SIEMENS

Datenblatt

Security Manager



Die Security APIs sind cloud-basierte Angebote innerhalb von Building X, um Identitäten und Zutrittsberechtigungen zu verwalten und um Sicherheitsereignisse und Alarme über APIs auszulesen.

- Building Security Identities and Privileges API
- Monitoring and Insights API
- Building Security Workflow API
- Building Security SCIM API
- Activity Log API

URLs

Entwicklerportal: https://developer.siemens.com/

API Manager: https://eu.buildingx.siemens.com/openness

Funktionen

Security Identities and Privileges API *(Add-on)*

Building Security Identities and Privileges API bietet Zugang zu:

- Identitäten lesen/schreiben
- Leserechte
- Berechtigungen lesen
- Berechtigungen einer Identität zuweisen

Security Monitoring API *(Add-on)*

Die Monitoring and Insights API bietet Zugang zu:

- Eine aggregierte Zählung, wie viele verschiedene Nutzer innerhalb eines bestimmten Zeitraums auf eine bestimmte Ressource zugegriffen haben.

Security Workflow API *(Add-on)*

Die Building Security Workflow API bietet Zugang zu:

- Auflistung und Starten von Sicherheitsworkflows.

Building Security SCIM API *(Add-on)*

Die Security SCIM API bietet Zugang zu:

- Einrichtung und Löschung von Identitäten über eine SCIM-Benutzeroberfläche (z. B. MS Azure ID)

Aktivitäten-API *(Add-On)*

Die Activity Log API bietet Zugang zu:

- Aktivitäten lesen

Building X Platform *(alle Add-ons)*

Accounts App

Möglichkeit zur Verwaltung von Benutzern mit rollenbasierter Zugriffskontrolle. Neue Benutzer können zur Nutzung des Cloud-Dienstes eingeladen und über Benutzergruppen mit den entsprechenden Zugriffsrechten versehen werden. Benutzer können sich mit Zwei-Faktor-Authentifizierung anmelden und ihr Benutzerkonto selbst verwalten. Daten können logisch in Partitionen gruppiert und über Benutzergruppen zugänglich gemacht werden.

Devices App

Ermöglicht die Verwaltung von Connected Devices, die mit dem Cloud-Dienst kompatibel sind.

Data Setup App

Ermöglicht, Daten durch Hinzufügung von Bedeutung und Struktur anzureichern. Die Daten können aus verschiedenen Quellen wie Connected Devices, Cloud-Systemen von Drittanbietern und Dateien übernommen werden.

Datenhosting und Datennutzung

Hostet und verarbeitet persönliche und nicht-persönliche Daten in Rechenzentren in Europa. Informationen zur Verarbeitung personenbezogener Daten und zu den Standorten finden Kunden in den Datenschutzbestimmungen: https://siemens.com/dpt

Developer Portal

Das Xcelerator Developer Portal bietet einen Überblick über alle verfügbaren APIs, Tutorials und die zugehörige OpenAPI v3-Spezifikation. Kunden mit den erforderlichen Abos können die APIs nutzen. Link: https://developer.siemens.com/

API Manager App

Die API Manager bietet (i) die Möglichkeit, die Anmeldedaten der Maschinenbenutzer zu verwalten, um den Zugriff auf die Benutzer APIs zu ermöglichen, (ii) einen Überblick über die API-Nutzung und (iii) die Möglichkeit, die API auszuprobieren.

Abo

Der Aboplan richtet sich nach der Vereinbarung zwischen der Kundschaft und Siemens.

