

Data Sheet

Security Manager

Building X



Security Manager is a cloud-based offering within Building X that extend access control systems with cloud services.

- Identity and Access Management
- PACS Privilege Groups
- Security Self Service Portal
- Membership Review for Security Groups
- Credential Management
- Security Monitoring and Insights Dashboards
- Print and Encode Security Cards
- Connect On-Prem Access Control Systems
- PACS SDK
- Manage SALTO Nebula

buildingx.siemens.com

Functions

Connect On-Prem Access Control Systems (*Connectivity – Physical 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 (*Connectivity – Physical Access Control Systems*)

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

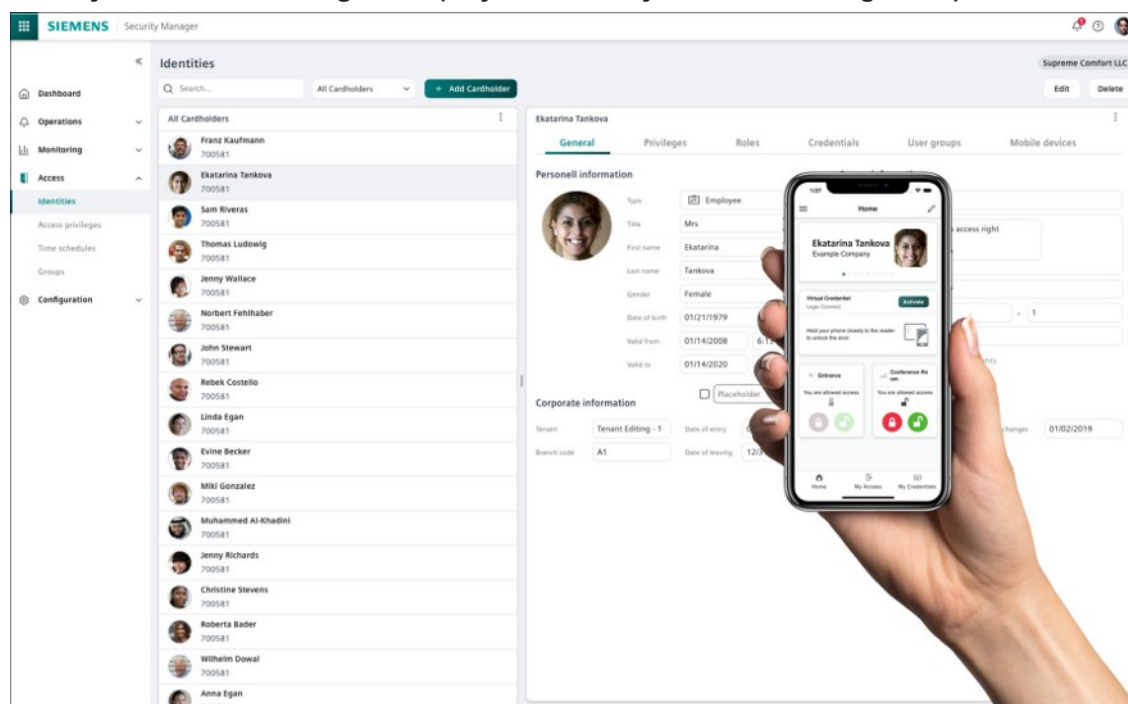
Manage SALTO Nebula (*Connectivity - SALTO Nebula Online/Offline Access Point*)

Service Engineers configure SALTO Access Points and Access Point Groups with the full feature set directly in SALTO Nebula, while Security Manager keeps a dedicated read-only SALTO Connection view for partition assignment.

Note: The following limits apply:

- Each privilege can be assigned up to 100 SALTO cloud-based locks or Access Point Groups, or any combination of both. Allowing access to up to 10,000 cloud-based locks per privilege.
- Each identity can hold up to 5 privileges
- 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

Identity and Access Management (*Physical Identity & Access Management*)



Manage newly created or imported identities:

- Manage identities based on the generic standard identity type
- Manage identities across multiple connected PACS systems
- Activate and deactivate identities
- 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)

PACS Privilege Groups (*Physical Identity & Access Management*)

SiPass Sync Agent 3.x designates Security Manager as the authoritative system for access privilege management. Access Groups are synchronized from SiPass to Security Manager and become read-only in SiPass. All assignments and modifications must be performed in Security Manager, where Access Groups are managed as Security Manager Groups with associated Access Levels. The Sync Agent ensures that changes such as group deletions or empty groups are reflected in SiPass, providing centralized, consistent, and up-to-date privilege management across systems.

