SIEMENS

Data Sheet

Security Manager

Building X

The Security APIs are cloud-based offerings within Building X that are used to manage identities and access privileges and read security events and security alarms via APIs.

- Building Security Identities and Privileges API
- Building Security Alarms and Events API
- Building Security Workflow API
- Building Security SCIM API
- Building Security Siveillance Intrusion API

URLs

Development Portal: https://developer.bpcloud.siemens.com

API Manager: https://developer.bpcloud.siemens.com

Functions

Building Security Identities and Privileges API

Building Security Identities and Privileges API provides access to:

- Read/write identities
- Read privileges
- Assign privileges to an Identity
- Assign credentials to an Identity

Building Security Alarms and Events API

The Building Security Alarms and Events API provides access to:

- Read activities

Building Security Workflow API

The Building Security Workflow API provides access to:

- Listing and starting security workflows

Building Security SCIM API

The Security SCIM API provides access to:

- Onboarding and offboarding of identities via a SCIM interface (e.g. MS Azure ID)

Building Security Siveillance Intrusion API

The Security Siveillance Intrusion API provides access to:

- Managing Siveillance Intrusion Advanced / Pro systems

Developer Portal

The Developer Portal provides an overview which APIs are available for use as well as tutorials, getting started and the Security API swagger description.

API Management

The API Manager app provides (i) the ability to manage machine user credentials for enabling access to the Security APIs, (ii) an overview about API usage and (iii) the ability to try out the API via swagger template.

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="6">Security API</th></tr>
<tr><th></th><th>Building Security Identities and Privileges API</th><th>Building Security Alarms and Events API</th><th>Building Security Workflow API</th><th>Building Security SCIM API</th><th>Building Security Siveillance Intrusion API</th></tr>
<tr><td>Precondition</td><td colspan="4">To use the API, one of the following subscriptions, must be active:
Connectivity – Physical Access Control Systems (PACS), or
Connectivity – Cloud-based Access Control
And one of the following subscriptions must be active:</td><td>To use the API, one of the following subscriptions, must be active:
Connectivity – Physical Intrusion Detection System
And one of the following subscriptions must be active:</td></tr>
<tr><td></td><td>• Building Access Essential or Building Access Standard
• Physical Identity & Access Management (PIAM)</td><td>• Building Access Essential or Building Access Standard
• Visitor Management Essential or Visitor Management Standard
• Physical Identity & Access Management (PIAM)
• Security Alarm & Task Management
• Security Self Service Portal
• Security Monitoring and Insights Dashboards
• Mobile Access - Virtual Credential for Card Readers
• Mobile Access - Access on Credential for Smart Locks</td><td>• Building Access Standard
• Security Self Service Portal</td><td>• Building Access Essential or Building Access Standard
• Physical Identity & Access Management (PIAM)</td><td>• Intrusion Detection Essential
• Intrusion Detection Standard</td></tr>
<tr><td>Functions</td><td colspan="2">User management
Developer Portal
API Management</td><td colspan="2">Developer Portal</td><td>User management
Developer Portal
API Management</td></tr>
<tr><td></td><td>Building Security Identities and Privileges API</td><td>Building Security Alarms and Events API</td><td>Building Security Workflow API</td><td>Building Security SCIM API</td><td>Building Security Siveillance Intrusion API</td></tr>
<tr><td>Subscription metric</td><td colspan="5">per 6 Mill. API calls per year</td></tr>
<tr><td>Subscription term</td><td colspan="5">Annually, auto-renewal</td></tr>
<tr><td>Billing term</td><td colspan="5">Annually, payment in advance</td></tr>
<tr><td>Upscale</td><td colspan="5">Effective immediately, pro-rated billing</td></tr>
<tr><td>Downscale / Cancellation</td><td colspan="5">Effective with end of subscription term</td></tr>
<tr><td>Connected Devices</td><td colspan="5">To be purchased separately</td></tr>
</table>

Security API					
	Building Security Identities and Privileges API	**Building Security Alarms and Events API**	**Building Security Workflow API**	**Building Security SCIM API**	**Building Security Siveillance Intrusion API**
Permitted Identities	Up to 10,000; Extended Use				

The Security API 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.

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 use cases, such as very large sites Customer may contact its sales representative for a 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).
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.

	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).
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.

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 API Data Sheet	www.siemens.com/buildingx/data-sheet/security-apis
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

General Contractual Documents	Links
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

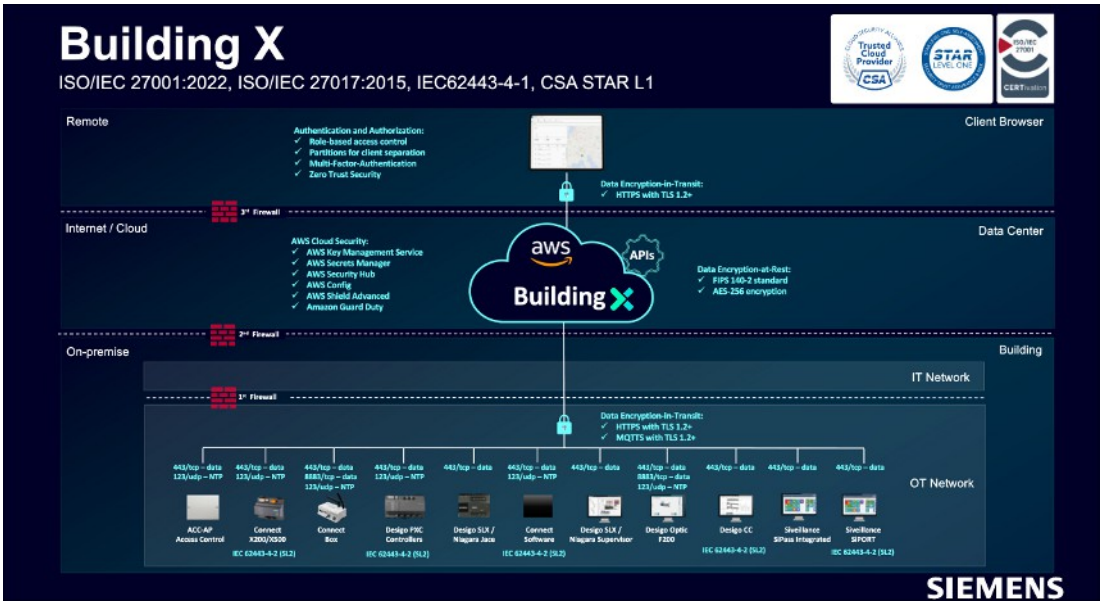
2) Product Documentation under a Custom Subscription Plan

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	A6V14152435_en--
Edition	2025-12-16