SIEMENS

Data Sheet

Security Manager - Mobile

Building X



Security Manager / Mobile Access are a cloud-based offerings within Building X that allows you to open doors with your smartphone.

- Virtual Credential for Card Readers
- Apple Wallet Credential
- Google Wallet Credential
- Credential for SALTO Access Points
- Mobile App SDK
- On-premises Virtual Credentials for SIPORT
- Mobile Credential Management
- Photo Upload
- Connect On-Prem Access Control Systems
- Manage SALTO Nebula

URL

buildingx.siemens.com

iOS: https://apps.apple.com/app/building-x-access/id1483078094

Android: https://play.google.com/store/apps/details?id=com.siemens.accessmobile&hl=gsw

Functions

Mobile App SDK *(Virtual Credential for Card Readers)*

Use the Mobile App SDK to integrate mobile access functionalities into your own mobile app

Mobile Credential Management *(Virtual Credential for Card Readers)*

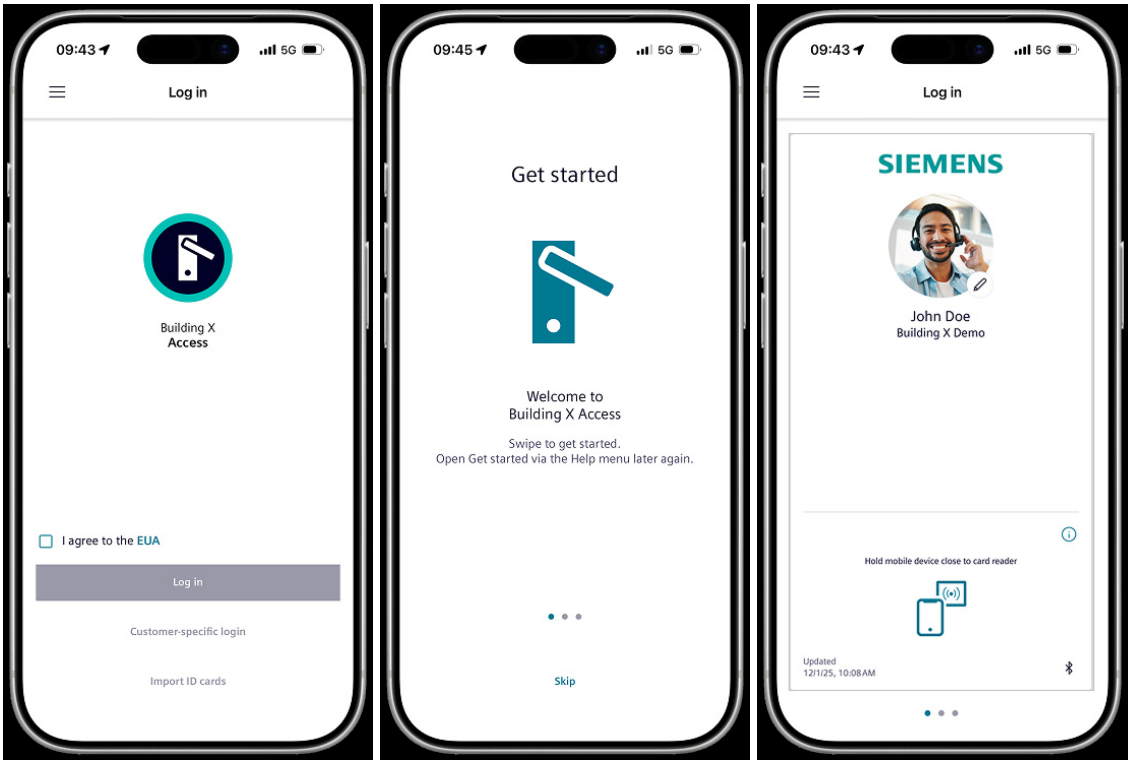
Service Engineer can configure the following:

- How many mobile credentials can be assigned to one identity
- How many mobile credentials can be activated at the same time
- How many mobile devices can be activated by user at the same time to avoid additional costs

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.
- Protect highly sensitive keys by restricting access and configuration actions to a dedicated user role.