Credential Management (*Physical Identity & Access Management*)

Service Engineers 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 Self Service Portal (*Security Self Service Portal*)

- Deploy predefined access approval workflow to enable employees' self-service. Configuration of approvers and the visibility in the self-service per access group.
- The 'Lost My Card' workflow allows users to report a lost card, which will be deactivated immediately. Users have a 5-day window to withdraw the request and reactivate their card if found, otherwise, the credentials will stay blocked and new ones need to be created.

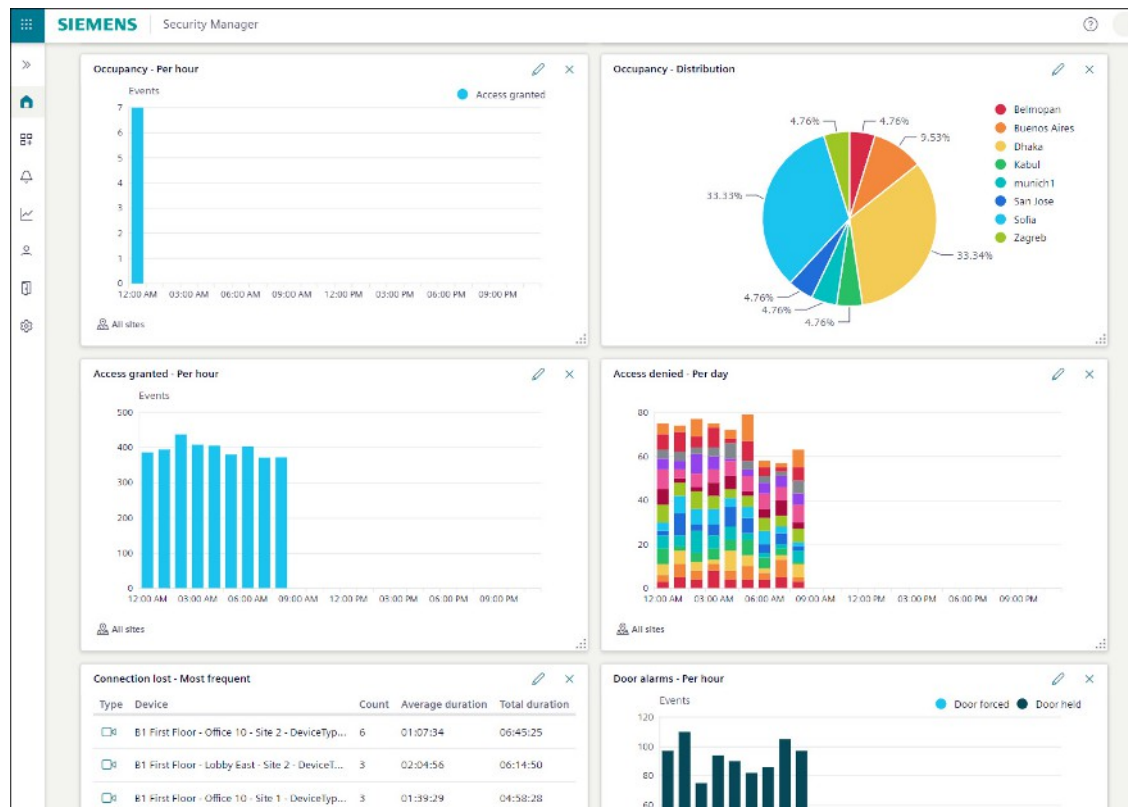
Self-service users can easily upload a new profile picture and see their photo reflected across the Building X Access app, Identity Management, and on printed access cards.

- 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.
- Workflow email notifications keep requesters, approvers, and delegates informed throughout the workflow lifecycle by providing relevant request information, status updates, approval decisions, and direct access to the corresponding workflow tasks.
- Enable LCB and DSC trained engineers to design self-service and customizable workflows (incl. the design of wizard forms via an UI editor and mapping tables) 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'.

Membership Review for Security Groups (*Security Self Service Portal*)

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.

