# Information Technology System Planning Guide

## 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.

## SmartStruxure Solution Cybersecurity Features

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

### Identification and Authentication

All human users are uniquely identified

- Admin logon password management (SBO v1.3)

Imported User Accounts are disabled by default (SBO v1.7)

Certificate functionality for - HTTPS connections

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

Password policies can be enforced (SBO v1.6)

- Days until password expires
- Minimum number of characters
- Minimum number of lowercase characters
- Minimum number of numeric characters
- Minimum number of special characters

- Number of consecutive unique passwords before reuse
- No more than three repeating identical characters

SSH connection control (SBO v1.6)

- Disabled after failed logon attempts
- Time-out for admin free connection re-enabling
- Rate limiting to protect against brute force attacks

Password policies are secure by default:

- Factory settings (SBO v1.7):
  - Days until password expires: Enabled: 90 days
  - Minimum number of characters: 8
  - Minimum number of lowercase characters: 1
  - Minimum number of numeric characters: 1
  - Minimum number of special characters: 1
  - Number of consecutive unique passwords before reuse: 6
  - Do now allow more than three repeating identical characters: Enabled
- Force Admin password change (SBO v1.7)
- Password blacklist (non editable) (SBO v1.7):
  - 123
  - admin
  - Admin
  - admin1
  - Admin1
  - Admin1!
  - password
  - Password
  - PaSsWoRd
  - Password1!

Active Directory/Windows Logon support is available for Workstation only (SBO v1.2).

Enterprise Server Run-As-Service selectable user account (SBO v1.5).

## Authorization

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

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

Role-based access control (permissions)

- Object level security

## Confidentiality

Encrypted transmission of data

- HTTPS using TLS 1.0 (SBO v1.2)
- EWS Encrypted Logon (SBO v1.5)
- Disable use of MD5 configuration option (SBO v1.6)
- SNMPv3 support, SNMPv1 and v2 removed (SBO v1.5)
- SmartStruxure server device: SSHv2, SSHv1 removed (SBO v1.5)
- Redirect web clients to HTTPS configuration option (SBO v1.6)
- SMTPS secure email notification support (SBO v1.8)

Password data is obscured from view

Passwords are stored and transmitted securely

CA certificate central log storage (SBO v1.6)

Basic secure key management

Basic data at rest protection (SBO v1.4)

## Integrity

Auto logoff (SBO v1.5)

Audit log with system-wide synchronized timestamps

Activity logs provide non-repudiation

SmartStruxure server device Boot Loader U-Boot disabled (SBO v1.5)

SmartStruxure server device Boot restricted to a single boot location (SBO v1.5)

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

Basic protection of audit information

Basic protection against program and data at rest modification

Basic protection for input validation

Basic protection for secure and effective error messages

### Restricted data flow

Basic capabilities for network segmentation

Basic options for enabling/disabling ports

- Disable HTTP (HTTPS only) configuration option (SBO v1.5)

World-writable programs or scripts removed (SBO v1.6)

### Timely response to events

Audit log access

SIEM Support: Remote system logging option (SBO v1.6)

Web server access logging configuration option (SBO v1.6)

### Resource availability

System backup, recovery and reconstitution

Access to network and security configuration settings

## 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 SmartStruxure solution 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.

