SIEMENS

Data Sheet

Security Manager

Building X

Security Manager / Building Access Add-Ons are cloud-based offerings within Building X that extend access control systems with cloud services.

- Essential Identity and Access Management
- Standard Identity and Access Management
- Security Self Service Portal
- Credential Management
- Security Alarm and Task Management
- Security Monitoring and Insights Dashboards
- Print and Encode Security Cards
- Manage Cloud-based Access Control
- Connect ACC-AP Door Controller
- Connect On-Prem Access Control Systems
- PACS SDK
- Data Setup
- Activity Log

URL

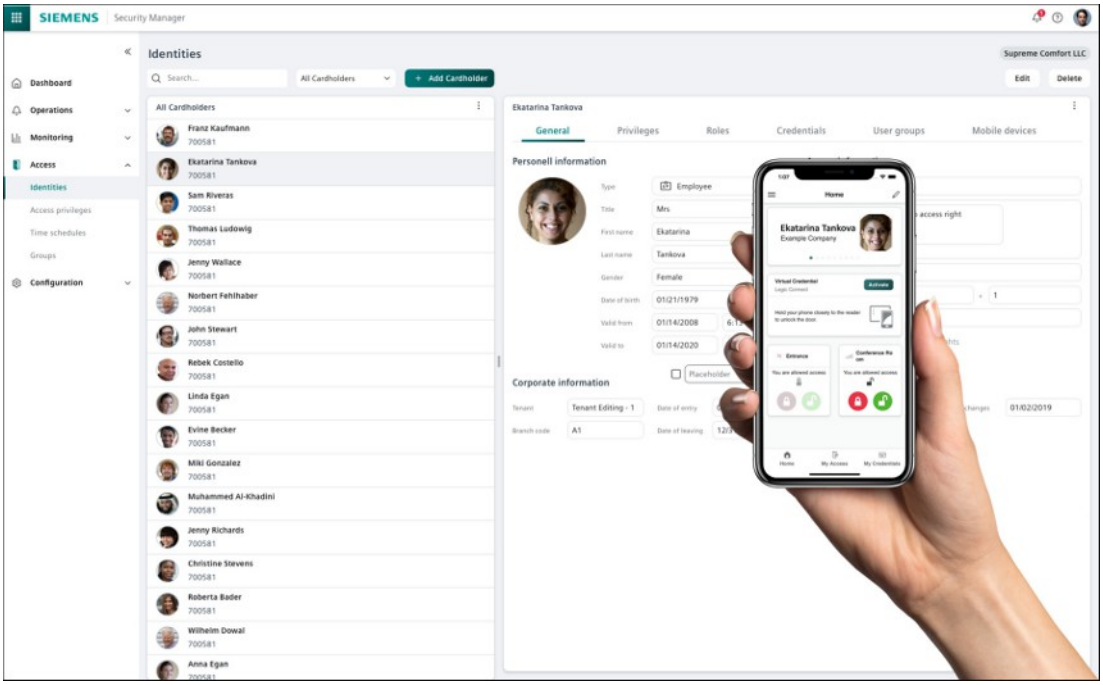
securitymanager.siemens.com

Functions

Essential Identity and Access Management

Manage identities based on the fixed basic identity type (incl. general identity information), assign access privileges and credentials, manage and assign security groups, manage mobile devices.

Standard Identity and Access Management



Manage newly created or imported identities:

- Manage identities based on the generic standard identity type
- Manage identities across multiple connected PACS systems
- Manage mobile devices
- Assign credentials
- Assign access privileges
- Manage and assign security groups
- Import of identities via a CSV file
- Define a unique identifier for identities (e.g., employee ID, email)

Security Self Service Portal

- Deploy predefined access approval workflow to enable employees' self-service. Configuration of approver and the visibility in the self-service per access group.
- Enable LCB and DSC trained engineers to design self-service and customizable workflows (incl. the design of wizard forms via an UI editor) for physical identity and access management. PDF files can be used in custom workflows. The files can be uploaded and displayed in the request creation, 'My Requests' and 'My Approvals'.
- Configure delegations for approvers and requesters: For each delegation a duration can be configured, an end date is optional. Delegates will be informed via email when a delegation is created or updated.
- Self-service users can easily upload a new profile picture and see their photo reflected across the Building X Access app, Identity Management, and on printed access cards.