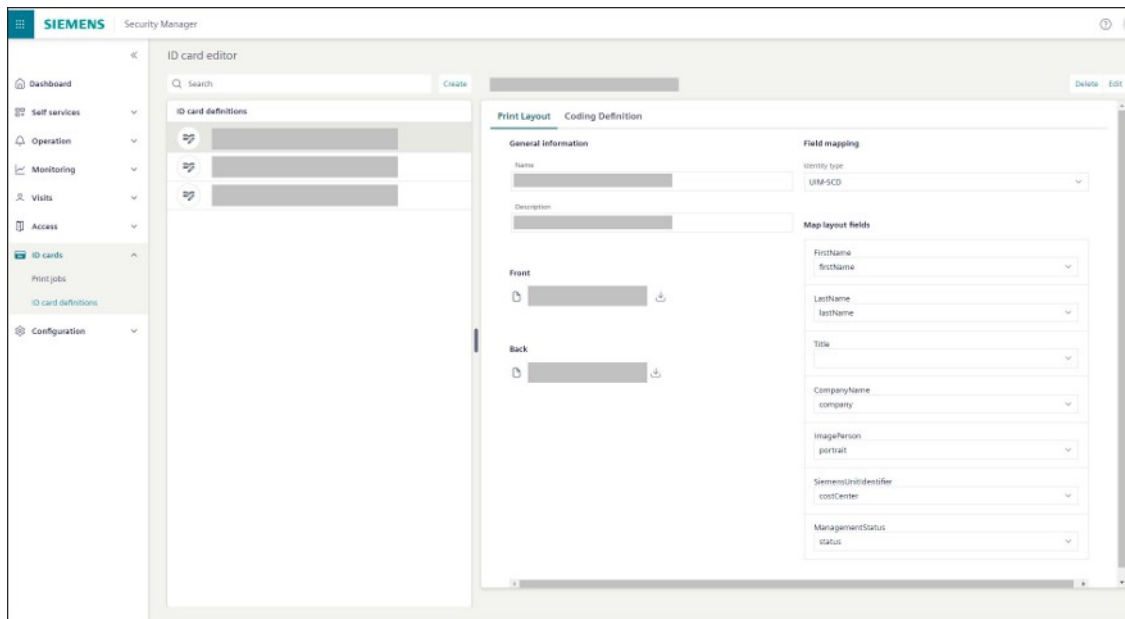
Security Monitoring and Insights Dashboards (Security Monitoring and Insights Dashboards)



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
- Visualize credential-type usage at doors/readers to assess contributions to granted vs. denied access events
- Reports to show the ID Card printing and Workflow request overall volume
- Automated reports for mobile credentials & access events by region and department
- Show the identity and virtual credentials count per partition in the widgets, monitoring and reports
- Credential expiration status widget and reporting
- Sharing of custom dashboards
- Configure scheduled reports

Print and encode Cards (Security Card Lifecycle Management)



Print and encode cards for SiPass, SIPOINT and SALTO Nebula):

- 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.

Building X Platform

Accounts Application

Ability to manage users with a role-based access control. New users can be invited to access the Cloud Service and given appropriate access rights via user groups. Users can log in with two-factor authentication and manage their user account themselves. Data can be logically grouped into partitions and given access via user groups.

Devices Application

Ability to manage Connected Devices compatible with the Cloud Service.

Data Setup Application

Ability to onboard data by adding meaning and structure to it. The data can be onboarded from multiple sources, such as Connected Devices, 3rd party cloud systems and files.

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: <https://siemens.com/dpt>

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
- Configure how long Activity Logs are retained based on your needs (e.g., 30, 90, 180, or 365 days).
- Advanced search capabilities, including structured filters, free-text search, and conditional operators such as Equal and Not Equal, to quickly locate relevant activities within large volumes of events

- Export activity log records to PDF and XLSX formats for reporting, offline analysis, auditing, and compliance purposes, using the currently selected filters

Ask Building X

Ability to ask questions in different languages about Building X technical information, utilizing GenAI.

Subscription

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

1) Default Subscription plan if the customer purchases the subscription via the Siemens online store

	Connectivity – Physical Access Control Systems (PACS)
Functions	
Connect On-Prem Access Control Systems	✓
PACS SDK	✓
Terms	
Subscription metric	per 1 door per year
Subscription term	Annually, auto-renewal
Billing term	Annually, payment in advance
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

	Connectivity – SALTO Nebula Online Access Point
Functions	
Manage SALTO Nebula	✓
Terms	
Subscription metric	per 1 door per year
Subscription term	Annually, auto-renewal
Billing term	Annually, payment in advance
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

	Connectivity – SALTO Nebula Offline Access Point
Functions	
Manage SALTO Nebula	✓
Terms	
Subscription metric	per 1 door per year
Subscription term	Annually, auto-renewal
Billing term	Annually, payment in advance
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

	Physical Identity & Access Management (PIAM)
Precondition	To use with PACS the following subscription must be active: Connectivity – Physical Access Control Systems (PACS)
Functions	
Building X Platform	✓
Identity and access management	✓

	Physical Identity & Access Management (PIAM)
PACS privilege groups	✓
Credential Management	✓
Terms	
Subscription metric	per 1 door per year
Subscription term	Annually, auto-renewal
Billing term	Annually, payment in advance
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

