

Security Manager / Starter Kit for SiPas and SIPOINT

Building X



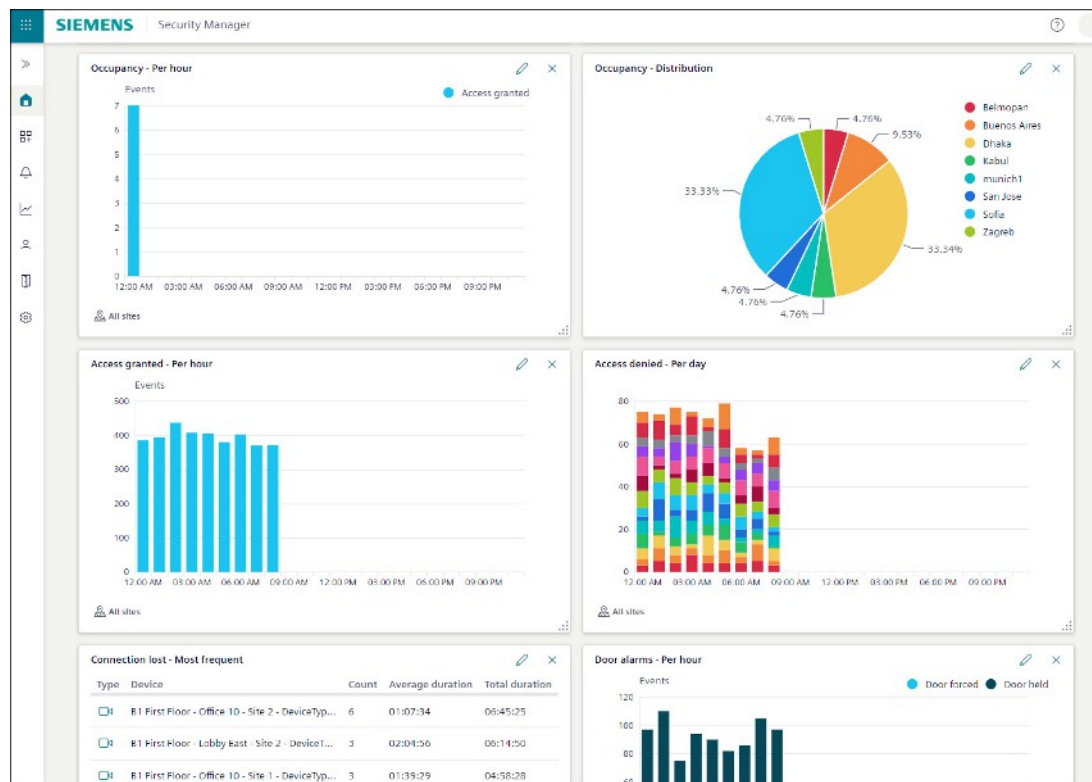
Security Manager / Starter Kit for SiPass and SIPOINT is a cloud-based offering within Building X for SiPass and SIPOINT customers with valid SUS / SUR.

- Security Monitoring and Insights Dashboards for up to 20 PACS doors
- Connect to one On-Prem Access Control Systems (SiPass or SIPOINT)

URL

securitymanager.siemens.com

Security Monitoring and Insights Dashboards for up to 20 PACS Doors



Get actionable insights based on security data for up to 20 PACS doors:

- Visualize unique access events per building
- Measure room or building utilization based on the number of "access-granted" events
- Identify maintenance candidates or utilization outliers as indicators for malfunctions
- Sharing of custom dashboards
- Configure scheduled reports

Connect to one On-Prem Access Control Systems (SiPass or SIPOINT)

Connect one SiPass or SIPOINT system to Building X Security Manager.

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.

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

Security Manager / Starter Kit SiPass & SIPORT	
Precondition	Valid SUS / SUR
Functions	Security Monitoring and Insights Dashboards for up to 20 PACS doors Connect to one On-Prem Access Control Systems (SiPass or SIPORT) User management Activity Log
Subscription metric	per SiPass or SIPORT System
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

The Security Manager / Starter Kit SiPass & SIPORT 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 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.

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 (HF09) 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-TMC2477-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).
SIEMENS: SIPORT	SIPORT with Sync Agent 2.x*: SIPORT software product is running on Windows computer hardware. The supported software version is SIPORT V3.5.0.118 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-TMC2477-UP, XMP-TMC3050, XMP-TMC3060, XMP-TMC3070, XMP-TMC3080.

	List of Supported Connected Devices
	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.

(*) Sync Agent 2.x supports the synchronization of identities (name, email, and virtual credential flag), privileges, the upload of events/alarms and the virtual credential download. It currently does not support the synchronization of profile pictures and credentials.

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 / Starter Kit for SiPass and SIPOINT Data Sheet	www.siemens.com/buildingx/data-sheet/security-manager-starter-sipass-siport
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

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) Data Privacy Terms

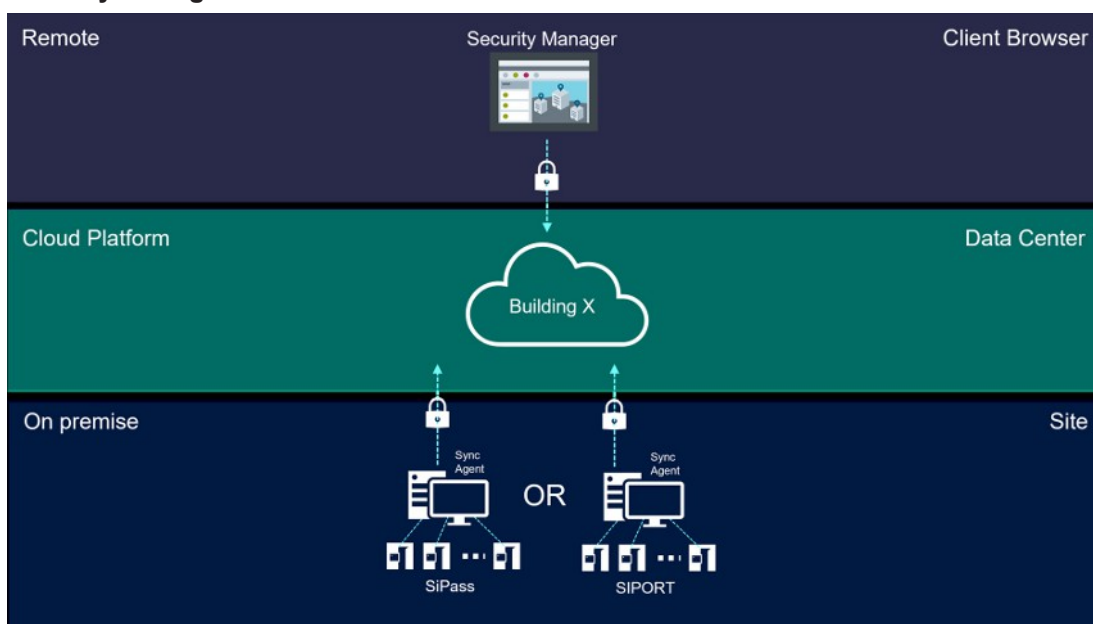
Data Privacy Terms	Links
Data Privacy Terms	https://www.siemens.com/dpt/si
Data Privacy Terms Annexes Building X	https://www.siemens.com/dpt/si

4) Technical Documents

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

Topology

Security Manager / Starter Kit SiPass & SIPOINT



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 monthly 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 net-working 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.

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

© Siemens 2025
Technical specifications and availability subject to change without notice.