system. For the EcoStruxure Building Operation software supported Windows versions, the default port range is 49152 to 65535.

b) Flexera does not specify a port for the vendor daemon. If the port has not been specified, the port will be chosen at random by the operating system at runtime. It is completely random and depends upon what (non-restricted) ports are available at the time the operating system assigns it. This port may be configured manually to align with local policies and standard network management practices.

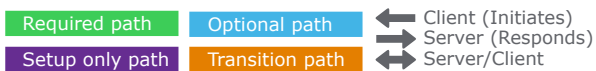
c) The link to the EcoStruxure Building Operation Registration portal, <https://registration.smartstruxure.schneider-electric.com/ebo>, is required for firewall configuration.

Information Technology System Planning Guide

EcoStruxure Building Management



* AS-P or AS-B server



Advanced Display (AD v3) – Communication paths

Information Technology System Planning Guide

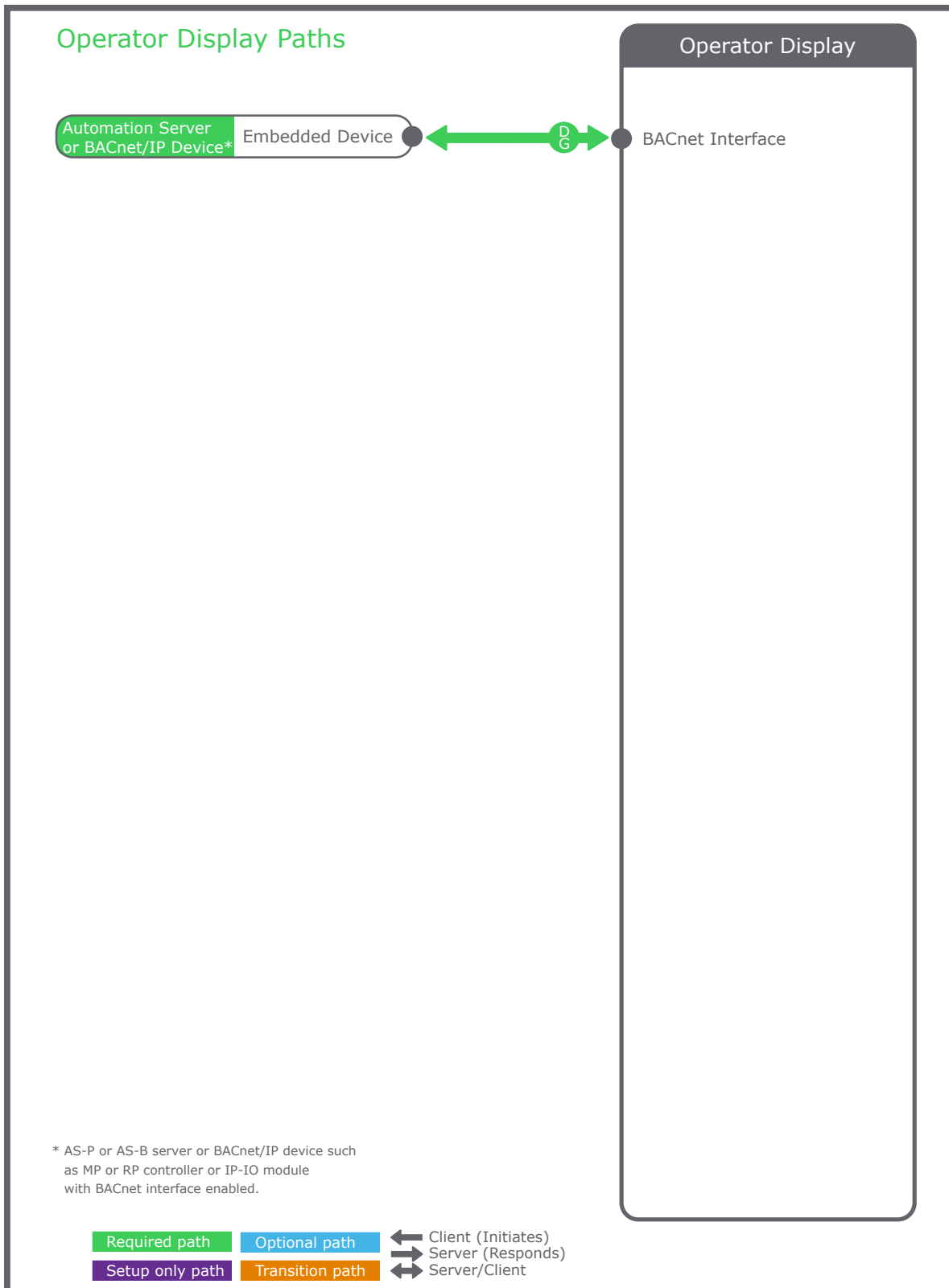
EcoStruxure Building Management

Advanced Display (AD v3) – Network Ports

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
BA	Data exchange	IT (IPv4 over USB)	HTTPS (Config.)	443 (TCP)	Yes	Yes	Persistent	-	-
BB	Data exchange	IT (IPv4)	HTTPS (Config.)	443 (TCP)	Yes	Yes	Persistent	-	-

Information Technology System Planning Guide

EcoStruxure Building Management



Operator Display – Communication paths

Information Technology System Planning Guide

EcoStruxure Building Management

Operator Display – Network Ports

Path	Function	Connection Type (IP Version)	Protocol (Default State)	Default Port (TCP or UDP)	Configurable Port	Can Be Disabled	Usage when Enabled	Internet Needed	Optional Settings
DG	BACnet integr.	BMS open protocol (IPv4)	BACnet/IP (Enabled)	47808 (UDP)	Yes	No	Persistent	No	-

Windows services

Windows Services

Application	Windows Service	Startup Type	Recovery	Log On As Default
Enterprise Central	Building Operation x.y Enterprise Central	Automatic	Run a Program	Local System
Enterprise Central ^a	Building Operation x.y Connect Agent	Automatic	Restart the service	Local System
Enterprise Central ^a	Building Operation x.y Enterprise Central GraphDB	Automatic	Restart the service	Local System
Enterprise Central ^a	Building Operation x.y Enterprise Central SamlAuthenticator	Automatic	Restart the service	Local System