1) Default-Abopläne, falls die Kundschaft das Abo über den Siemens Online-Shop kauft

	Security Identities and Privileges API - Add-on
Voraussetzung	Für die Verwendung der API müssen das folgende Abos aktiv sein: ● Connectivity – Physical Access Control Systems (PACS) und ● Physical Identity & Access Management (PIAM)
Bedingungen	
Abometriken	pro 6 Mill. API-Aufrufe pro Jahr
Abodauer	Jährliche, automatische Verlängerung
Abrechnungszeit	Jährlich, Vorauszahlung
Upscaling	Gültig ab sofort, anteilige Abrechnung
Downscaling/Kündigung	Gültig zum Ende der Abolaufzeit
Angeschlossene Geräte	Separat zu erwerben
Zugelassene Benutzer	Bis zu 10.000; Erweiterte Nutzung

	Security Monitoring API - Add-on
Voraussetzung	Für die Verwendung der API müssen das folgende Abos aktiv sein: ● Connectivity – Physical Access Control Systems (PACS) und ● Sicherheitsüberwachung und Insights Dashboards
Bedingungen	
Abometriken	pro 6 Mill. API-Aufrufe pro Jahr
Abodauer	Jährliche, automatische Verlängerung
Abrechnungszeit	Jährlich, Vorauszahlung
Upscaling	Gültig ab sofort, anteilige Abrechnung
Downscaling/Kündigung	Gültig zum Ende der Abolaufzeit
Angeschlossene Geräte	Separat zu erwerben
Zugelassene Benutzer	Bis zu 10.000; Erweiterte Nutzung

	Security Workflow API - Add-on
Voraussetzung	Für die Verwendung der API müssen das folgende Abos aktiv sein: ● Connectivity – Physical Access Control Systems (PACS) und ● Sicherheits-Selbstverwaltungsportal
Bedingungen	
Abometriken	pro 6 Mill. API-Aufrufe pro Jahr
Abodauer	Jährliche, automatische Verlängerung
Abrechnungszeit	Jährlich, Vorauszahlung
Upscaling	Gültig ab sofort, anteilige Abrechnung
Downscaling/Kündigung	Gültig zum Ende der Abolaufzeit
Angeschlossene Geräte	Separat zu erwerben
Zugelassene Benutzer	Bis zu 10.000; Erweiterte Nutzung

	Security SCIM API - Add-on
Voraussetzung	Für die Verwendung der API müssen das folgende Abos aktiv sein: ● Connectivity – Physical Access Control Systems (PACS) und ● Physical Identity & Access Management (PIAM)
Bedingungen	
Abometriken	pro 6 Mill. API-Aufrufe pro Jahr
Abodauer	Jährliche, automatische Verlängerung
Abrechnungszeit	Jährlich, Vorauszahlung

	Security SCIM API - Add-on
Upscaling	Gültig ab sofort, anteilige Abrechnung
Downscaling/Kündigung	Gültig zum Ende der Abolaufzeit
Angeschlossene Geräte	Separat zu erwerben
Zugelassene Benutzer	Bis zu 10.000; Erweiterte Nutzung

	Aktivitäten-API – Add-On
Voraussetzung	Um die API verwenden zu können, muss ein Building X-Abo aktiv sein.
Bedingungen	
Abometriken	pro 6 Mill. API-Aufrufe pro Jahr
Abodauer	Jährliche, automatische Verlängerung
Abrechnungszeit	Jährlich, Vorauszahlung
Upscaling	Gültig ab sofort, anteilige Abrechnung
Downscaling/Kündigung	Gültig zum Ende der Abolaufzeit
Angeschlossene Geräte	Separat zu erwerben
Zugelassene Benutzer	Bis zu 10.000; Erweiterte Nutzung

Das Abo für Security API entspricht dem regulären, skalierbaren Angebot für diesen Cloud-Dienst. Die Abolaufzeit beträgt zwölf (12) Monate mit automatischer Verlängerung; die Gebühr für den Cloud-Dienst wird im Voraus bezahlt. Für das Abo kann jederzeit ein Upgrade erworben werden, wobei die Gebühren anteilig berechnet werden. Zu Ende der aktuellen Abolaufzeit kann der Cloud-Dienst auch herabgestuft werden. Die Abogebühr wird an den kommenden Abrechnungszeitraum angepasst. Der Cloud-Dienst kann jederzeit mit Wirkung zum Ende der aktuellen Abolaufzeit gekündigt werden.

