

Security Manager

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
- Access on Credential for Smart Locks
- Apple Wallet Credential
- Mobile App SDK
- On-premises Virtual Credentials for SIPOINT
- Mobile Credential Management
- Photo Upload
- Connect ACC-AP Door Controller
- Connect On-Prem Access Control Systems
- Activity Log

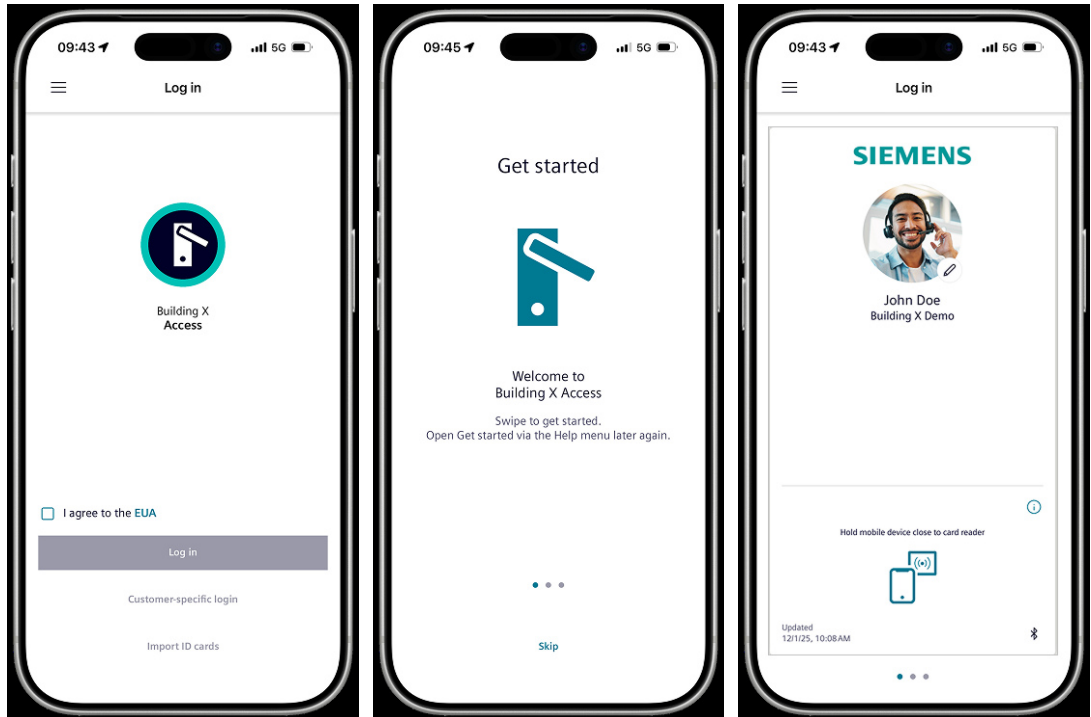
URL

Web: securitymanager.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>

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 SIPOINT 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.

