SIEMENS

Data Sheet

Security Manager

Building X

Security Manager / Intrusion Detection are cloud-based offerings within Building X that are used to remotely monitor and operate Siveillance Intrusion systems.

- Essential Identity and Access & Arming / Disarming Management
- Standard Identity and Access & Arming / Disarming Management
- Security Self Service Portal
- Membership Review for Security Groups
- Credential Management
- Security Alarm Management
- Security Monitoring and Insights Dashboards
- Connect On-Prem Siveillance Intrusion Systems
- Keypad NXT Edge
- Activity Log

URL

securitymanager.siemens.com

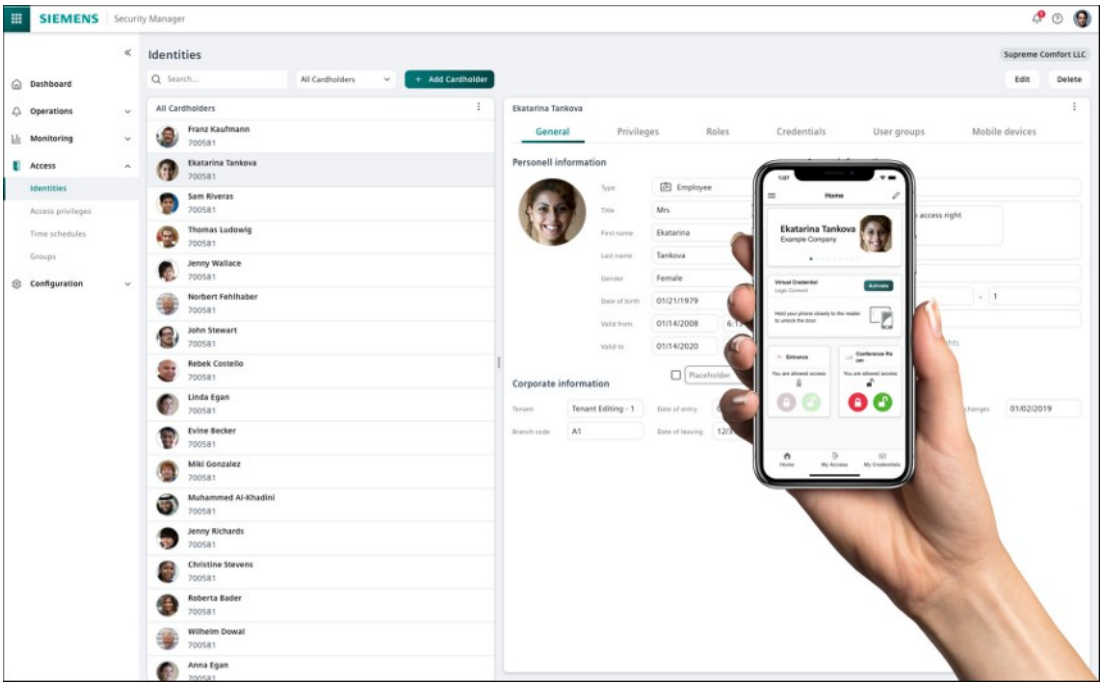
Functions

Essential Identity and Access Management

Manage identities based on the fixed basic identity type (incl. general identity information), assign access and arming / disarming privileges and credentials, manage and assign security groups, manage mobile devices.

Note: It is currently possible to assign multiple access privileges associated with different Siveillance Intrusion Advanced / Pro authorization groups to a single identity within Security Manager. However, due to system limitations in Siveillance Intrusion, only one authorization group per system can be active for a user at any given time. The most recently assigned privilege in Security Manager will take precedence and be synchronized with Siveillance Intrusion.

Standard Identity and Access Management



Manage newly created or imported identities:

- Manage identities based on the generic standard identity type
- Manage identities across multiple connected Siveillance Intrusion systems
- Manage mobile devices
- Assign credentials
- Assign access and arming / disarming privileges
- Manage and assign security groups
- Import of identities via a CSV file

Note: It is currently possible to assign multiple access privileges associated with different Siveillance Intrusion Advanced / Pro authorization groups to a single identity within Security Manager. However, due to system limitations in Siveillance Intrusion, only one authorization group per system can be active for a user at any given time. The most recently assigned privilege in Security Manager will take precedence and be synchronized with Siveillance Intrusion.

Security Self Service Portal

- Deploy predefined access approval workflow to enable employees' self-service. Configuration of approver and the visibility in the self-service per access group.
- Configure delegations for approvers: 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.