Enterprise Central ^a	Building Operation x.y Enterprise Central CertAgent	Automatic	Restart the service	Local System
Enterprise Server	Building Operation x.y Enterprise Server	Automatic	Run a Program	Local System
Enterprise Server ^b	Building Operation x.y Connect Agent	Automatic	Restart the service	Local System
Enterprise Server ^b	Building Operation x.y Enterprise Server GraphDB	Automatic	Restart the service	Local System
Enterprise Server ^b	Building Operation x.y Enterprise Server SamlAuthenticator	Automatic	Restart the service	Local System
Enterprise Server ^b	Building Operation x.y Enterprise Server CertAgent	Automatic	Restart the service	Local System
Cloud connectivity ^c	Building Operation Cloud Certificate Agent	Automatic	Restart the service	Local System
Cloud connectivity ^c	Building Operation Cloud Agent	Automatic	Restart the service	Local System
Cloud connectivity ^c	Building Operation Update Agent	Automatic	Restart the service	Local System

Information Technology System Planning Guide

EcoStruxure Building Management

Continued

Application	Windows Service	Startup Type	Recovery	Log On As Default
License Administrator ^d	Building Operation x.y License Server	Automatic	Restart the service	Local System

- a) The Enterprise Central installation file includes the Connect Agent, the semantic graph database (GraphDB), software for SAML 2.0 authentication, and the CertAgent.
- b) The Enterprise Server installation file includes the Connect Agent, the semantic graph database (GraphDB), software for SAML 2.0 authentication, and the CertAgent.
- c) The Cloud Agent Software Administrator installs three agents: Cloud Certificate Agent, Cloud Agent, and Update Agent.
- d) The License Administrator installation file includes two components: License Administrator and License Server. You can select to install both components or one of them. Only the License Server has a Windows service.

Bandwidth requirements

As in all instances of planning, more is generally better. Although the current field servers are limited to 100 Mbps, a single installation may contain many field servers each with a significant number of field devices resulting in substantial data traffic. Insufficient bandwidth may affect the overall performance of the building.