Access on Credential for Smart Locks

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

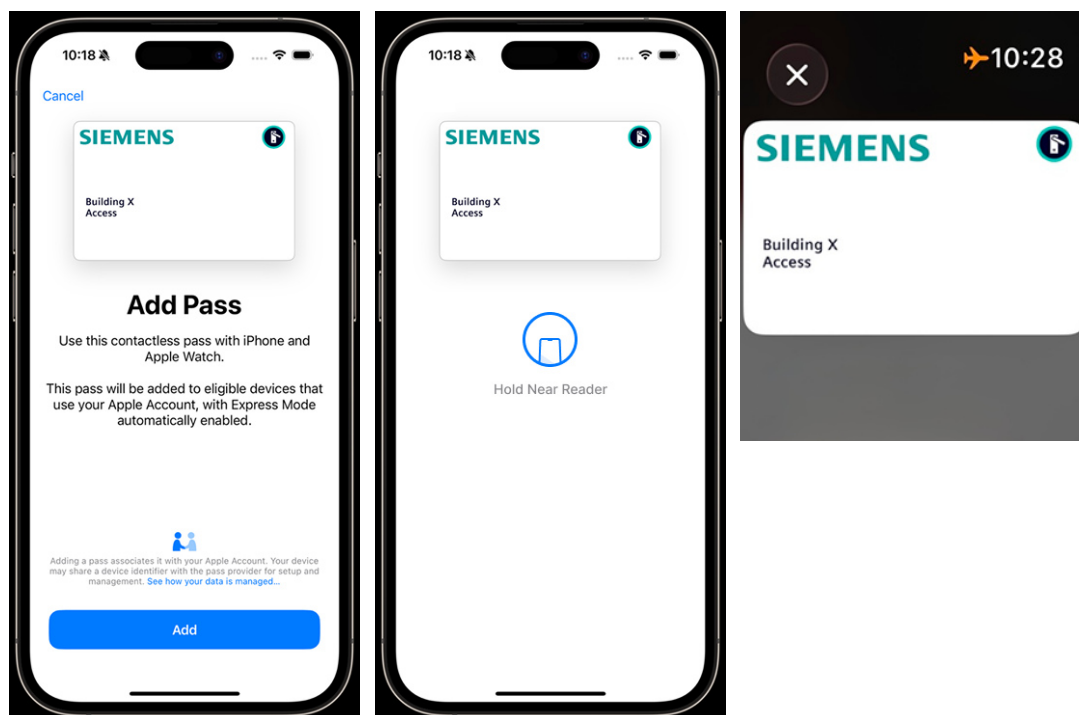
The following conditions apply:

- 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

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 securitymanager.si@siemens.com.

Mobile App SDK

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

On-premise Virtual Credentials for SIPORT

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

Mobile Credential Management

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.

Photo Upload

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.

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.

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

Security Manager / Mobile Access					
	Mobile Access - Virtual Credential for Card Readers	Mobile Access - Access on Credential for Smart Locks	Mobile Access - Apple Wallet Credential	Connectivity – Physical Access Control Systems (PACS)	Connectivity – Cloud-based Access Control
Precondition	<p>To use with PACS the following subscription must be active:</p> <ul style="list-style-type: none"> • Connectivity – Physical Access Control Systems (PACS) <p>To use with cloud-based access control the following subscriptions, must be active:</p> <ul style="list-style-type: none"> • Connectivity – Cloud-based Access Control • Building Access Essential or Building Access Standard • Photo upload 	<p>One of the following subscriptions must be active:</p> <ul style="list-style-type: none"> • Connectivity – Cloud-based Access Control • Building Access Essential or Building Access Standard • Photo upload 	<p>To use with PACS the following subscription must be active:</p> <ul style="list-style-type: none"> • Connectivity – Physical Access Control Systems (PACS) <p>To use with cloud-based access control the following subscriptions, must be active:</p> <ul style="list-style-type: none"> • Connectivity – Cloud-based Access Control • Building Access Essential or Building Access Standard 		-
Functions	User management Activity Log				
	Virtual Credential for Card Readers Mobile App SDK Mobile Credential Management On-premises Virtual Credentials for SIPORT	Access on Credential for Smart Locks Mobile App SDK Upload Portrait Picture through Smartphone Mobile Credential Management	Apple Wallet Credential	Connect On-Prem Access Control Systems PACS SDK	Connect ACC-AP door controller

Security Manager / Mobile Access					
	Mobile Access - Virtual Credential for Card Readers	Mobile Access - Access on Credential for Smart Locks	Mobile Access - Apple Wallet Credential	Connectivity – Physical Access Control Systems (PACS)	Connectivity – Cloud-based Access Control
Subscription metric	per 1 device per year The subscription plan can be purchased in packages of 1 device		per 1 Apple ID user per year The subscription plan can be purchased in packages of 1 Apple ID user	per 1 door per year The subscription plan can be purchased in packages of 1 door	
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.