Membership Review for Security Groups

Once a user is configured as the owner of a Security Group, membership reviews can be started in self-services. Every review is logged to the Activity Log and My Requests.

Credential Management

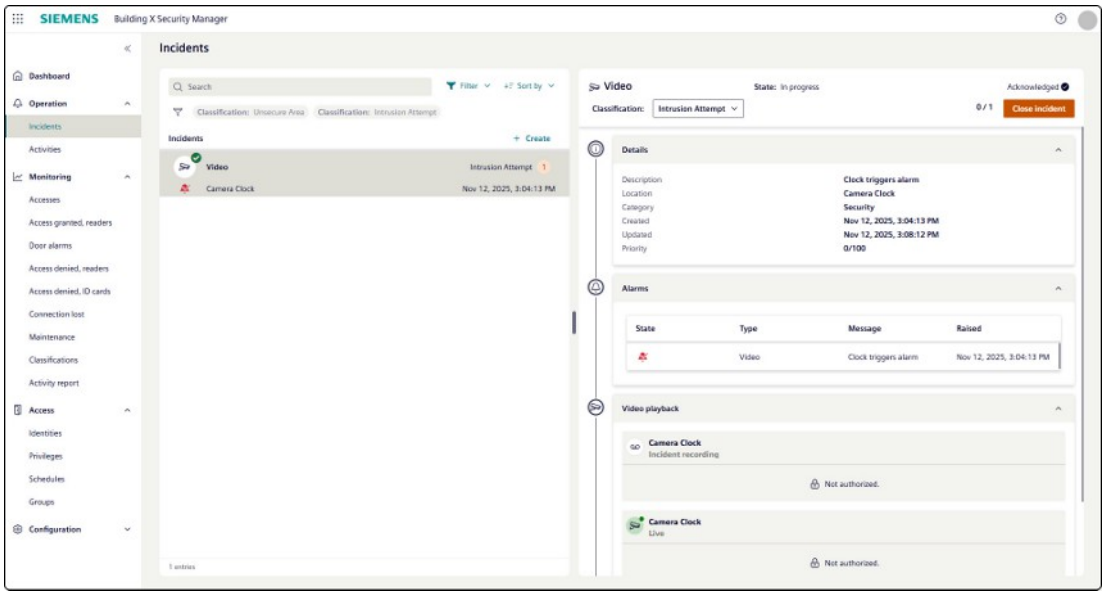
Service Engineer can configure the following:

- How many physical credentials can be assigned to one identity
- How many physical credentials can be activated at the same time

Security Manager can enable / disable virtual ID and virtual credentials:

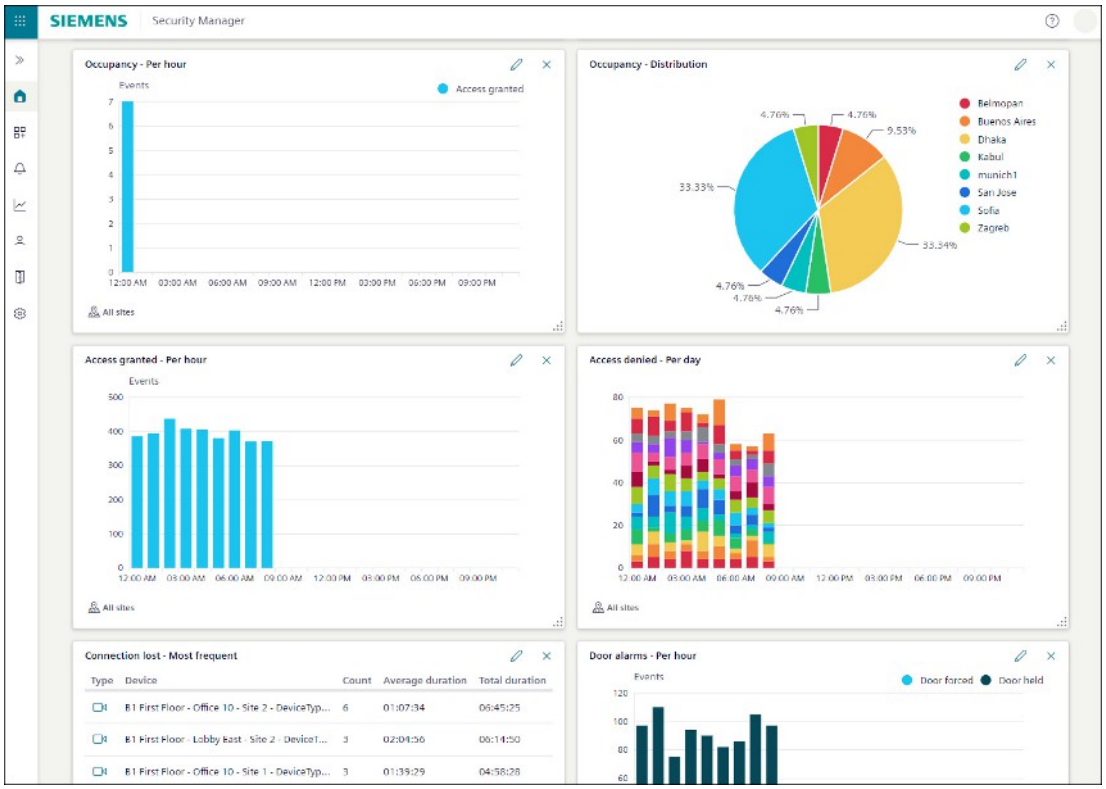
- With the flag „Enable virtual ID card in Building X Access app” the virtual ID card (identity badge) can be enabled or disabled for a specific identity. If it is enabled, the Building X Access app will show the virtual ID card as well as all available digital keys to the user. If it is disabled, the virtual ID card and all digital keys will be hidden, and doors cannot be accessed.

Security Alarm and Task Management



- Provide “out-of-the-box” standard operating procedures (SOPs) to resolve security tasks.
- Combine alarms that occur at the same location into a single security task.
- Alert mechanism via notification email

Security Monitoring and Insights Dashboards

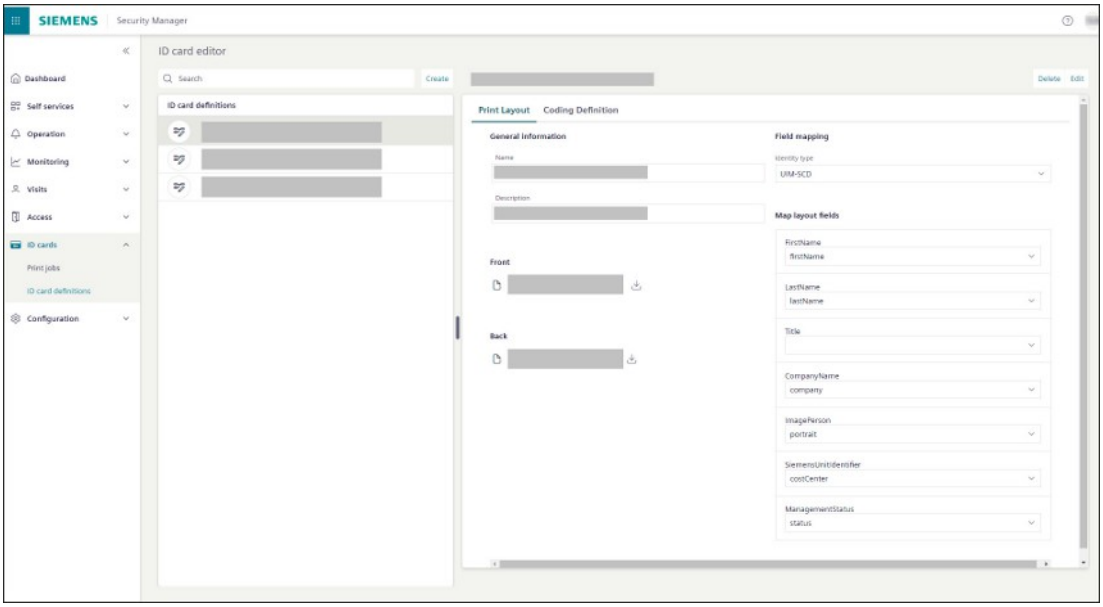


Get actionable insights based on security data:

- Visualize unique access events per building/site
- Measure room or building utilization based on the number of "access-granted" events
- Identify maintenance candidates or utilization outliers as indicators for malfunctions

- Displays system health status for readers connected to an Edge Controller and connected cameras
- Automated reports for mobile credentials & access events by region and department
- Sharing of custom dashboards
- Configure scheduled reports

Print and encode Cards



Print and encode cards for cloud-based access control with door controller (ACC-AP):

- Predefined card layouts can be selected by a commissioning engineer.
- Encoding definitions can be configured by a commissioning engineer.
- Trigger the print job via a workflow.
- Virtual SAM Card support: Encode physical cards without having a Physical Secure Access Module (SAM) for storing the keys.

Manage Cloud-based Access Control

Manage ACC-AP door controllers in Building X Security Manager. Manage smart locks from the SALTO XS+ system family. Manage access privileges, time schedules and doors. Set SALTO cloud-based locks to office mode.

Note: When used in combination with SALTO locks the following limits apply:

- Each privilege can now be assigned to up to 100 SALTO cloud-based locks.
- Each identity can hold up to 5 privileges, allowing access to up to 500 locks.
- Each privilege includes one time schedule. (Note: Adding more time schedules per privilege will reduce the maximum number of assignable privileges per identity.)
- On request, the limit can be extended to 20 privileges per identity, enabling access to up to 2,000 SALTO cloud-based locks.

Connect ACC-AP Door Controller

Connect up to 10 doors to an ACC-AP door controller via Building X Devices.

Connect On-Prem Access Control Systems

Connect to up to 5 SiPass and SIPORT systems. Connect 3rd Party PACS via the PACS SDK. Exported profile images from SiPass and SIPORT systems can be manually imported via the Connection Manager.

Note: Sync Agent 2.x cannot be installed on Servers where another Siemens Building Connect Agent is already installed.

PACS SDK

Use the PACS SDK to enable the integration of 3rd party access control systems.

Data Setup

Enrich data points coming from the cloud-based access control with ACC-AP door controllers or from SiPass/SIPORT systems via Building X Data Setup.

Activity Log

The Activity Log provides verifiable documentation of audit-relevant actions, capturing both user-initiated and system-driven changes.

Currently tracked activities include:

- User actions within the Point vertical (e.g., modifying point values)
- User actions within the User vertical (e.g., adding users, assigning groups)
- Full activity logs from Security Manager
- Full activity logs from Visitor Manager

User Management

Provides role-based access control. The Customer is activating the subscription in the Building X Accounts application. Users and role assignments are managed within Security Manager (Left navigation pane in category: Access, menu item: Identities).

Data Hosting and Data Usage

Hosts and processes personal and non-personal data in data centers located in Europe. For information regarding processing of personal data and locations Customer may refer to the Data Privacy Terms.

Subscription

The subscription plan depends on the agreement between Customer and Siemens.

1) Standard Subscription Plan if the customer purchases the subscription via the Siemens online store

<table>
<tr><th colspan="9">Security Manager / Building Access Add-Ons</th></tr>
<tr><th></th><th>Physical Identity & Access Management (PIAM)</th><th>Security Self Service Portal</th><th>Security Monitoring and Insights Dashboards</th><th>Security Alarm & Task Management</th><th>Security Card Lifecycle Management</th><th>Building Access - Essential</th><th>Connectivity – Physical Access Control Systems (PACS)</th><th>Connectivity – Cloud-based Access Control</th></tr>
<tr><td>Precondition</td><td colspan="5">The following subscriptions must be active:
● Connectivity – Physical Access Control Systems (PACS)
Or the following subscriptions must be active:
● Connectivity – Cloud-based Access Control and Building Access - Essential</td><td>One of the following subscriptions must be active:
● Connectivity – Physical Access Control Systems (PACS)
● Connectivity – Cloud-based Access Control</td><td colspan="2">-</td></tr>
<tr><td rowspan="2">Functions</td><td colspan="8">User management
Activity Log</td></tr>
<tr><td>Standard Identity and access management</td><td>Security Self Service Portal
Membership review for Security Groups</td><td>Security Monitoring and Insights Dashboards</td><td>Security Alarm and Task Management</td><td>Print and Encode Security Cards</td><td>Essential Identity and access management
Manage Cloud-based Access Control</td><td>Connect On-Prem Access Control Systems
PACS SDK</td><td>Connect ACC-AP door controller
Data Setup</td></tr>
<tr><td>Subscription metric</td><td colspan="8">per 1 door per year
The subscription plan can be purchased in packages of 1 door</td></tr>
<tr><td>Subscription term</td><td colspan="8">Annually, auto-renewal</td></tr>
<tr><td>Billing term</td><td colspan="8">Annually, payment in advance</td></tr>
</table>