2) Benutzerdefiniertes Abo

Abos, die nicht im Siemens Online-Shop gekauft werden, sind benutzerdefinierte Abos. Im Rahmen eines benutzerdefinierten Abos werden die Details zu Funktionen, Abo-Metrik, Laufzeit, Abrechnung, Up- und Downscaling, verbundenen Geräten sowie zugelassenen Identitäten in der Vereinbarung zwischen dem Kunden und Siemens festgelegt.

In speziellen Fällen, wie z. B. bei sehr großen Standorten, kann die Kundschaft das Verkaufspersonal für ein benutzerdefiniertes Abo kontaktieren

Voraussetzungen

Unterstützte verbundene Geräte

Der Cloud-Dienst ist zur Zeit mit den handelsüblichen verbundenen Geräten von Siemens kompatibel. Connected Devices ermöglichen dem Cloud Service den Datenaustausch mit der technischen Gebäudeinfrastruktur. Im Folgenden finden Sie eine Beschreibung der verfügbaren Connected Devices.

	Liste von unterstützten verbundenen Geräten
SIEMENS: SiPass	**SiPass mit Sync Agent 2.x** Unterstützte Versionen sind SiPass MP 2.95 HF11 oder höher und SiPass 3.0 IR05 oder höher. **Funktionen von Sync Agent 2.x** ● Synchronisierung von Identitäten ● Synchronisierung von Berechtigungen und Berechtigungszuweisungen ● Synchronisierung physischer und virtueller Zugangsdaten ● Hochladen von Ereignissen und Alarmen ● Veröffentlichung von Türgruppen, Zugangspunkten, Eingabepunkten und Ausgabepunkten in „Data Setup“ ● Virtuelle Zuweisung von Anmeldedaten vom Security Manager an SiPass **Einschränkungen**

	Liste von unterstützten verbundenen Geräten
	● Profilbilder stehen über den ersten Profilbild-Export zur Verfügung. Nachträgliche Änderungen an Profilbildern und neu zugewiesene Profilbilder werden nicht automatisch synchronisiert. ● Änderungen an Türsätzen, Zugangspunkten, Eingabepunkten, Ausgabepunkten und neu hinzugefügten Geräten werden nach der ersten Veröffentlichung nicht mit „Data Setup“ synchronisiert. ● Berechtigungen müssen in SiPass vergeben werden. In Security Manager erstellte Berechtigungen werden nicht mit SiPass synchronisiert. **SiPass mit Sync Agent 3.x** Unterstützte Versionen sind SiPass 2.95 IR23 oder höher und SiPass 3.0 IR05 oder höher. **Funktionen von Sync Agent 3.x** ● Synchronisierung von Identitäten ● Synchronisierung von Zugriffsgruppen und Berechtigungszuweisungen ● Synchronisierung physischer und virtueller Zugangsdaten ● Hochladen von Ereignissen und Alarmen ● Virtuellen Zertifikat herunterladen ● Veröffentlichung von Türgruppen, Zugangspunkten, Eingabepunkten und Ausgabepunkten in „Data Setup“ **Einschränkungen** ● Zugriffsgruppen werden im Security Manager verwaltet und sind nach der Einbindung in SiPass schreibgeschützt. ● Profilbilder stehen über den ersten Profilbild-Export zur Verfügung. Nachträgliche Änderungen an Profilbildern und neu zugewiesene Profilbilder werden nicht automatisch synchronisiert. ● Änderungen an Türsätzen, Zugangspunkten, Eingabepunkten, Ausgabepunkten und neu hinzugefügten Geräten werden nach der ersten Veröffentlichung nicht mit „Data Setup“ synchronisiert. **Unterstützte Kartenlesegeräte** Die folgenden Kartenlesegeräte wurden für die Verwendung mit der SiPass-Integration validiert: ● 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 Die oben aufgeführten Lesegeräte sind geprüft und werden unterstützt. Möglicherweise sind auch weitere von SiPass unterstützte Lesegeräte kompatibel. Einzelheiten finden Sie in den SiPass-Versionshinweisen. Einzelheiten zur Kompatibilität mit der Funktion für virtuelle Berechtigungsnachweise finden Sie im Security Manager / Mobile Access Datenblatt: www.siemens.com/buildingx/data-sheet/security-manager-mobile-access.
SIEMENS: SIPORT	**SIPORT mit Sync Agent 2.x** Das Softwareprodukt SIPORT läuft auf Windows-Computerhardware. Unterstützte Versionen sind SIPORT V3.5.0.134 oder höher SIPORT 4.0 oder höher. **Funktionen von Sync Agent 2.x** ● Synchronisierung von Identitäten (Name, E-Mail-Adresse und Kennzeichen für virtuelle Zugangsdaten)