EcoStruxure BMS LAN descriptions

Field servers, Enterprise Server, and Enterprise Central

The field servers include the AS-P-3, AS-P, and AS-B servers, Edge Server, and the FDP server. The AS-P-3, AS-P, and AS-B servers are hardware devices with embedded Linux operating systems. Edge Server is software only. The FDP server is software in a fire detection panel. Enterprise Server and Enterprise Central are Windows based software applications that are installed on a PC. These EcoStruxure BMS servers are multi-function IP addressable devices that can provide the following functions:

Server Functions

Function	AS-P-3, AS-P, and AS-B Servers	Edge Server	FDP Server	Enterprise Server	Enterprise Central
Server (for data exchange) – a server for open and proprietary protocols	Yes	Yes	Yes	Yes	Yes
Server (for clients) – a web server and server for application-based user interfaces	Yes	Yes	Yes	Yes	Yes

Router Functions

Function	AS-P-3, AS-P, and AS-B Servers	Edge Server	FDP Server	Enterprise Server	Enterprise Central
IP Networks – a router for LON IP, BACnet/IP, Modbus TCP, Web Services, proprietary networks	Yes	Yes ^a	Yes ^a	Yes	Yes ^b

Information Technology System Planning Guide

EcoStruxure Building Management

Continued

Function	AS-P-3, AS-P, and AS-B Servers	Edge Server	FDP Server	Enterprise Server	Enterprise Central
Private RS-485 Networks – a router for BACnet MS/TP, LON, Modbus RTU, proprietary networks	Yes	-	-	-	-
Private FT-10a Networks – a router for LON TP networks	Yes	-	-	Yes ^c	-

a) Edge Server and the FDP server do not support LON IP networks.

b) Enterprise Central includes only a router for Web Services.

c) With optional adapter

Gateway Functions

Function	AS-P-3, AS-P, and AS-B Servers	Edge Server	FDP Server	Enterprise Server	Enterprise Central
Gateway – a gateway for open and proprietary building automation protocols	Yes	Yes	Yes	Yes	-

Clients

The field servers, Enterprise Server, and Enterprise Central support the following clients:

- WorkStation: An application-based Microsoft Windows client.
- WebStation: A browser-based client.

The BACnet/IP devices support the following clients:

- Commission: A mobile application designed for local configuration, field deployment, and commissioning of BACnet/IP devices.

RP controllers support the following clients:

- Engage: A mobile application designed to enable control of room temperature, fan speed, lights, and blinds/shades directly from a smartphone.

Advanced Display

Advanced Display is a touch screen device that can be locked to an application such as the preinstalled web browser running WebStation. The preinstalled HMI Kiosk app prevents the user from closing the selected application or switching to another application. Advanced Display is connected to the EcoStruxure BMS using the USB ports on Advanced Display and an automation server. The preinstalled USBnet driver enables IP communication over USB.

Operator Display

Operator Display is a touch-screen Human Machine Interface (HMI) designed for local monitoring of SpaceLogic BACnet/IP devices and automation servers. Operator Display communicates over BACnet/IP open protocol with a direct connection to MP or RP controllers, IP-IO modules, AS-P-3, AS-P, or AS-B servers.

External log storage for historical data

External storage(s) can be used as an option for storing historical data from Enterprise Central, Enterprise Servers, and field servers.

Information Technology System Planning Guide

EcoStruxure Building Management

The historical data stored in the external log storage is available natively to viewers built into the EcoStruxure Building Operation clients.

External reporting tools can be used to access the external log storage and create reports based upon the stored historical data.

The EcoStruxure BMS servers support an external log storage solution based on the following databases:

- TimescaleDB with PostgreSQL
- Microsoft SQL server
- AVEVA PI System

External log storage based on TimescaleDB and PostgreSQL databases

The external log storage option for EcoStruxure BMS servers enables connectivity with the third party TimescaleDB time-series database, built on top of the PostgreSQL database. Ensure that the hardware and software requirements for TimescaleDB (www.timescale.com) and PostgreSQL (www.postgresql.org) are met. High-performance SSD storage is required and additional CPU/RAM capacity is required for larger EcoStruxure BMSs. As an example, at least 64 GB of RAM is recommended for systems with 100 EcoStruxure BMS servers.

External log storage based on Microsoft SQL Server database

The external log storage option for EcoStruxure BMS servers enables connectivity with the third party Microsoft SQL Server database. Ensure that the hardware and software requirements for Microsoft SQL Server (www.microsoft.com) are met. High-performance SSD storage is required and additional CPU/RAM capacity is required for larger EcoStruxure BMSs. As an example, at least 64 GB of RAM is recommended for systems with 100 EcoStruxure BMS servers.