Virtual Credential for Card Readers *(Virtual Credential for Card Readers)*



Use of Customer’s smartphone to open doors that are secured by a LEGIC Connect enabled card reader connected to either a SiPass or SIPORT controller or to cloud connected ACC-AP door controller.

The following conditions apply:

- A user can switch devices up to three times per year without any additional cost.
- Deactivating and reactivating a device does not result in extra cost.
- Reporting a device as stolen and reactivating it after it is found does not lead to extra costs.
- Disabling and re-enabling the "Enable Virtual Credential" option in Security Manager / Identities will generate new virtual credentials for all of the user's devices, which will result in additional charges.

On-premise Virtual Credentials for SIPORT *(Virtual Credential for Card Readers)*

Support of on-premises virtual credentials via offline import for SIPORT customers.

Upload Portrait Picture through Smartphone *(Virtual Credential for Card Readers)*

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

Credential for SALTO Access Points *(Credential for SALTO Access Points)*

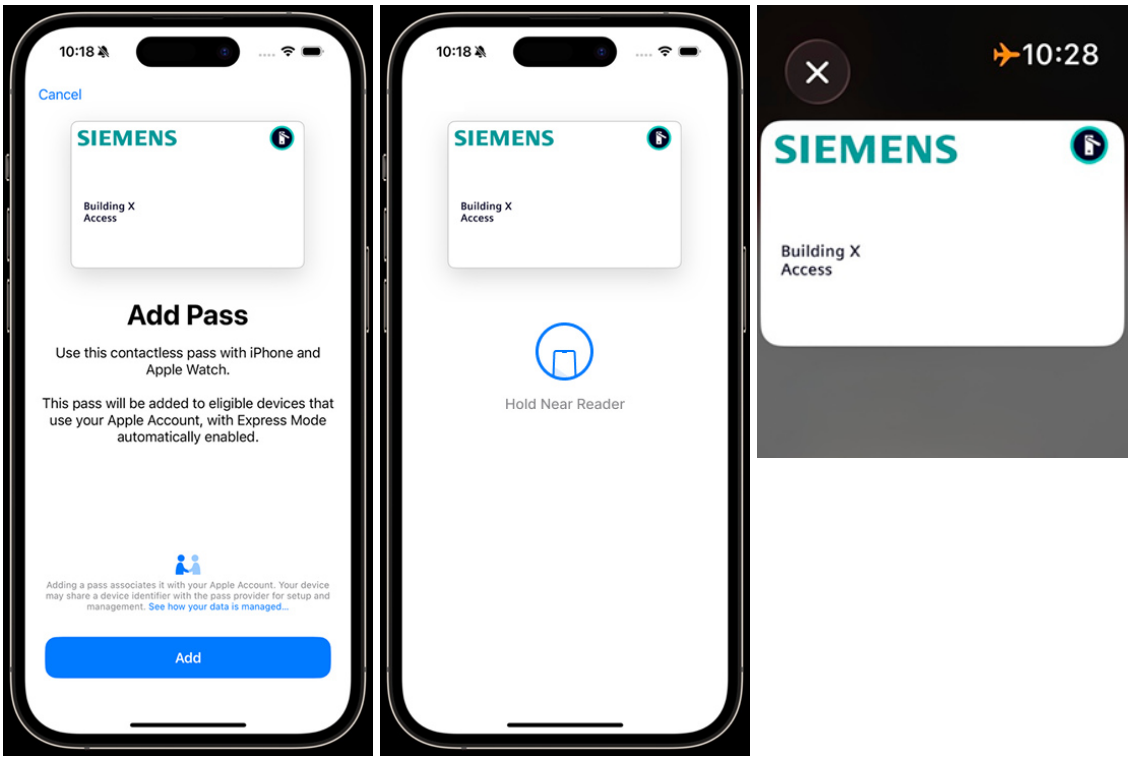
Use of Customer's smartphone or a physical card to open doors that are secured by smart locks from SALTO.