	Liste von unterstützten verbundenen Geräten
	● Synchronisierung von Berechtigungen und Berechtigungszuweisungen ● Synchronisierung physischer und virtueller Zugangsdaten ● Hochladen von Ereignissen und Alarmen ● Virtuellen Zertifikat herunterladen ● Veröffentlichung von Türgruppen, Zugangspunkten, Eingabepunkten und Ausgabepunkten in „Data Setup“ **Einschränkungen** ● Die Profilbilder der Karteninhaber stehen über den ersten Profilbild-Export zur Verfügung. ● Nachträgliche Änderungen an Profilbildern und neu zugewiesene Profilbilder werden nicht automatisch synchronisiert. ● Änderungen an Türsätzen, Zugangspunkten, Eingabepunkten, Ausgabepunkten und neu hinzugefügten Geräten werden nach der ersten Veröffentlichung nicht mit „Data Setup“ synchronisiert. **Unterstützte Kartenlesegeräte** Die folgenden Kartenlesegeräte wurden für die Verwendung mit der SIPORT-Integration validiert: ● Autec: XMP-TMC2150, XMP-TMC2160, XMP-TMC2170, XMP-TMC2180, XMP-TMC2357, XMP-TMC2367, XMP-TMC2457-UP, XMP-TMC3050, XMP-TMC3060, XMP-TMC3070, XMP-TMC3080 Einzelheiten zur Kompatibilität mit der Funktion für virtuelle Berechtigungsnachweise finden Sie im Security Manager / Mobile Access Datenblatt: www.siemens.com/buildingx/data-sheet/security-manager-mobile-access.
SALTO Nebula	Zu den unterstützten SALTO Nebula-Geräten gehören elektronische Zylinder, Vorhängeschlösser, Rosetten, Smart-Schlösser, Wandleser, motorisierte Schlösser und Geräte zur Kartenaktualisierung, darunter: Neo Cylinder, Neoxx-Vorhängeschloss, XS4 Original+, XS4 One, XS4 One S, XS4 Mini, DBolt, DLok, Wandlesegeräte (einschließlich BLUEnet-Controller) und NCoder Nebula. **Einschränkung** Der PIN-basierte Zugriff wird derzeit vom Security Manager nicht unterstützt. Daher können die Funktionen des Tastenfelds nicht über den Security Manager konfiguriert oder verwaltet werden. : Es werden nur Schlösser ohne Tastenfeld unterstützt, da der Security Manager noch keine PIN-Funktionalität bietet.. **Hinweis**: Die Hardwarekonfiguration wurde in die SALTO Nebula-Anwendung verlagert. Die Inbetriebnahme der Geräte und die gerätespezifischen Einstellungen müssen in SALTO Nebula konfiguriert werden und werden nicht vom Security Manager verwaltet. Die aktuelle Liste der unterstützten SALTO Nebula-Geräte finden Sie unter: https://support.saltosystems.com/nebula/user-guide/installer/device-overview/

Um den Cloud-Service nutzen zu können, muss ein angeschlossenes Gerät vor Ort installiert, voll funktionsfähig und mit dem Internet verbunden sein. Der Kunde ist für die Bereitstellung des Connected Device vor Ort und alle damit verbundenen Kosten für die Bereitstellung des Cloud-Dienstes in Übereinstimmung mit der zugehörigen Dokumentation für das Connected Device verantwortlich.