External log storage based on AVEVA PI System

The external log storage option for EcoStruxure BMS servers enables connectivity with AVEVA PI System. Selected trend logs and the event log can be sent to AVEVA PI System directly without the need for intermediate storage or specialized PI System connectors. EcoStruxure BMS servers write data to PI System but can also read data back from PI System for viewing or reporting. Ensure that the hardware and software requirements for PI System (www.aveva.com) are met. High-performance SSD storage is required

and additional CPU/RAM capacity is required for larger EcoStruxure BMSs. As an example, at least 64 GB of RAM is recommended for systems with 100 EcoStruxure BMS servers.

External storage for semantic information

The EcoStruxure Building Operation software supports a database solution for external storage of semantic information.

The semantic information is a contextual representation of a building that follows the Brick Schema. It includes representation of building assets such as points, locations, and equipment.

The semantic information is configured in WorkStation, and the information is available in WorkStation and WebStation. The information is also available through EcoStruxure Web Services.

All EcoStruxure BMS servers can communicate with the external semantic data storage. The database solution is based on Ontotext's GraphDB™, a semantic graph database that supports external access through SPARQL and encrypted communication.

The EcoStruxure Building Operation software supports one semantic data storage per EcoStruxure BMS.

Enterprise Server and Enterprise Central for Windows:

- The database is included in the Enterprise Central and Enterprise Server installation packages. It is recommended to change the password for the admin account after installation.
- The database is running as a Windows service. It is recommended to stop the Windows service if semantic information is not used for the EcoStruxure BMS and the site.

Enterprise Server and Enterprise Central for Linux:

- The servers do not come with a prepackaged semantic graph database, but support the use of GraphDB from Ontotext to achieve semantic functionality. For more information on deployment and licensing, see the Ontotext website.
- The semantic graph database can also be installed in Docker using a script included in the Enterprise Central and Enterprise Server installation packages.

Information Technology System Planning Guide

EcoStruxure Building Management

Project Configuration Tool

Project Configuration Tool is an off-site engineering platform for the EcoStruxure BMS. The Project Configuration Tool simulates all functions of the Enterprise Central, Enterprise Server, and automation servers virtually before deployment.

The Project Configuration Tool sever provides an environment within which all virtual EcoStruxure BMS servers of the project can run while being engineered. The Project Configuration Tool provides a web browser based user interface for project management. WorkStation provides a full-featured user interface for configuration of EcoStruxure BMS servers.

Project Configuration Tool should only be deployed in private isolated networks and never be exposed directly to the Internet.

Project Configuration Tool is available for Windows and for Linux.

EcoStruxure Building Operation software OS requirements

To install and use the EcoStruxure Building Operation software, users must have the following credentials:

- All software requires the installing user to have administrative privileges on the PC onto which the installation is to take place.

- Enterprise Central, Enterprise Server, and License Server are installed as services and require a user with administrative privileges to start and stop the services.
- The PC running the Enterprise Central, Enterprise Server service or License Server service needs to be running under an administrative user's account.
- Use of the Software Administrator or License Administrator requires that the user have administrative privileges.
- Operation of WorkStation and Device Administrator requires normal user privileges.

The PC running License Server and License Administrator needs TLS 1.2 to be enabled during license activation.

EcoStruxure BMS requirements

WorkStation includes Graphics Editor, Script Editor, Function Block Editor, and WorkPlace Tech Editor.

WorkStation

Hardware and software requirements	Supported versions
Processor	Minimum: Intel Core i5 @ 2.0 GHz, or another x86-64 processor with comparable performance Recommended: Intel Core i5 @ 3.0 GHz or better
Memory	Minimum: 4 GB Recommended: 8 GB or higher
Storage capacity	Minimum: 20 GB
Operating systems	Microsoft Windows 11 Microsoft Windows Server 2016 Microsoft Windows Server 2019 Microsoft Windows Server 2022 Microsoft Windows Server 2025