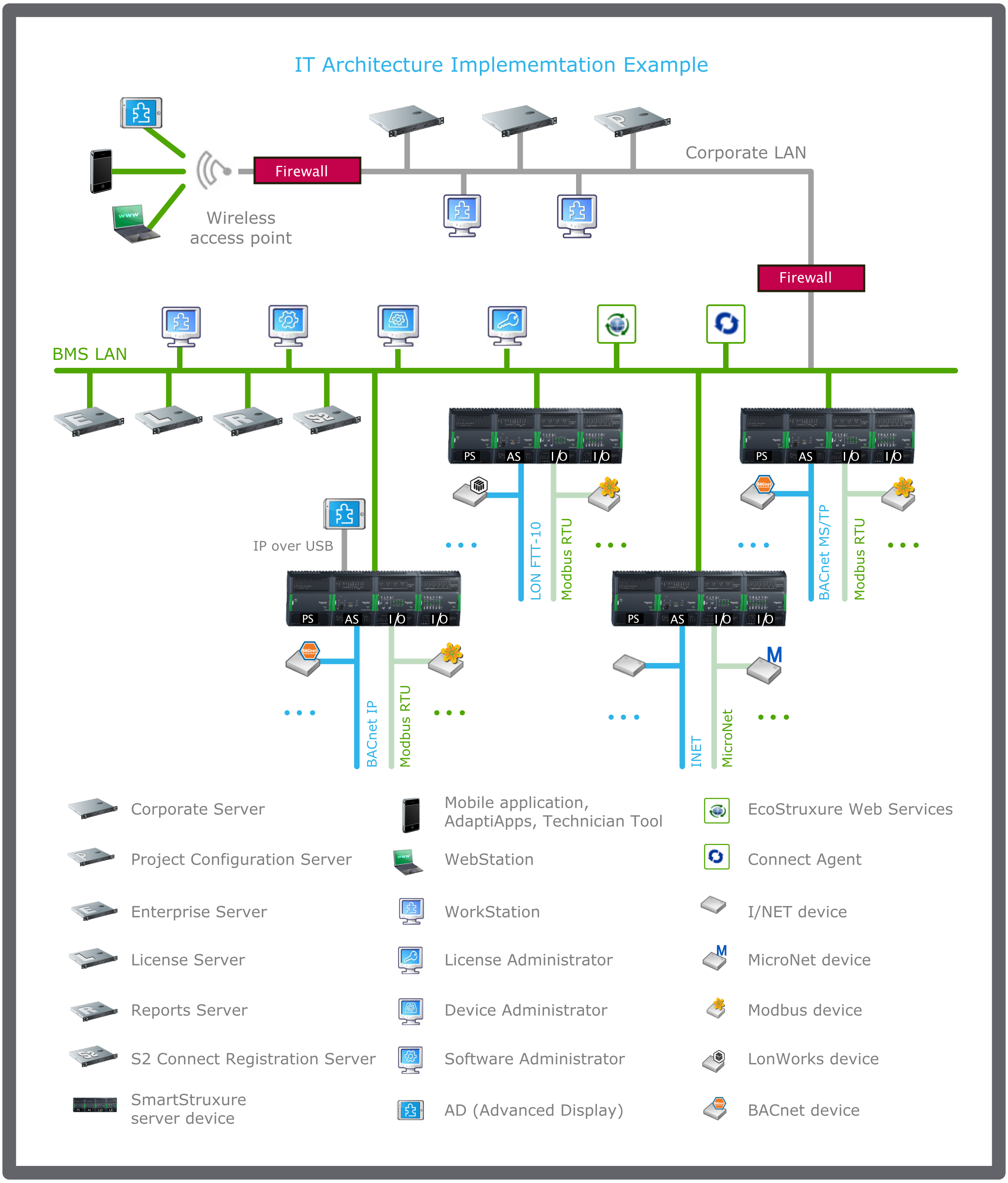

Figure: IT architecture implementation example

On the Corporate LAN side, there may be many StruxureWare 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:

- StruxureWare Building Operation WorkStations
- StruxureWare Building Operation servers (Enterprise Server, License Server, and Reports Server)
- SmartStruxure server devices (Automation Server and AS-P): These servers use TCP/IP for their main communications and additionally support a wide array of open and proprietary serial bus protocols.

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.
- SSH: This protocol is used for StruxureWare Building Operation upgrade operations. The need to have this port open depends on network use policy.
- SNMPv3: This protocol is used to monitor servers within a SmartStruxure solution using standard SNMP Managers supporting SNMP version 3 authentication.
- SMTPS: This protocol is used to send secure email messages.