Webbrowser und Anzeigegeräte

Für die Nutzung des Cloud-Dienstes wird Chrome empfohlen, aber auch andere Standardbrowser können eingesetzt werden. Für ein optimales Benutzererlebnis wird eine Bildschirmauflösung von 1920 x 1080 Pixel oder höher empfohlen.

Internetverbindung
Die Bandbreite der Internetverbindung des Kunden bestimmt die Leistung des Cloud-Dienstes.

Bestellung

Um den Cloud-Dienst zum ersten Mal zu bestellen, muss die Kundschaft ein Angebot von seinem Siemens-Vertriebspartner anfordern.

Produktdokumentation

1) Produktdokumentation im Rahmen eines Standardabos

Allgemeine Vertragsdokumente	Links
Building X - Security API Datenblatt	www.siemens.com/buildingx/data-sheet/de/security-apis
Ergänzende Richtlinien für Gebäudeprodukte	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
Zu akzeptierende Nutzungsrichtlinien von Siemens	https://www.siemens.com/si/cloud/terms
Min. Nutzungsbedingungen	www.siemens.com/buildingx/data-sheet/minimum-terms
Datenschutzbestimmungen	https://www.siemens.com/dpt/si
Datenschutz Anhang	https://www.siemens.com/dpt/si
EU Data Act	https://www.siemens.com/buildingx/terms

2) Produktdokumentation im Rahmen eines Benutzerdefinierten Abos

Die Vertragsdokumente und die Produktdokumentation werden im Angebot von Siemens an die Kundschaft aufgeführt.