	Security Self Service Portal
Precondition	To use with PACS the following subscription must be active: Connectivity – Physical Access Control Systems (PACS)
Functions	
Building X Platform	✓
Security self service portal	✓
Membership review for security groups	✓
Terms	
Subscription metric	per 1 door per year
Subscription term	Annually, auto-renewal
Billing term	Annually, payment in advance
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

	Security Monitoring and Insights Dashboards
Precondition	To use with PACS the following subscription must be active: Connectivity – Physical Access Control Systems (PACS)
Functions	
Building X Platform	✓
Security monitoring and insights dashboards	✓
Terms	
Subscription metric	per 1 door per year
Subscription term	Annually, auto-renewal
Billing term	Annually, payment in advance
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

	Security Card Lifecycle Management
Precondition	To use with PACS the following subscription must be active: Connectivity – Physical Access Control Systems (PACS)
Functions	
Building X Platform	✓

	Security Card Lifecycle Management
Print and encode security cards	✓
Terms	
Subscription metric	per 1 door per year
Subscription term	Annually, auto-renewal
Billing term	Annually, payment in advance
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 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.

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 Supported versions are SiPass MP 2.95 HF11 or later and SiPass 3.0 IR05 or later. Sync Agent 2.x capabilities • Synchronization of identities • Synchronization of privileges and privilege assignments • Synchronization of physical and virtual credentials • Upload of events and alarms • Publication of door sets, access points, input points, and output points to Data Setup • Virtual credential assignment from Security Manager to SiPass Limitations • Profile pictures are available through the initial profile picture export. Subsequent changes to profile pictures and newly assigned profile pictures are not synchronized automatically. • Updates to door sets, access points, input points, output points, and newly added devices are not synchronized to Data Setup after the initial publication. • Privileges must originate in SiPass. Privileges created in Security Manager are not synchronized to SiPass. SiPass with Sync Agent 3.x Supported versions are SiPass 2.95 IR23 or later and SiPass 3.0 IR05 or later. Sync Agent 3.x capabilities • Synchronization of identities • Synchronization of access groups and privilege assignments • Synchronization of physical and virtual credentials • Upload of events and alarms • Virtual credential download • Publication of door sets, access points, input points, and output points to Data Setup Limitations • Access groups are managed in Security Manager and become read-only in SiPass after onboarding. • Profile pictures are available through the initial profile picture export. Subsequent changes to profile pictures and newly assigned profile pictures are not synchronized automatically. • Updates to door sets, access points, input points, output points, and newly added devices are not synchronized to Data Setup after the initial publication. Supported card readers The following card readers have been validated for use with the SiPass integration: • Autec: XMP-TMC2150, XMP-TMC2160, XMP-TMC2170, XMP-TMC2180, XMP-TMC2357, XMP-TMC2367, XMP-TMC2457-UP, XMP-TMC3050, XMP-TMC3060, XMP-TMC3070, XMP-TMC3080

	List of Supported Connected Devices
	• 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 The readers listed above are validated and supported. Additional readers supported by SiPass may also be compatible. For details, refer to the SiPass release notes. For information about compatibility with the Virtual Credential feature, refer to the Security Manager Mobile Access Data Sheet: www.siemens.com/buildingx/data-sheet/security-manager-mobile-access.
SIEMENS: SIPORT	SIPORT with Sync Agent 2.x The SIPORT software product runs on Windows-based hardware. Supported versions are SIPORT V3.5.0.134 or later and SIPORT 4.0 or later. Sync Agent 2.x capabilities • Synchronization of identities (name, email address, and virtual credential flag) • Synchronization of privileges and privilege assignments • Synchronization of physical and virtual credentials • Upload of events and alarms • Virtual credential download • Publication of door sets, access points, input points, and output points to Data Setup Limitations • Cardholder profile pictures are available through the initial profile picture export. • Subsequent changes to profile pictures and newly assigned profile pictures are not synchronized automatically. • Updates to door sets, access points, input points, output points, and newly added devices are not synchronized to Data Setup after the initial publication. Supported card readers The following card readers have been validated for use with the SIPORT integration: • 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 information about compatibility with the Virtual Credential feature, refer to the Security Manager Mobile Access Data Sheet: www.siemens.com/buildingx/data-sheet/security-manager-mobile-access.
SALTO Nebula	Supported SALTO Nebula devices include electronic cylinders, padlocks, escutcheons, smart locks, wall readers, motorized locks, and card update devices, including: Neo Cylinder, Neoxx Padlock, XS4 Original+, XS4 One, XS4 One S, XS4 Mini, DBolt, DLok, Wall Readers (including BLUenet Controller), and NCoder Nebula. Restriction PIN-based access is currently not supported by Security Manager. Therefore, keypad functionality cannot be configured or managed through Security Manager. : Only locks without keypads are supported, as Security Manager does not yet provide PIN functionality. Note: Hardware configuration has been moved to the SALTO Nebula application. Device commissioning and device-specific settings must be configured in SALTO Nebula and are not managed by Security Manager.