## Open port on segregation firewall

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

Table: Communication paths

| **Communi-cation Path** | **Function** | **A-Side** | ↔ | **B-Side** | **Internet Access** |
|---|---|---|---|---|---|
| A | Server to server communications | Enterprise Server, SmartStruxure server device | ↔ | Enterprise Server, SmartStruxure server device | Not recommended |
| B | Administrative tool to server communications | Device Administrator | ↔ | SmartStruxure server device | No |
| B | Administrative tool to server communications | License Server | ↔ | License Administrator, Enterprise Server | Optional |

*Continued*

| Communi-cation Path | Function | A-Side | ↔ | B-Side | Internet Access |
|---|---|---|---|---|---|
| B | Administrative tool to server communications | Software Administrator | ↔ | Enterprise Server | No |
| C | Server to BMS open protocol device | Enterprise Server, SmartStruxure server device | ↔ | BACnet Device | Not recommended |
| D | Server to BMS open protocol device | Enterprise Server, SmartStruxure server device | ↔ | LON Device | No |
| E | Server to BMS open protocol device | Enterprise Server, SmartStruxure server device | ↔ | Modbus Device | No |
| F | Server to BMS proprietary system interface | Enterprise Server running INET IO Service | ↔ | I/NET System | No |
| G | Server to BMS proprietary system interface | Enterprise Server | ↔ | MicroNet System | No |
| H | Client to server communications | WorkStation, Reports Server | ↔ | Enterprise Server, SmartStruxure server device | Optional |
| I | Client to server communications | WebStation | ↔ | Enterprise Server, SmartStruxure server device | Optional |
| J | Mobile client to server communications | Technician Tool Mobile App, AdaptiApps | ↔ | Enterprise Server, SmartStruxure server device | Not recommended |
| K | System to system web service communications | Enterprise Server, SmartStruxure server device | ↔ | EcoStruxure Web Services based client or server | Optional[a] |
| L | System to system web service communications | Enterprise Server, SmartStruxure server device | ↔ | Generic web service based server | Optional[a] |
| M | System to Schneider Electric cloud service | License Server | ↔ | License Activation Server | Required if Network licenses are used. Local licenses do not required Internet |
| N | System to Schneider Electric cloud service | Connect Agent | ↔ | S2 Connect Registration server | Required for online registration from Workstation |
| O | Client to Server communications | WorkStation | ↔ | License Server | Optional[a] |

*Continued*

| **Communi-cation Path** | **Function** | **A-Side** | ↔ | **B-Side** | **Internet Access** |
|---|---|---|---|---|---|
| P | Mobile app to software activation servers | SmartXKiosk, SmartX AD-Link | ↔ | Software activation servers | Required for mobile app activation, one-time communication |
| Q | Mobile app to software download servers | Technician Tool Mobile App, AdaptiApps Shell App | ↔ | App Store, Google Play, AdaptiApps portal | Optional for mobile app upgrade |
| R | Mobile app to software deployment server | AdaptiApps Shell App | ↔ | AdaptiApps deployment server | Required when deployment is done from the cloud. Deployment on premises is available as an option. |
| S | Network Service | DHCP Server | ↔ | Enterprise Server, SmartStruxure server device | Optional |
| T | Network Service | DNS Server | ↔ | Enterprise Server, SmartStruxure server device | Optional |
| U | Network Service | SNMP Manager | ↔ | Enterprise Server, SmartStruxure server device | Not recommended |
| V | Network Service | SMTP Server | ↔ | Enterprise Server, SmartStruxure server device | Optional |
| X | Network Service | NTP Server | ↔ | Enterprise Server, SmartStruxure server device | Optional |

a) Not recommended over insecure channel.