The following conditions apply:

- A user can switch devices up to three times per year without any additional cost.
- Deactivating and reactivating a device does not result in extra cost.
- Reporting a device as stolen and reactivating it after it is found does not lead to extra costs.

Apple Wallet Credential *(Apple Wallet Credential)*

iPhone: Apple Watch:



Apple Wallet allows instant access when users hold their iPhone or Apple Watch near a compatible card reader, eliminating the delay experienced with Bluetooth Low Energy (BLE) systems.

To use the service with Apple Wallet, additional Terms and Conditions are required, which must be signed in advance. For further details, please contact request.securitymanager.si@siemens.com.

Google Wallet Credential *(Google Wallet Credential)*

Android users can add their credential to Google Wallet and open doors straight from the lock screen without launching or even keeping the Building X Access app, while Security Managers keep central control over enabling, suspending, and resuming that credential across all of an identity's devices.

To use the service with Google Wallet, additional Terms and Conditions are required, which must be signed in advance. For further details, please contact *request.securitymanager.si@siemens.com*.

Connect ACC-AP Door Controller *(Connectivity – Cloud-based Access Control)*

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

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.
- Each identity can hold up to 5 privileges.
- Each privilege includes one time schedule.
- Up to 100 Access Points can be included in an Access Point Group.

Device commissioning and device-specific settings must be configured in SALTO Nebula. For the latest list of supported SALTO Nebula devices, refer to: https://support.saltosystems.com/nebula/user-guide/installer/device-overview

Building X Platform *(Virtual Credential for Card Readers, Apple Wallet Credential)*

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

Subscription

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

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

	Virtual Credential for Card Readers
Precondition	To use with PACS the following subscription must be active: ● Connectivity – Physical Access Control Systems (PACS)
Functions	
Building X Platform	✓
Mobile App SDK	✓
Mobile Credential Management	✓
Virtual Credential for Card Readers	✓
On-premises Virtual Credentials for SIPORT	✓
Terms	
Subscription metric	per 1 device 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

	Apple Wallet Credential
Precondition	To use with PACS the following subscription must be active: ● Connectivity – Physical Access Control Systems (PACS)
Functions	
Building X Platform	✓
Apple Wallet Credential	✓
Terms	
Subscription metric	per 1 Apple ID user 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

	Google Wallet Credential
Precondition	To use with PACS the following subscription must be active: ● Connectivity – Physical Access Control Systems (PACS)
Functions	
Building X Platform	✓
Google Wallet Credential	✓
Terms	
Subscription metric	per 1 Apple ID user per year
Subscription term	Annually, auto-renewal

	Google Wallet Credential
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

	Credential for SALTO Access Points
Precondition	One of the following subscriptions must be active: • Connectivity: SALTO Nebula Online Access Point • Connectivity: SALTO Nebula Offline Access Point
Functions	
Building X Platform	✓
Credential for SALTO Access Points	✓
Terms	
Subscription metric	per 1 Google ID user 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 – 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

The Security Manager / Mobile Access 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.

	List of Supported Connected Devices
	● 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 and the virtual credential feature: ● Autec: XMP-TMC2170, XMP-TMC2180, XMP-TMC3070, XMP-TMC3080 ● Elatec: Secustos SQ80 Legic, Secustos SQ80 K Legic, Secustos MU20 LEGIC, Secustos MU20 K LEGIC ● Acre: AR10S-MF, AR40S-MF, AR20M-MF, AR50M-MF ● Apple Wallet Credential is supported by all ECP2 certified card readers
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**

	List of Supported Connected Devices
	The following card readers have been validated for use with the SIPORT integration and the virtual credential feature: ● Autec: XMP-TMC2170, XMP-TMC2180, XMP-TMC3070, XMP-TMC3080 ● Apple Wallet Credential is supported by all ECP2 certified card readers
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. 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.