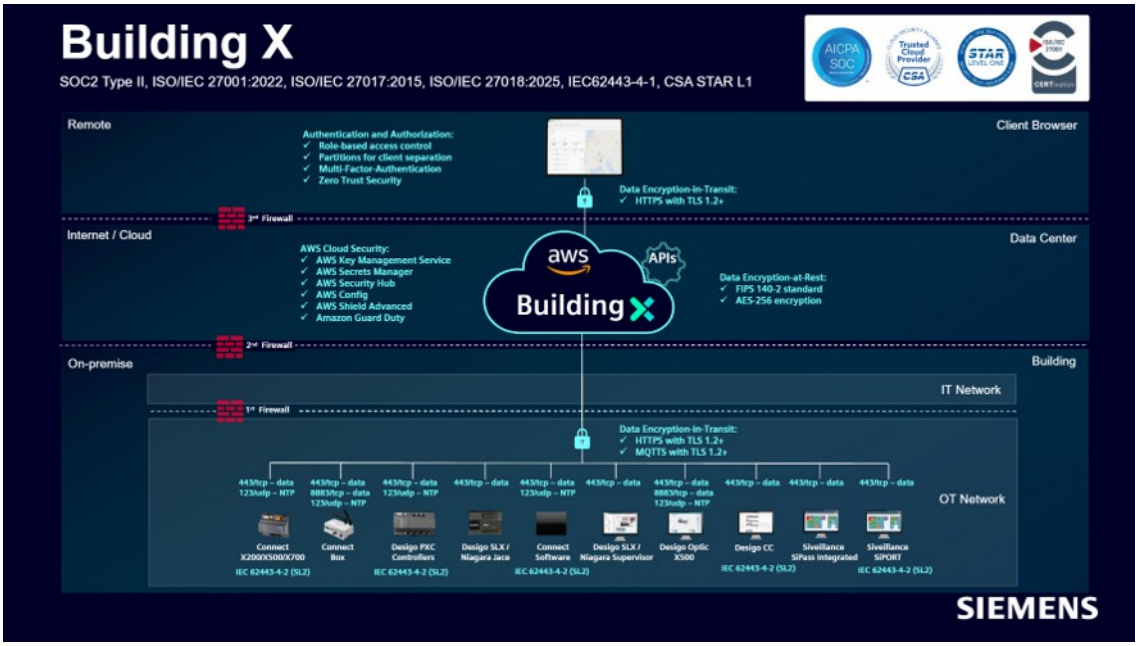
3) Technische Dokumente

Technische Dokumente	Link
Building X- Online-Hilfe	www.siemens.com/buildingx/sid

4) Compliance

Cybersicherheit	Link
Cyber Security Alliance – STAR Stufe 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 Typ-II-Bericht	Bericht auf Anfrage erhältlich
SOC-3-Bericht	https://www.siemens.com/en-us/system-certificates/si-b/

Topologie



Die Topologie zeigt die Gesamtheit der Möglichkeiten für die Verbindung von Daten mit Gebäude X. Die für diesen digitalen Dienst verfügbaren Optionen finden Sie in der Liste der unterstützten angeschlossenen Geräte und der Softwarekonnektivität von Drittanbietern.

Für die Datenkommunikation zwischen den verbundenen Geräten vor Ort und der Cloud ist eine Internetverbindung erforderlich (von der Kundschaft bereitzustellen).

Spezifische Bedingungen

Verwendung mit hohem Risiko

Die Kundschaft erkennt an und stimmt zu, dass:

a) die Angebote nicht dazu bestimmt sind, für den Betrieb eines Hochrisikosystems oder innerhalb eines Hochrisikosystems verwendet zu werden, wenn das Funktionieren des Hochrisikosystems von dem ordnungsgemäßen Funktionieren der Angebote abhängt; und
b) das Ergebnis der Verarbeitung von Daten durch die Nutzung der Angebote außerhalb der Kontrolle von Siemens liegt.

Service Level Agreement

Siemens wird sich in wirtschaftlich vertretbarem Umfang bemühen, die Cloud Services mit einer jährlichen Betriebszeit von achtundneunzig Prozent (98%) zur Verfügung zu stellen.

Mit Ausnahme von:

a) Geplante Ausfallzeiten, vereinbarte Ausfallzeiten, Routine- und Notfallwartungen,
b) Cyberattacken,
c) öffentliche, fremde und/oder kundeneigene Internet- und Kommunikationsnetze,
d) nicht von Siemens zur Verfügung gestellte Daten, Software, Hardware, Telekommunikation, Infrastruktur, Strom, Build-Packs oder Netzbetriebsmittel,
e) Fahrlässigkeit oder Versagen von Kunden und Nutzern bei der Nutzung des Cloud Service und/oder bei Nichtbeachtung der Anweisungen der veröffentlichten Dokumentation,
f) Systemkonfigurationen und Plattformen, die von Siemens nicht unterstützt werden,
g) Systemadministrationen, Handlungen, Befehle und Dateiübertragungen des Kunden oder Nutzers,
h) Modifikationen oder Änderungen, die nicht von Siemens vorgenommen wurden,
i) unbefugter Zugriff über die Zugangsdaten des Kunden und/oder
j) sonstige Fehler, die außerhalb der zumutbaren Kontrolle von Siemens liegen.

Customer Support

Siemens bietet Helpdesk-Unterstützung. Die Kundschaft kann sich für weitere Informationen an seinen Siemens-Vertriebspartner wenden. Kunden können auch online eine Supportanfrage stellen: https://www.siemens.com/support-request.

Herausgegeben von
Siemens Schweiz AG
Smart Infrastructure
Global Headquarters
Theilerstrasse 1a
CH-6300 Zug
+41 58 724 2424
www.siemens.com/buildingtechnologies

© Siemens 2026
Liefermöglichkeiten und technische Änderungen vorbehalten.

Dokument-ID A6V14152435_de--
Ausgabe 22.09.2026