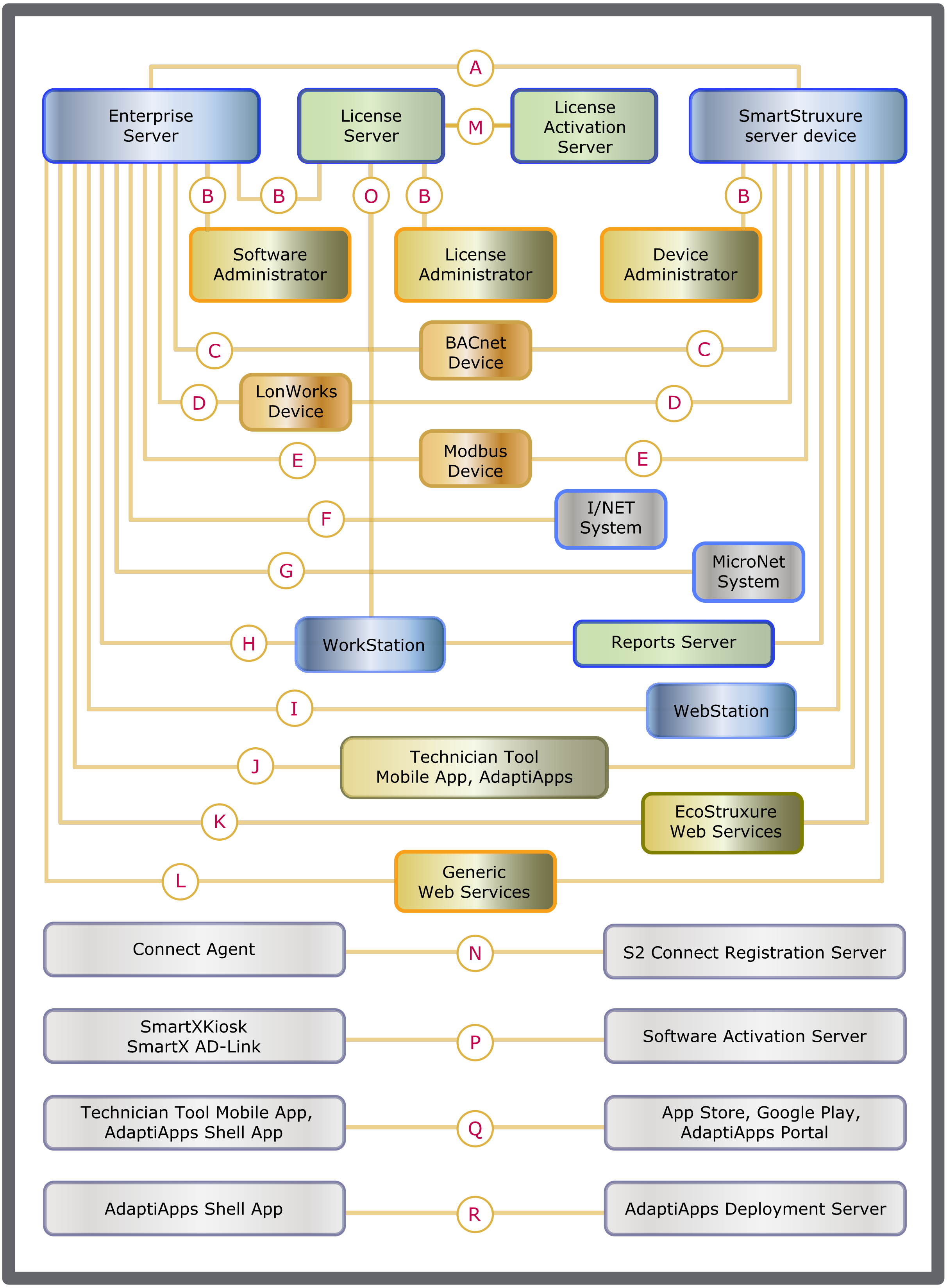

Figure: Communication paths

Table: Network ports

| Function | Protocol (Default State) | Default Port (TCP/UDP) | Configurable Port | Communi- cation Paths | Optional Settings |
|---|---|---|---|---|---|
| IT Communication Protocols | HTTP<br>(Disabled) | 80<br>(TCP) | Yes | A[a], H[a], I, J, O[a] | Redirect all WebStation connections to HTTPS |
| | HTTP<br>(Unconfigured) | 80<br>(TCP) | Yes | K, L | – |
| | HTTPS<br>(Enabled) | 443<br>(TCP) | Yes | A[a], H[a], I, J, K, L, M, O[a], P, Q | For SBO: Disable MD5 hash algorithm |
| | SSH<br>(Enabled) | 22<br>(TCP) | – | B, M, N | – |
| | MQTT<br>(Enabled) | 1883<br>(TCP) | – | R | – |
| Proprietary Communications | CSP<br>(Enabled) | 4444<br>(TCP) | – | A[a], H[a], I, O[a] | – |
| | FLEXnet Publisher Licensing<br>(Enabled) | Random (TCP)[b] | Yes | O[a] | – |
| | License Server<br>(Enabled) | 27000-27009<br>(TCP) | – | B, O[a] | – |
| | License Administrator<br>(Enabled) | 8888[c]<br>(TCP) | – | B | – |
| BMS Open Protocol Device Interface | BACnet/IP<br>(Unconfigured) | 47808/33487<br>(UDP) | Yes | C | – |
| | LonWorks IP<br>(Unconfigured) | 1628<br>(UDP) | – | D | – |
| | Modbus TCP<br>(Unconfigured) | 502<br>(TCP) | – | E | – |
| | I/NET<br>(Unconfigured) | User set from 49152 to 65535. Default to 50069 for unencrypted communication and to 49152 for encrypted<br>(UDP) | – | F | – |
| | MicroNet<br>(Unconfigured) | 7001<br>(TCP) | – | G | – |