Credential Management

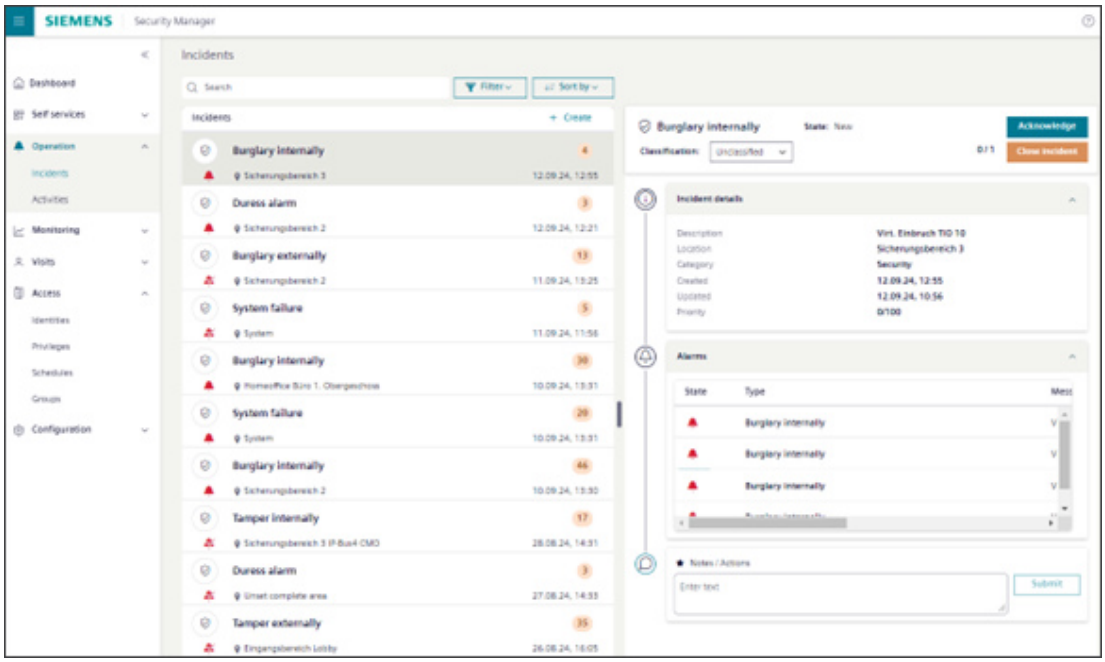
Service Engineer can configure the following:

- 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:

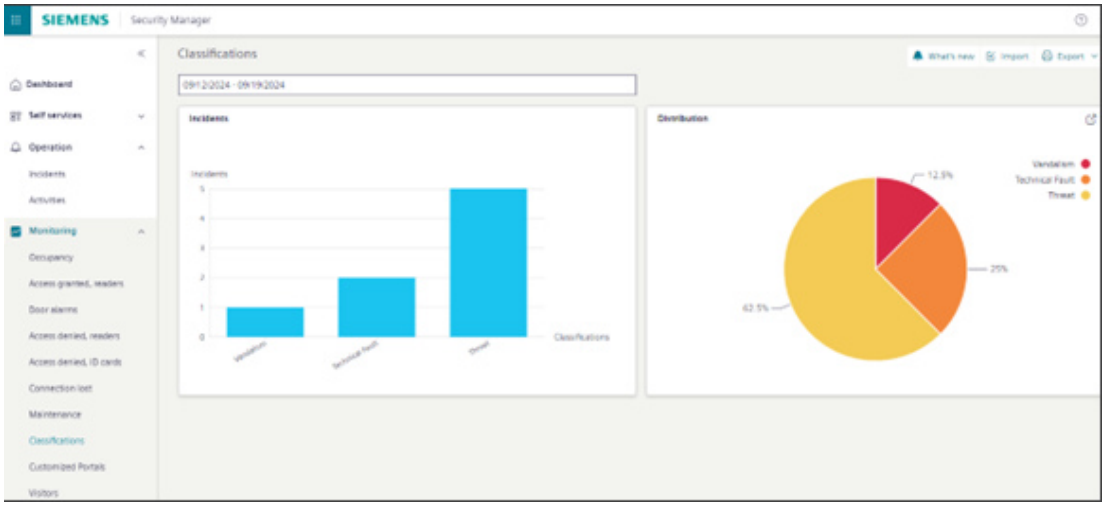
- With the flag „Enable virtual ID card in Building X Access app” the virtual ID card (identity badge) can be enabled or disabled for a specific identity. If it is enabled, the Building X Access app will show the virtual ID card as well as all available digital keys to the user. If it is disabled, the virtual ID card and all digital keys will be hidden, and doors cannot be accessed.

Security Alarm and Task Management



- Combine alarms that occur at the same location into a single security task.

Security Monitoring and Insights Dashboards



- Show classified number of incidents

Connect On-Prem Siveillance Intrusion Systems

Connect to Siveillance Intrusion Advanced and PRO via the Cloud Agent to sync credentials, privileges, identities and push data to Building X point- and alarm vertical.