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	<p>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.</p> <p>SiPass includes multiple software applications collectively referenced herein as Software to supply building data to this Cloud Service. The following card readers support the virtual credential feature supported:</p> <ul style="list-style-type: none"> Autec: XMP-TMC2170, XMP-TMC2180, XMP-TMC3070, XMP-TMC3080 Elatec: Secustos SQ80 Legic, Secustos SQ80 K Legic, Secustos MU20 LEGIC, Secustos MU20 K LEGIC <p>Apple Wallet Credential is supported by all ECP2 certified card readers</p>

List of Supported Connected Devices	
SIEMENS: SIPORT	<p>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.</p> <p>SiPass with Sync Agent 3.x: SiPass software product is running on Windows computer hardware. The supported software version is SiPass 2.95 IR23 or higher and is not compatible with SiPass 3.0. With this version, Security Manager is the leading system, and Access Groups synchronized from SiPass become read-only in SiPass. Multi-PACS setups are not supported.</p> <p>SIPORT includes multiple software applications collectively referenced herein as Software to supply building data to this Cloud Service. The following card readers support the virtual credential feature supported:</p> <ul style="list-style-type: none"> • Autec: XMP-TMC2170, XMP-TMC2180, XMP-TMC3070, XMP-TMC3080 <p>Apple Wallet Credential is supported by all ECP2 certified card readers</p>
SALTO Nebula Electronic lock	<p>Neo Cylinder, Neoxx padlock, XS4 Original+, XS4 One and XS4 One S (only models that support HSE), XS4 Mini, DBolt.</p> <p>Restriction: Only locks without keypads are supported, as Security Manager does not yet provide PIN functionality</p>
SALTO Nebula Gateways	<p>IQ3, IQ3 Mini</p>
SIEMENS: ACC-AP	<p>ACC-AP with firmware V6.5.X or higher, based on the ACC-AP hardware, to supply access door data to this Cloud Service.</p> <p>The following card readers support the virtual credential feature supported:</p> <ul style="list-style-type: none"> • Autec: XMP-TMC2170, XMP-TMC2180, XMP-TMC3070, XMP-TMC3080 • Elatec: Secustos SQ80 Legic, Secustos SQ80 K Legic, Secustos MU20 LEGIC, Secustos MU20 K LEGIC <p>Apple Wallet Credential is supported by all ECP2 certified card readers.</p>

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.

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
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

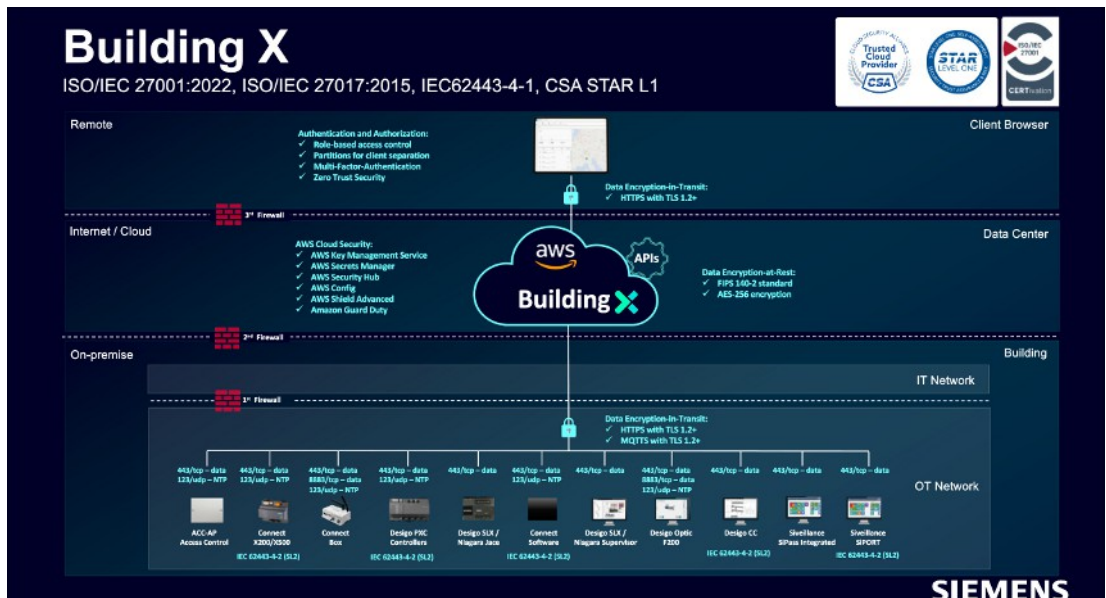
2) Product Documentation under a Custom Subscription Plan

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

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.

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>.