*Continued*

| Function | Protocol (Default State) | Default Port (TCP/UDP) | Configurable Port | Communi-cation Paths | Optional Settings |
|---|---|---|---|---|---|
| | DHCP (Enabled) | 68 (UDP) | – | S | – |
| | DNS (Enabled) | 53 (TCP/UDP) | – | T | – |
| | SNMPv3 (Enabled) | 161/162 (UDP) | – | U | – |
| | SMTP (Enabled) | 25 (TCP) | – | V | – |
| | SMTPS (Enabled) | 587 (TCP) | Yes | V | TLS (Default) or SSL |
| | NTP (Enabled) | 123 (UDP) | – | X | – |

a) This communication path uses dynamic port assignment. The port assignment is controlled by the operating system (Windows or Linux). The allowable range for the port assignment is configurable only from Windows. The default dynamic port range depends on the operating system. For SmartStruxure server devices (Linux), the default port range is 32768 to 61000. For the Building Operation 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) This is the port that a network scanner picks up when the Admin page starts up.

Table: Software Activation Servers

| Americas | China | Asia, Africa, Europe and all other regions |
|---|---|---|
| gslb.secb2b.com | china-gslb.secb2b.com.cn | gslb.secb2b.com |
| us-prod-klm.secb2b.com | china-klm.secb2b.com.cn | eu-prod-klm.secb2b.com |
| us-elm.secb2b.com | china-elm.secb2b.com.cn | eu-elm.secb2b.com |

Table: Windows Services

| Application | Windows Service | Startup Type | Recovery | Log On As Default |
|---|---|---|---|---|
| Enterprise Server | Building Operation x.y Enterprise Server | Automatic | Run a Program | Local System |
| Enterprise Server[a] | Building Operation x.y Connect Agent | Automatic | Restart the service | Local System |
| License Administrator[b] | Building Operation x.y License Server | Automatic | Restart the service | Local System |
| Project Configuration Tool | Project Configuration Tool Modules Service | Automatic | Restart the service | Local System |

*Continued*

| Application | Windows Service | Startup Type | Recovery | Log On As Default |
|---|---|---|---|---|
| WebReports | Building Operation x.y WebReports Agent | Automatic | Restart the service | Local System |

a) The Enterprise Server installation file includes the Connect Agent.

b) 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 SmartStruxure server devices are limited to 100 Mbps, a single installation may contain many SmartStruxure server devices each with a significant number of field devices resulting in substantial data traffic. Insufficient bandwidth may affect the overall performance of the building.

## SmartStruxure solution LAN descriptions

### SmartStruxure server devices and Enterprise Server

The SmartStruxure server devices are hardware devices with embedded Linux operating systems and the Enterprise Server is a software application that is installed on a PC. These SmartStruxure servers are multi-function IP addressable devices that can provide the following functions:

Table: Server functions

| Function | SmartStruxure server devices | Enterprise Server |
|---|---|---|
| **Server** (for data exchange) – a server for open and proprietary protocols | Yes | Yes |
| **Server** (for clients) – a web server and server for application-based user interfaces | Yes | Yes |