Security Manager / Building Access Add-Ons								
	Physical Identity & Access Management (PIAM)	**Security Self Service Portal**	**Security Monitoring and Insights Dashboards**	**Security Alarm & Task Management**	**Security Card Lifecycle Management**	**Building Access - Essential**	**Connectivity – Physical Access Control Systems (PACS)**	**Connectivity – Cloud-based Access Control**
Upscale	Effective immediately, pro-rated billing							
Downscale / Cancellation	Effective with end of subscription term							
Connected Devices	To be purchased separately							
Permitted Users	Up to 10,000; Extended Use							

The Security Manager / Building Access Add-Ons subscription plan is the regular, scalable Offering for this Cloud Service. The subscription term is twelve (12) months with automatic renewal; the Cloud Service fee is paid in advance. The subscription plan can be upscaled at any time and Cloud Service fees for upscales are calculated on a pro-rated basis. The Customer can also scale down the Cloud Service effective with the end of the current subscription term. The subscription fee will be adjusted for the upcoming billing term. The Cloud Service can be cancelled any time, effective with the end of the current subscription term.

Customer may purchase required Connected Devices separately.

Extended Use entitles Customer to authorize its Affiliates and third parties to access and use the Cloud Services in accordance with the rights set out in the Terms and Conditions.

2) Custom Subscription Plan

Any subscriptions that are not purchased via a Siemens online store are Custom Subscription Plans. Under a Custom Subscription Plan the details regarding functions, subscription metric, term, billing, up- and downscaling, Connected Devices as well as Permitted Users are set out in the agreement between the Customer and Siemens.

For custom uses cases, such as a very large number of doors and identity per site (e.g., more than 10,000 identities and/or 1,000 doors), Customer may contact its sales representative for custom subscription plan.

Prerequisites

Supported Connected Devices

The Cloud Service is currently compatible with commercially available Connected Devices. Connected Devices enable the Cloud Service to exchange data with the technical building infrastructure. A description of the available Connected Devices is provided below.

	List of Supported Connected Devices
SIEMENS: SiPass	SiPass with Sync Agent 2.x: SiPass software product is running on Windows computer hardware. The supported software version is SiPass MP 2.95 (HF11) or higher. SiPass includes multiple software applications collectively referenced herein as Software to supply building data to this Cloud Service. The following card readers are supported: ● Autec: XMP-TMC2150, XMP-TMC2160, XMP-TMC2170, XMP-TMC2180, XMP-TMC2357, XMP-TMC2367, XMP-TMC2457-UP, XMP-TMC3050, XMP-TMC3060, XMP-TMC3070, XMP-TMC3080. ● Elatec: Secustos SQ80, Secustos SQ80 K, Secustos SQ80 Legic, Secustos SQ80 K Legic, Secustos MU20 LEGIC, Secustos MU20 K LEGIC ● Acre: AR10S-MF, AR40S-MF, AR20M-MF, AR50M-MF For details on compatibility with the virtual credential feature, please refer to the Security Manager / Mobile Access data sheet (www.siemens.com/buildingx/data-sheet/security-manager-mobile-access).