	List of Supported Connected Devices
	For the latest list of supported SALTO Nebula devices, refer to: https://support.saltosystems.com/nebula/user-guide/installer/device-overview/

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

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 Packages Data Sheet	www.siemens.com/buildingx/data-sheet/security-manager-building-access-packages
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.

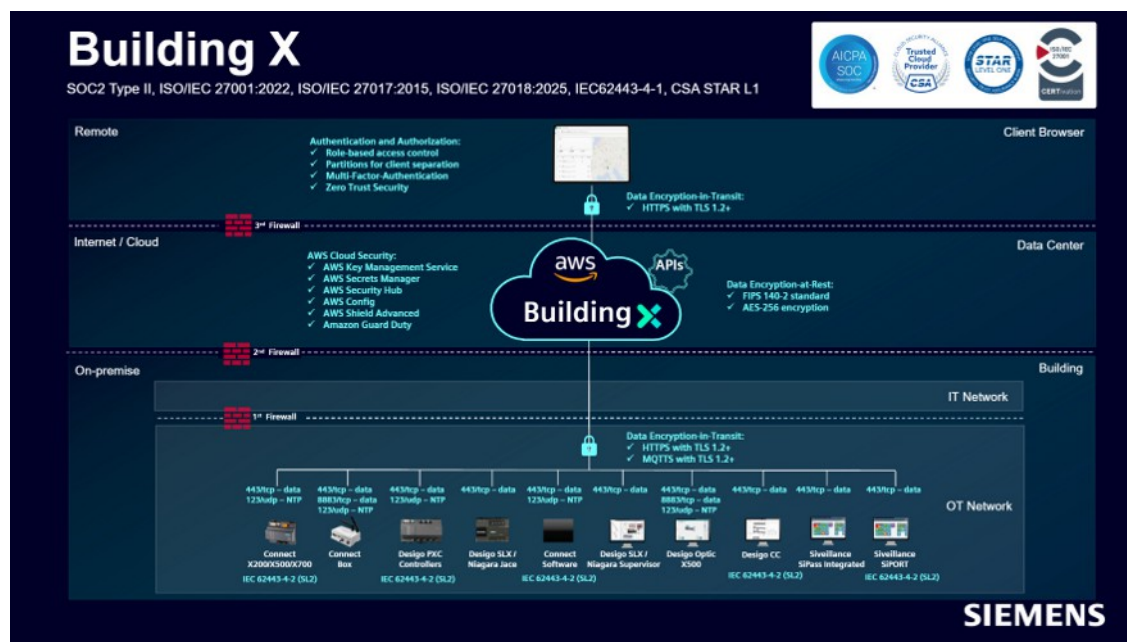
3) Technical Documents

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

4) Compliance

Cybersecurity	Link
Cyber Security Alliance - STAR Level 1	https://cloudsecurityalliance.org/star/registry/siemens-ag/services/building-x
IEC 62443-4-1	https://www.siemens.com/en-us/system-certificates/si-b/
ISO/IEC 27001:2022	https://www.siemens.com/en-us/system-certificates/si-b/
ISO/IEC 27017:2015	https://www.siemens.com/en-us/system-certificates/si-b/
ISO/IEC 27018:2025	https://www.siemens.com/en-us/system-certificates/si-b/
SOC 2 Type II Report	Report available on request
SOC 3 Report	https://www.siemens.com/en-us/system-certificates/si-b/

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:

- 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
- 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 yearly uptime percentage of ninety-eight percent (98%).

Except for:

- Planned downtime, agreed downtime, routine and emergency maintenance,
- Cyberattacks,
- the public, third party and/or customer's internet and communications networks,
- data, software, hardware, telecommunications, infrastructure, power, build-packs or networking equipment not provided by Siemens,
- Customers and Users negligence or failure in using the Cloud Service and/or in not following the instructions of published documentation,
- system configurations and platforms not supported by Siemens,
- system administrations, action, commands and file transfers of Customer or User,
- modifications or alterations not made by Siemens,
- unauthorized access via Customer's credentials and/or
- 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

© Siemens 2026
Technical specifications and availability subject to change without notice.

Document ID	A6V13175246_en--
Edition	2026-09-22