Table: Router functions

| Function | SmartStruxure server devices | Enterprise Server |
|---|---|---|
| **IP Networks** – a router for LON IP, BACnet/IP, Modbus TCP, Web Services, Proprietary networks | Yes | Yes |
| **Private RS-485 Networks** – a router for BACnet MS/TP, LON, Modbus RTU, Proprietary networks | Yes | No |
| **Private FT-10a Networks** – a router for LON TP networks | Yes | Yes[a] |

a) With optional adaptor

Table: Gateway functions

| Function | SmartStruxure server devices | Enterprise Server |
|---|---|---|
| **Gateway** – a gateway for open and proprietary building automation protocols | Yes | Yes |

### Clients

The SmartStruxure server devices and the Enterprise Server support the following clients:

- WorkStation: An application-based Microsoft Windows client.
- WebStation: A browser-based client.
- Technician Tool Mobile App: A mobile application client.
- AdaptiApps: A mobile application design environment that creates custom applications for iPad, Android tablet, Microsoft Windows, and Mac OS Platforms.

### AD

AD is a touch screen device on which you can run the AdaptiApps or the preinstalled Technician Tool Mobile App. The preinstalled SmartXKiosk app prevents the user from closing AdaptiApps or Technician Tool Mobile App, or switching to another application. AD is connected to the SmartStruxure system using either the wireless network or the USB ports on AD and a SmartStruxure server device. The preinstalled SmartX AD-Link app enables IP communication over USB.

### Reports Server

The Reports Server is used to gather data from the Building Management System and generate reports. The Reports Server requires the following Microsoft applications:

- ASP.NET
- Internet Information Services (IIS)
- SQL Server
- SQL Server Reporting Services

For more information on supported versions, see StruxureWare Building Operation requirements.

### StruxureWare Building Operation Software OS user requirements

To install and use the StruxureWare 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 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 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, Device Administrator, and WebReports requires normal user privileges.

## StruxureWare Building Operation requirements

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

Table: WorkStation

| Software requirements | Supported versions |
|---|---|
| Operating systems | Microsoft Windows 7 (32-bit)<br>Microsoft Windows 7 (64-bit)<br>Microsoft Windows 8.1 (32-bit)<br>Microsoft Windows 8.1 (64-bit)<br>Microsoft Windows 10 (64-bit)<br>Microsoft Windows Server 2008 R2 (64-bit)<br>Microsoft Windows Server 2012 (64-bit)<br>Microsoft Windows Server 2012 R2 (64-bit) |
| Visio versions (WorkPlace Tech Editor) | Microsoft Office Visio 2010 SP1 (32-bit)<br>Microsoft Office Visio 2007 SP2<br>Microsoft Office Visio 2003* |
| Required additional software | Microsoft .NET Framework 4.5 or 4.6<br>Microsoft .NET Framework 3.5 SP1 (WorkPlace Tech Editor) |

* Upgrade is recommended

The following Microsoft Windows 7 editions are supported: Professional, Enterprise, and Ultimate.

The following Microsoft Windows 8.1 editions are supported: Pro, Pro N, Enterprise, and Enterprise N.

The following Microsoft Windows 10 editions are supported: Pro and Enterprise.

The following Microsoft Windows Server 2008 R2 editions are supported: Standard, Web, Enterprise, Datacenter, and Itanium.

The following Microsoft Windows Server 2012 and Microsoft Windows Server 2012 R2 editions are supported: Datacenter, Standard, Essentials, and Foundation.

Table: WebStation

| Software requirements | Supported versions |
|---|---|
| Web browsers | Microsoft Internet Explorer 11<br>Mozilla Firefox<br>Google Chrome |

Table: Enterprise Server and Project Configuration Server

| Software requirements | Supported versions |
|---|---|
| Operating systems | Microsoft Windows 7 (32-bit)<br>Microsoft Windows 7 (64-bit)<br>Microsoft Windows 8.1 (32-bit)<br>Microsoft Windows 8.1 (64-bit)<br>Microsoft Windows 10 (64-bit)<br>Microsoft Windows Server 2008 R2 (64-bit)<br>Microsoft Windows Server 2012 (64-bit)<br>Microsoft Windows Server 2012 R2 (64-bit) |
| Required additional software | Microsoft .NET Framework 4.5 or 4.6 |

The following Microsoft Windows 7 editions are supported: Professional, Enterprise, and Ultimate.