Information Technology System Planning Guide

EcoStruxure Building Management

Continued

Hardware and software requirements	Supported versions
Visio versions (WorkPlace Tech Editor)	Microsoft Office Visio 2016 (32-bit and 64-bit) Microsoft Office Visio 2019 (32-bit and 64-bit) Microsoft Office Visio 2021 (32-bit and 64-bit) Microsoft Office Visio Plan 2 (32-bit and 64-bit) Microsoft Office Visio 2024 (32-bit and 64-bit)
Required additional software	Microsoft .NET Framework 4.7.2 and later
<p>The following Microsoft Windows 11 editions are supported: Pro and Enterprise.</p> <p>The following Microsoft Windows Server 2016 editions are supported: Datacenter, Standard, and Essentials.</p> <p>The following Microsoft Windows Server 2019 editions are supported: Datacenter, Standard, and Essentials.</p>	<p>The following Microsoft Windows Server 2022 editions are supported: Datacenter, Standard, and Essentials.</p> <p>The following Microsoft Windows Server 2025 editions are supported: Datacenter, Standard, and Essentials.</p>

WebStation

Software requirements (web browsers)	Supported versions
Minimum web browser versions required	Google Chrome 119 and later Mozilla Firefox 119 and later Microsoft Edge 119 and later Safari 14 and later
Recommended web browser versions	Google Chrome latest Mozilla Firefox latest Microsoft Edge latest Safari latest

Enterprise Central

Hardware and software requirements	Supported versions
Processor	Minimum: Intel Core i5 @ 3.0 GHz, or another x86-64 processor with comparable performance Recommended: Intel Core i5 @ 4.0 GHz or better
Memory	Minimum: 8 GB Recommended: 16 GB or higher
Storage capacity	Minimum: 1 TB Recommended: 4 TB

Information Technology System Planning Guide

EcoStruxure Building Management

Continued

Hardware and software requirements	Supported versions
Storage device	<p>Recommended: Enterprise Solid State Drive (SSD)</p> <p>An Enterprise SSD is recommended to maintain the necessary speed and stability. The database and the binaries should both be installed on the Enterprise SSD.</p>
Operating systems – Enterprise Central for Windows	<p>Microsoft Windows 11</p> <p>Microsoft Windows Server 2016</p> <p>Microsoft Windows Server 2019</p> <p>Microsoft Windows Server 2022</p> <p>Microsoft Windows Server 2025</p>
Operating systems – Enterprise Central for Linux	<p>OCI compliant container runtime on Linux x86-64</p> <p>Quality assurance testing has been performed on, and support is provided with, Ubuntu 22.04 and 24.04 with Docker Engine. Other deployment scenarios have not been tested by Schneider Electric. Product Support Services may require that potential issues can be reproduced in tested and supported environment for full support.</p>
Required additional software – Enterprise Central for Windows	<p>Microsoft .NET Framework 4.7.2 and later</p> <p>The Microsoft .NET Framework is required by Software Administrator.</p>
External log storage PostgreSQL option	<p>Supported versions of PostgreSQL (www.postgresql.org) with matching version of TimescaleDB extension (www.timescale.com).</p> <p>Note: To use compression for trend data, TimescaleDB 2.11 or later is required.</p> <p>Quality assurance testing has been performed by Schneider Electric with TimescaleDB and PostgreSQL installed natively in Windows 11, Windows Server 2016, 2019, 2022, and 2025. Other deployment scenarios have not been tested by Schneider Electric.</p>
External log storage Microsoft SQL option	<p>Microsoft SQL Server versions under full support by Microsoft (www.microsoft.com).</p> <p>The following Microsoft SQL Server editions are supported: Enterprise, Standard, and Express.</p>
External log storage AVEVA PI System option	<p>PI Web API 2021 SP3 and database compatible with that version</p> <p>Quality assurance testing has been performed by Schneider Electric with PI Web API 2021 SP3, and database compatible with that version, installed on Windows Server 2019. Other deployment scenarios have not been tested by Schneider Electric.</p>

Processor power, memory, and storage capacity should be scaled upwards to accommodate targeted system size as impacted by the total quantity of Enterprise Servers, automation servers, and expected historical archiving. Enterprise Central is tested on a server with an 8-core 3.6 GHz processor, a 16 GB of memory, and an SSD storage capacity of 4 TB.

The following Microsoft Windows 11 editions are supported: Pro and Enterprise.

The following Microsoft Windows Server 2016 editions are supported: Datacenter, Standard, and Essentials.

The following Microsoft Windows Server 2019 editions are supported: Datacenter, Standard, and Essentials.

The following Microsoft Windows Server 2022 editions are supported: Datacenter, Standard, and Essentials.