	List of Supported Connected Devices
SIEMENS: SIPORT	SIPORT with Sync Agent 2.x: SIPORT software product is running on Windows computer hardware. The supported software version is SIPORT V3.5.0.127 or higher and SIPORT 3.4.1.321 or higher. SIPORT includes multiple software applications collectively referenced herein as Software to supply building data to this Cloud Service. The following card readers are supported: ● Autec: XMP-TMC2150, XMP-TMC2160, XMP-TMC2170, XMP-TMC2180, XMP-TMC2357, XMP-TMC2367, XMP-TMC2457-UP, XMP-TMC3050, XMP-TMC3060, XMP-TMC3070, XMP-TMC3080. For details on compatibility with the virtual credential feature, please refer to the Security Manager / Mobile Access data sheet (www.siemens.com/buildingx/data-sheet/security-manager-mobile-access).
SALTO Nebula Electronic lock	Neo Cylinder, Neoxx padlock, XS4 Original+, XS4 One and XS4 One S (only models that support HSE), XS4 Mini, DBolt. **Restriction**: Only locks without keypads are supported, as Security Manager does not yet provide PIN functionality
SALTO Nebula Gateways	IQ3, IQ3 Mini
SIEMENS: ACC-AP	ACC-AP with firmware V6.5.X or higher, based on the ACC-AP hardware, to supply access door data to this Cloud Service. The following card readers are supported: ● Autec: XMP-TMC2150, XMP-TMC2160, XMP-TMC2170, XMP-TMC2180, XMP-TMC2357, XMP-TMC2367, XMP-TMC2457-UP, XMP-TMC3050, XMP-TMC3060, XMP-TMC3070, XMP-TMC3080. ● Elatec: Secustos SQ80, Secustos SQ80 K, Secustos SQ80 Legic, Secustos SQ80 K Legic, Secustos MU20 LEGIC, Secustos MU20 K LEGIC ● Acre: AR10S-MF, AR40S-MF, AR20M-MF, AR50M-MF For details on compatibility with the virtual credential feature, please refer to the Security Manager / Mobile Access data sheet (www.siemens.com/buildingx/data-sheet/security-manager-mobile-access).

To use the Cloud Service, a Connected Device must be installed on site, fully operational and connected to the Internet. The Customer is responsible for the provision of the Connected Device on site and all associated costs for the provision of the Cloud Service in accordance with the associated documentation for the Connected Device.

Supported Third-Party Software Connectivity

The Cloud Service is currently compatible with commercially available Third-Party Software. Third-Party Software Connectivity enable the Cloud Service to exchange data with Third-Party Software. A description of the available Third-Party Software connectivity is provided below.

	List of Supported Third-Party Software
Software Specific connectors	● SDK for 3rd party PACS ● Mobile App SDK

The customer is responsible for the Third-Party Software at the site and all associated costs for the provision of the cloud service in accordance with the associated documentation for the Third-Party Software.

Web browser and Viewing Devices

Chrome is recommended to use the Cloud Service, but other standard browsers might also serve this function. Screen resolution of 1920x1080 pixels or higher is recommended for best user experience.

Internet Connection

The bandwidth of Customer's internet connection determines the performance of the Cloud Service.

Ordering

To order a subscription plan and connected devices, Customer must request a quote from its Siemens sales representative.

Product Documentation

1) Product Documentation under a Standard Subscription Plan

General Contractual Documents	Links
Building X - Security Manager / Building Access Add-Ons Data Sheet	www.siemens.com/buildingx/data-sheet/security-manager-building-access-add-ons
Supplemental Terms for Buildings	www.siemens.com/buildingx/data-sheet/supplemental-terms
General Software Terms and Cloud Supplemental Terms	https://www.siemens.com/si/cloud/terms
Base Terms International	https://www.siemens.com/si/cloud/terms
Siemens Acceptable Use Policy	https://www.siemens.com/si/cloud/terms
Minimum Terms	www.siemens.com/buildingx/data-sheet/minimum-terms
Data Privacy Terms	https://www.siemens.com/dpt/si
Data Privacy Terms Annexes Building X	https://www.siemens.com/dpt/si
EU Data Act	https://www.siemens.com/buildingx/terms