The following Microsoft Windows 8.1 editions are supported: Pro, Pro N, Enterprise, and Enterprise N.

The following Microsoft Windows 10 editions are supported: Pro and Enterprise.

The following Microsoft Windows Server 2008 R2 editions are supported: Standard, Web, Enterprise, Datacenter, and Itanium.

The following Microsoft Windows Server 2012 and Microsoft Windows Server 2012 R2 editions are supported: Datacenter, Standard, Essentials, and Foundation.

Table: Reports Server

| Software requirements | Supported versions |
|---|---|
| Operating systems | Microsoft Windows 7 (32-bit), English<br>Microsoft Windows 7 (64-bit), English<br>Microsoft Windows 8.1 (32-bit), English<br>Microsoft Windows 8.1 (64-bit), English<br>Microsoft Windows 10 (64-bit), English<br>Microsoft Windows Server 2008 R2 (64-bit), English<br>Microsoft Windows Server 2012 (64-bit), English<br>Microsoft Windows Server 2012 R2 (64-bit), English |
| SQL versions | Microsoft SQL Server 2008 R2 (64-bit) SP2 or SP3, English<br>Microsoft SQL Server 2012 (64 bit)*, English |
| Required additional software | Microsoft .NET Framework 4.5 or 4.6 |

* Microsoft SQL Server 2012 SP1, SP2 or SP3 is required if the operating system Windows Server 2012 R2 is used

The following Microsoft Windows 7 edition is supported: English edition of Professional.

The following Microsoft Windows 8.1 editions are supported: English editions of Pro and Enterprise.

The following Microsoft Windows 10 editions are supported: English editions of Pro and Enterprise.

The following Microsoft Windows Server 2008 R2 editions are supported: English editions of Standard, Web, Enterprise, Datacenter, and Itanium.

The following Microsoft Windows Server 2012 edition is supported: English edition of Standard.

The following Microsoft Windows Server 2012 R2 editions are supported: English editions of Datacenter and Standard.

The following Microsoft SQL Server 2008 R2 and Microsoft SQL Server 2012 editions are supported: English editions of Standard and Express with Advanced Services.

For more information on software requirements for installing SQL Server 2008 R2, see https://msdn.microsoft.com/en-us/library/ms143506(v=sql.105).

For more information on software requirements for installing SQL Server 2012, see https://msdn.microsoft.com/en-us/library/ms143506(v=sql.110).aspx/html.

Table: WebReports

| **Software requirements** | **Supported versions** |
|---|---|
| Web browsers | Microsoft Internet Explorer 9 (32-bit)<br>Microsoft Internet Explorer 11<br>Mozilla Firefox<br>Google Chrome |

Table: Technician Tool Mobile App

| **Hardware and software requirements** | **Supported versions** |
|---|---|
| Hardware | Minimum: iPad 2<br>Minimum: iPhone 4<br>Android Phones<br>Android Tablets |
| Operating systems | iOS 7.1 to 10.x<br>Android 4.4 to 4.4.4 (KitKat)<br>Android 4.4W to 4.4W.2 (KitKat)<br>Android 5.0 to 5.1 (Lollipop)<br>Android 6.0 (Marshmallow) |
| SmartStruxure servers | Minimum: 1.6.1<br>Minimum: 1.7.1 for graphics and SmartX AD-Link support |

Table: AdaptiApps

| **Hardware and software requirements** | **Supported versions** |
|---|---|
| Hardware | iPads<br>iPhones<br>Android Phones<br>Android Tablets |

*Continued*

| **Hardware and software requirements** | **Supported versions** |
|---|---|
| Operating systems | iOS 7.x to 10.x<br>Android 4.4 to 4.4.4 (KitKat)<br>Android 4.4W to 4.4W.2 (KitKat)<br>Android 5.0 to 5.1 (Lollipop)<br>Android 6.0 (Marshmallow)<br>Microsoft Windows 7.x, Windows 8.x, or Windows 10<br>Mac OS 10.x |
| SmartStruxure servers | Minimum: 1.6.1<br>Minimum: 1.7.1 for SmartX AD-Link support |