The following Microsoft Windows Server 2025 editions are supported: Datacenter, Standard, and Essentials.

Information Technology System Planning Guide

EcoStruxure Building Management

Enterprise Server

Hardware and software requirements	Supported versions
Processor	<p>Minimum: Intel Core i5 @ 2.0 GHz, or another x86-64 processor with comparable performance</p> <p>Recommended: Intel Core i5 @ 3.0 GHz or better</p>
Memory	<p>Minimum: 8 GB</p> <p>Recommended: 16 GB or higher</p>
Storage capacity	<p>Minimum: 100 GB</p> <p>Recommended: 1 TB</p>
Storage device	<p>Recommended: Enterprise Solid State Drive (SSD)</p> <p>An Enterprise SSD is recommended to maintain the necessary speed and stability. The database and the binaries should both be installed on the Enterprise SSD.</p>
Operating systems – Enterprise Server for Windows	<p>Microsoft Windows 11</p> <p>Microsoft Windows Server 2016</p> <p>Microsoft Windows Server 2019</p> <p>Microsoft Windows Server 2022</p> <p>Microsoft Windows Server 2025</p>
Operating systems – Enterprise Server for Linux	<p>OCI compliant container runtime on Linux x86-64</p> <p>Quality assurance testing has been performed on, and support is provided with, Ubuntu 22.04 and 24.04 with Docker Engine. Other deployment scenarios have not been tested by Schneider Electric. Product Support Services may require that potential issues can be reproduced in tested and supported environment for full support.</p>
Required additional software – Enterprise Server for Windows	<p>Microsoft .NET Framework 4.7.2 and later</p> <p>The Microsoft .NET Framework is required by Software Administrator.</p>
External log storage PostgreSQL option	<p>Supported versions of PostgreSQL (www.postgresql.org) with matching version of TimescaleDB extension (www.timescale.com).</p> <p>Note: To use compression for trend data, TimescaleDB 2.11 or later is required.</p> <p>Quality assurance testing has been performed by Schneider Electric with TimescaleDB and PostgreSQL installed natively in Windows 11, Windows Server 2016, 2019, 2022, and 2025. Other deployment scenarios have not been tested by Schneider Electric.</p>
External log storage Microsoft SQL option	<p>Microsoft SQL Server versions under full support by Microsoft (www.microsoft.com).</p> <p>The following Microsoft SQL Server editions are supported: Enterprise, Standard, and Express.</p>
External log storage AVEVA PI System option	<p>PI Web API 2021 SP3 and database compatible with that version</p> <p>Quality assurance testing has been performed by Schneider Electric with PI Web API 2021 SP3, and database compatible with that version, installed on Windows Server 2019. Other deployment scenarios have not been tested by Schneider Electric.</p>

Information Technology System Planning Guide

EcoStruxure Building Management

Processor power, memory, and storage capacity should be scaled upwards to accommodate targeted system size as impacted by the total quantity of Enterprise Servers, automation servers, and expected historical archiving. Enterprise Central is tested on a server with an 8-core 3.6 GHz processor, a 16 GB of memory, and an SSD storage capacity of 4 TB.

The following Microsoft Windows 11 editions are supported: Pro and Enterprise.

The following Microsoft Windows Server 2016 editions are supported: Datacenter, Standard, and Essentials.

The following Microsoft Windows Server 2019 editions are supported: Datacenter, Standard, and Essentials.

The following Microsoft Windows Server 2022 editions are supported: Datacenter, Standard, and Essentials.

The following Microsoft Windows Server 2025 editions are supported: Datacenter, Standard, and Essentials.