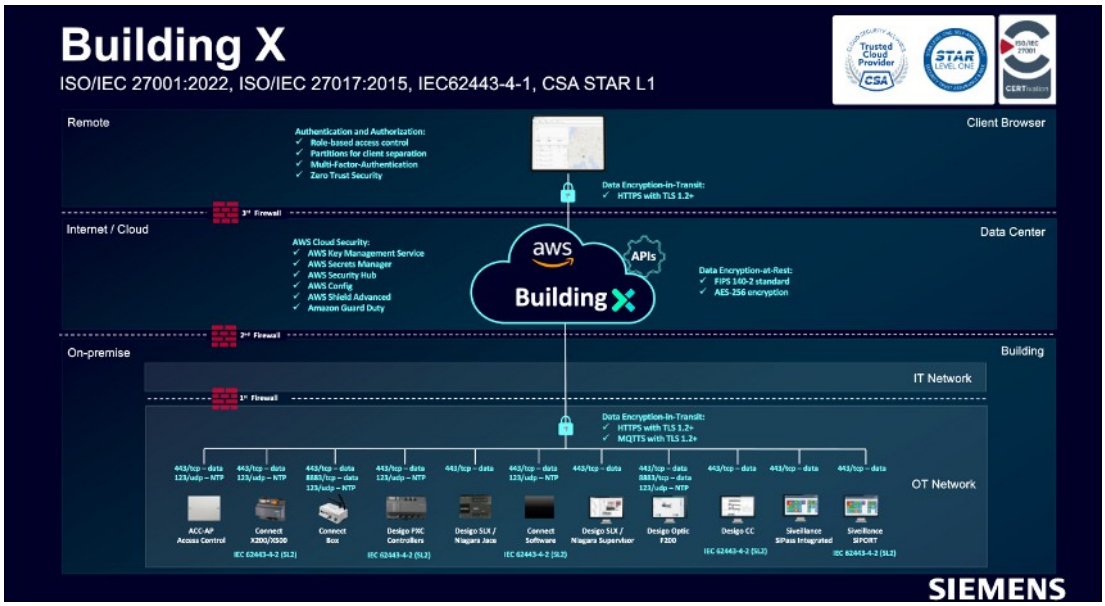
2) Product Documentation under a Custom Subscription Plan

The contractual documents and the Product Documentation are set out in Siemens' offer to the Customer.

3) Technical Documents

Technical Documentation	Link
Building X - Online help	www.siemens.com/buildingx/sid

Topology



The topology shows the superset of possibilities for connecting data to Building X. The options available for this Digital Service can be found in the list of supported connected devices and third-party software connectivity.

Data communication between the Connected Devices on-premises and the Cloud Service requires internet connectivity (to be provided by the Customer).

Specific Terms

High-Risk Use

Customer acknowledges and agrees that:

a) the Offerings are not designed to be used for the operation of or within a High-Risk System if the functioning of the High-Risk System is dependent on the proper functioning of the Offerings; and

b) the outcome from any processing of data through the use of the Offerings is beyond Siemens' control.

Service Level Agreement

Siemens shall use commercially reasonable efforts to make the Cloud Services available for a monthly uptime percentage of ninety-eight percent (98%).

Except for:

a) Planned downtime, agreed downtime, routine and emergency maintenance,
b) Cyberattacks,
c) the public, third party and/or customer's internet and communications networks,
d) data, software, hardware, telecommunications, infrastructure, power, build-packs or networking equipment not provided by Siemens,
e) Customers and Users negligence or failure in using the Cloud Service and/or in not following the instructions of published documentation,
f) system configurations and platforms not supported by Siemens,
g) system administrations, action, commands and file transfers of Customer or User,
h) modifications or alterations not made by Siemens,
i) unauthorized access via Customer's credentials and/or
j) any other failure outside of Siemens reasonable control.

Customer Support

Siemens offers helpdesk support. Customer may contact its local Siemens representative for support requests. Customers can also submit a support request online: https://www.siemens.com/support-request.

Issued by
Siemens Switzerland Ltd
Smart Infrastructure
Global Headquarters
Theilerstrasse 1a
CH-6300 Zug
+41 58 724 2424
www.siemens.com/buildingtechnologies

Document ID	A6V13175246_en--
Edition	2025-12-16