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.

Mobile Devices

To install the mobile app, iOS 16.0 and above or Android 10 and above is required.

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 / Mobile Access Data Sheet	www.siemens.com/buildingx/data-sheet/security-manager-mobile-access
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

General Contractual Documents	Links
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.

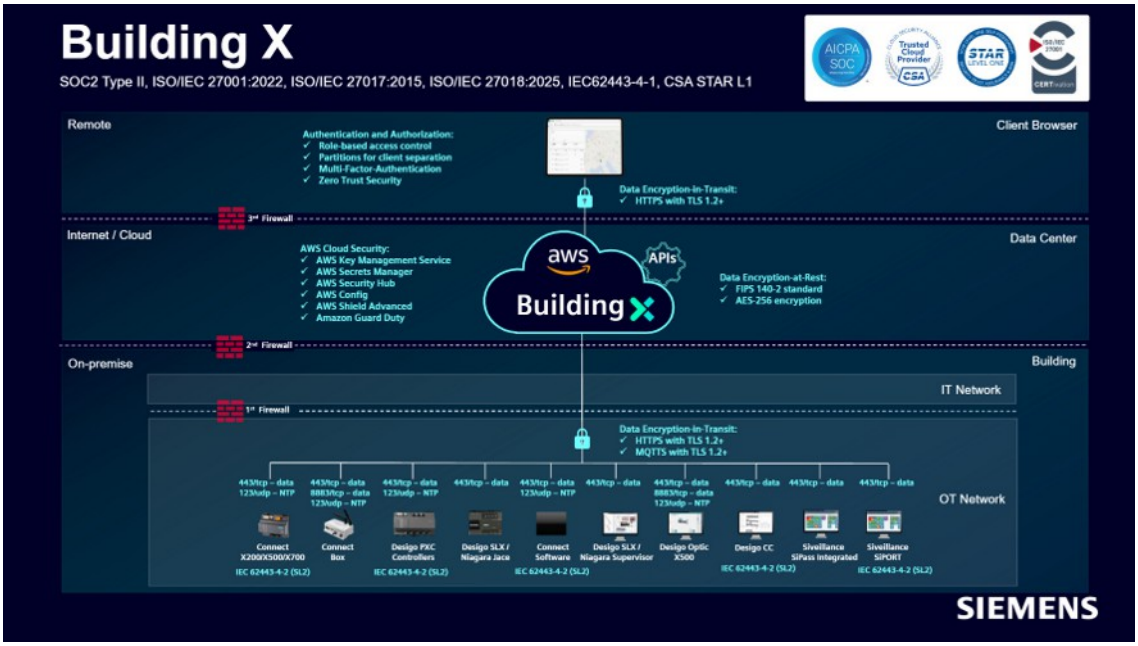
3) Technical Documents

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

Terms and Conditions for Use of Apple Wallet Functionality

1. As a prerequisite of using the Apple Wallet Functionality, Customer receives and shall agree Apple's Participating Provider Pass-Through Terms (including Apple's Apple Brand Guidelines) with Legic Identsystems AG with registered seat in CH-8620 Wetzikon, Switzerland.
2. Customer ensures that by using the Apple Wallet Functionality none of its Users is in breach by of a user agreement and will amend the user agreement if so required.
3. Customer shall make the relevant executives, relationship managers, and engineers available to participate in meetings (in person, via telephone or via video conference) as may be requested by Apple and communicated by Siemens to Customer from time to time.

Terms and Conditions for Use of Google Wallet Functionality

1. As a prerequisite of using the Google Wallet Functionality, Customer receives and shall agree to the separate document with Google's Participating Provider Pass-Through Terms with Siemens.
2. Customer ensures that by using the Google Wallet Functionality none of its users is in breach by of a user agreement and will amend the user agreement if so required.

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 yearly 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

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

Document ID A6V15573372_en--
Edition 2026-09-22