Field Server (Automation Server) – Edge Server

Hardware and software requirements	Supported versions
Processor frequency	1 GHz
Processor architecture	AMD64 or x86-64
Processor cores	2
Memory	1 GB
Storage capacity	4 GB
Operating systems	OCI compliant container runtime on Linux x86-64 Quality assurance testing has been performed on, and support is provided with, Ubuntu 22.04 and 24.04 with Docker Engine. Other deployment scenarios have not been tested by Schneider Electric. Product Support Services may require that potential issues can be reproduced in tested and supported environment for full support.
External log storage PostgreSQL option	Supported versions of PostgreSQL (www.postgresql.org) with matching version of TimescaleDB extension (www.timescale.com). Note: To use compression for trend data, TimescaleDB 2.11 or later is required. Quality assurance testing has been performed by Schneider Electric with TimescaleDB and PostgreSQL installed natively in Windows 11, Windows Server 2016, 2019, 2022, and 2025. Other deployment scenarios have not been tested by Schneider Electric.
External log storage Microsoft SQL option	Microsoft SQL Server versions under full support by Microsoft (www.microsoft.com). The following Microsoft SQL Server editions are supported: Enterprise, Standard, and Express.
External log storage AVEVA PI System option	PI Web API 2021 SP3 and database compatible with that version Quality assurance testing has been performed by Schneider Electric with PI Web API 2021 SP3, and database compatible with that version, installed on Windows Server 2019. Other deployment scenarios have not been tested by Schneider Electric.

Information Technology System Planning Guide

EcoStruxure Building Management

Project Configuration Tool (Version 2)

Hardware and software requirements	Supported versions
Server	
Processor	Intel Core i7-7820X @ 3.60 GHz or higher (at least 4 CPU cores)
Memory	2 GB plus 170 MB x number of running EcoStruxure BMS servers Minimum: 16 GB The Virtual Machine is configured by default with 8 GB.
Storage capacity - Project Configuration Tool for Windows	Minimum: 50 GB and 5 GB in Windows Temp folder Recommended: 1 TB or higher
Storage capacity - Project Configuration Tool for Linux	Minimum: 50 GB Recommended: 1 TB or higher
Required BIOS configuration	Intel VT-x or AMD-V virtualization support enabled
Operating systems – Project Configuration Tool for Windows	Microsoft Windows 11 Microsoft Windows Server 2019 Microsoft Windows Server 2022 Microsoft Windows Server 2025
Operating systems – Project Configuration Tool for Linux	Ubuntu 22.04 LTS, Desktop and Server Ubuntu 24.04 LTS, Desktop and Server
Hyper-V - Project Configuration Tool for Windows	Hyper-V must be enabled
Required additional software - Project Configuration Tool for Windows	Microsoft .NET Framework 4.7.2 and later WorkStation version 5.0.3.5001 and later ^a a) For WorkStation version 3.2.4 and 4.0.5, it is required to install WorkStation version 5.0.3.5001 (or later) in parallel. For WorkStation version 5.0.3, it is sufficient to install version 5.0.3.5001. For WorkStation versions later than 5.0.3, version 5.0.3.5001 is not needed.

Processor power, memory, and storage capacity should be scaled upwards to accommodate targeted system size as impacted by the total quantity of EcoStruxure BMS projects. Project Configuration Tool is tested on a server with an 8-core 3.6 GHz processor, 32 GB of memory, and storage capacity of 1 TB.

Installing Project Configuration Tool and the virtual machine require approximately 50 GB of storage space on the installation drive. Project Configuration Tool for Windows also requires 5 GB on the Windows Temp folder, which is typically located on the C drive (C:).

The following Microsoft Windows 11 editions are supported: Pro and Enterprise.

The following Microsoft Windows Server 2019 editions are supported: Datacenter, Standard, and Essentials.

The following Microsoft Windows Server 2022 editions are supported: Datacenter, Standard, and Essentials.

The following Microsoft Windows Server 2025 editions are supported: Datacenter, Standard, and Essentials.

Information Technology System Planning Guide

EcoStruxure Building Management

Commission Mobile Application

Hardware and software requirements	Supported versions
Hardware	Android phones and tablets Apple iPhones and iPads PCs, laptops, and tablets running Microsoft Windows 11
Operating systems	Android 8.1 (Oreo) and later Apple iOS 11.2 and later Microsoft Windows 11
MP controller communication	EcoStruxure Building Operation version 2.0.1 and later
RP-C communication	EcoStruxure Building Operation version 3.0.1 and later
Configuration Menu support	EcoStruxure Building Operation version 3.0.1 and later
Bluetooth connectivity	EcoStruxure Building Operation version 3.0.2 and later
RP controller expansion module support	EcoStruxure Building Operation version 3.1.1 and later

Engage

Hardware and software requirements	Supported versions
Hardware	Android phones Apple iPhones
Operating systems	Android 5.0 (Lollipop) and later Apple iOS 11 and later
RP-C communication	EcoStruxure Building Operation version 3.1.2 and later

Information Technology System Planning Guide

EcoStruxure Building Management