Keypad NXT Edge

Manage HMI SW for Siveillance Intrusion running on X200, X300 or Connect SW and provide Remote Client functionality via Building X.

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

<table>
<tr><th colspan="5">Security Manager / Intrusion Detection</th></tr>
<tr><th></th><th>Intrusion Detection - Essential</th><th>Intrusion Detection – Standard</th><th>Connectivity – Physical Intrusion Detection System</th><th>Intrusion Detection - Keypad NXT Edge</th></tr>
<tr><td>Precondition</td><td colspan="2">The following subscription must be active:
Connectivity – Physical Intrusion Detection System</td><td colspan="2">-</td></tr>
<tr><td rowspan="2">Functions</td><td colspan="4">User management
Activity Log</td></tr>
<tr><td>Essential Identity and access / arming & disarming management</td><td>● Standard Identity and access / arming & disarming management
● Security Self Service Portal
● Membership review for Security Groups
● Credential management Security Alarm and Task Management
● Security Monitoring and Insights Dashboards</td><td>Connect On-Prem Siveillance Intrusion Systems</td><td>Keypad NXT Edge</td></tr>
<tr><td>Subscription metric</td><td colspan="4">per 1 intrusion area per year
The subscription plan can be purchased in packages of 1 intrusion area</td></tr>
<tr><td>Subscription term</td><td colspan="4">Annually, auto-renewal</td></tr>
<tr><td>Billing term</td><td colspan="4">Annually, payment in advance</td></tr>
<tr><td>Upscale</td><td colspan="4">Effective immediately, pro-rated billing</td></tr>
<tr><td>Downscale / Cancellation</td><td colspan="4">Effective with end of subscription term</td></tr>
<tr><td>Connected Devices</td><td colspan="4">To be purchased separately</td></tr>
<tr><td>Permitted Users</td><td colspan="4">Up to 10,000; Extended Use</td></tr>
</table>

The Security Manager / Intrusion Detection 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 intrusion areas, 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
Siveillance Intrusion Advanced	Siveillance Intrusion detection panel Advanced 100 & 200, powered with 230 VAC.
Siveillance Intrusion PRO	Siveillance Intrusion detection panel PRO 300, PRO 400 and PRO 800, powered with 230 VAC.

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 Manager / Intrusion Detection Data Sheet	www.siemens.com/buildingx/data-sheet/security-manager-intrusion-detection
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

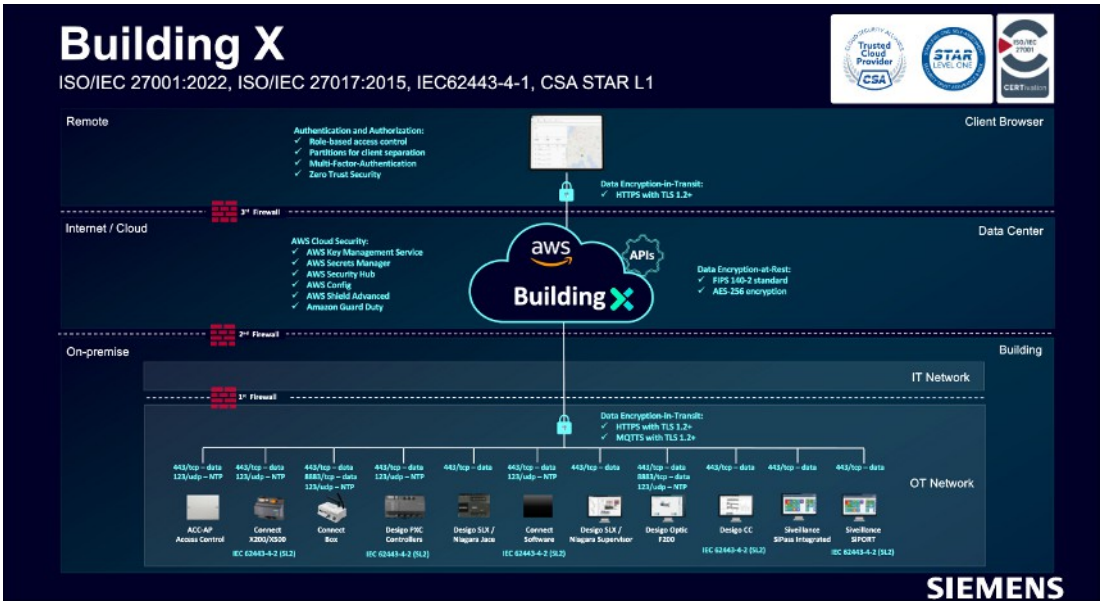
2) Product Documentation under a Custom Subscription Plan

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

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	A6V16055141_en--
Edition	2025-12-16