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

URLs

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

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

Funktionen

Building Security Identities and Privileges API

Die Building Security Identities and Privileges API bietet folgende Zugriffsmöglichkeiten:

- Identitäten lesen/schreiben
- Berechtigungen lesen
- Einer Identität Berechtigungen zuweisen
- Einer Identität Berechtigungsnachweise zuweisen

Building Security Alarms and Events API

Die Building Security Alarms and Events API bietet folgende Zugriffsmöglichkeiten:

- Aktivitäten lesen

Building Security Workflow API

Die Building Security Workflow API bietet Zugang zu:

- Auflisten und Starten von Sicherheits-Workflows

Building Security SCIM API

Die Security SCIM API bietet folgende Zugriffsmöglichkeiten:

- On- und Offboarding von Identitäten über eine SCIM-Schnittstelle (z. B. MS Azure ID)

Building Security Siveillance Intrusion API

Die Security Siveillance Intrusion API bietet Zugang zu:

- Verwaltung von Siveillance Intrusion Advanced / Pro Systemen

Entwicklerportal

Das Entwicklerportal stellt eine Übersicht mit den zur Verfügung stehenden APIs bereit sowie Tutorials, Schnelleinstieg und die Security API-Beschreibung.

API-Management

Mit der App API Manager erhalten Sie (i) die Möglichkeit, Berechtigungsnachweise für Computerbenutzer für den Zugriff auf Sicherheits-APIs zu verwalten, (ii) eine Übersicht über die API-Nutzung und (iii) die Möglichkeit, die API über eine Swagger-Vorlage zu testen.

Datenhosting und Datennutzung

Hostet und verarbeitet personenbezogene und nicht-personenbezogene Daten in Rechenzentren in Europa. Informationen zur Verarbeitung personenbezogener Daten und Orte finden Sie in den Data Privacy Terms.

Abo

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

1) Standard-Aboplan, falls die Kundschaft das Abo über den Siemens Online-Shop kauft

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**
Voraussetzung	Um die API nutzen zu können, muss eines der folgenden Abos aktiv sein: Connectivity – Physical Access Control Systems (PACS), or Connectivity – Cloud-based Access Control **Und** eines der folgenden Abos muss aktiv sein:				Um die API nutzen zu können, muss eines der folgenden Abos aktiv sein: Connectivity - Physical Intrusion Detection System Und eines der folgenden Abos muss aktiv sein:
	• Building Access Essential or Building Access Standard • Physical Identity & Access Management (PIAM)	• Building Access Essential or Building Access Standard • Visitor Management Essential or Visitor Management Standard • Physical Identity & Access Management (PIAM) • Security Alarm & Task Management • Sicherheits-Selbstverwaltungsportal • Sicherheitsüberwachung und Insights Dashboards • Mobiler Zugang - Virtueller Ausweis für Kartenleser • Mobiler Zugang - Zugang mit Berechtigungsnachweis für intelligente Schlösser	• Building Access Standard • Sicherheits-Selbstverwaltungsportal	• Building Access Essential or Building Access Standard • Physical Identity & Access Management (PIAM)	• Intrusion Detection Essential • Intrusion Detection Standard
Funktionen	Benutzerverwaltung Developer Portal API-Management		Developer Portal		Benutzerverwaltung Developer Portal API-Management
	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
Abometriken	pro 6 Mill. API-Aufrufe pro Jahr				
Abodauer	Jährliche, automatische Verlängerung				
Abrechnungszeit	Jährlich, Vorauszahlung				
Upscaling	Gültig ab sofort, anteilige Abrechnung				

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**
Downscaling/Kündigung	Gültig zum Ende der Abolaufzeit				
Angeschlossene Geräte	Separat zu erwerben				
Erlaubte Identitäten	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: Das Softwareprodukt SiPass läuft auf Windows-Computerhardware. Die unterstützte Softwareversion ist SiPass MP2.95 (HF11) oder höher. SiPass enthält mehrere Softwareapplikationen, die im Weiteren als "Software" bezeichnet werden und Gebäudedaten an den Cloud-Dienst übermitteln. Folgende Ereigniszustände werden unterstützt: ● 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 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. Die unterstützte Softwareversion ist SIPORT V3.5.0.127 oder höher und SIPORT 3.4.1.321 oder höher. SIPORT enthält mehrere Softwareapplikationen, die im Weiteren als "Software" bezeichnet werden und Gebäudedaten an den Cloud-Dienst übermitteln. Folgende Ereigniszustände werden unterstützt: ● Autec: XMP-TMC2150, XMP-TMC2160, XMP-TMC2170, XMP-TMC2180, XMP-TMC2357, XMP-TMC2367, XMP-TMC2457-UP, XMP-TMC3050, XMP-TMC3060, XMP-TMC3070, XMP-TMC3080.

	Liste von unterstützten verbundenen Geräten
	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 Elektronikschloss	Neo-Zylinder, Neoxx-Vorhängeschloss, XS4 Original+, XS4 One und XS4 One S (nur Modelle, die HSE unterstützen), XS4 Mini, DBolt. **Einschränkung**: Es werden nur Schlösser ohne Tastenfeld unterstützt, da der Security Manager noch keine PIN-Funktionalität bietet.
SALTO Nebula Gateways	IQ3, IQ3 Mini
SIEMENS: ACC-AP	ACC-AP Folgende Ereigniszustände werden unterstützt: ● 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 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).

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

Allgemeine Vertragsdokumente	Links
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

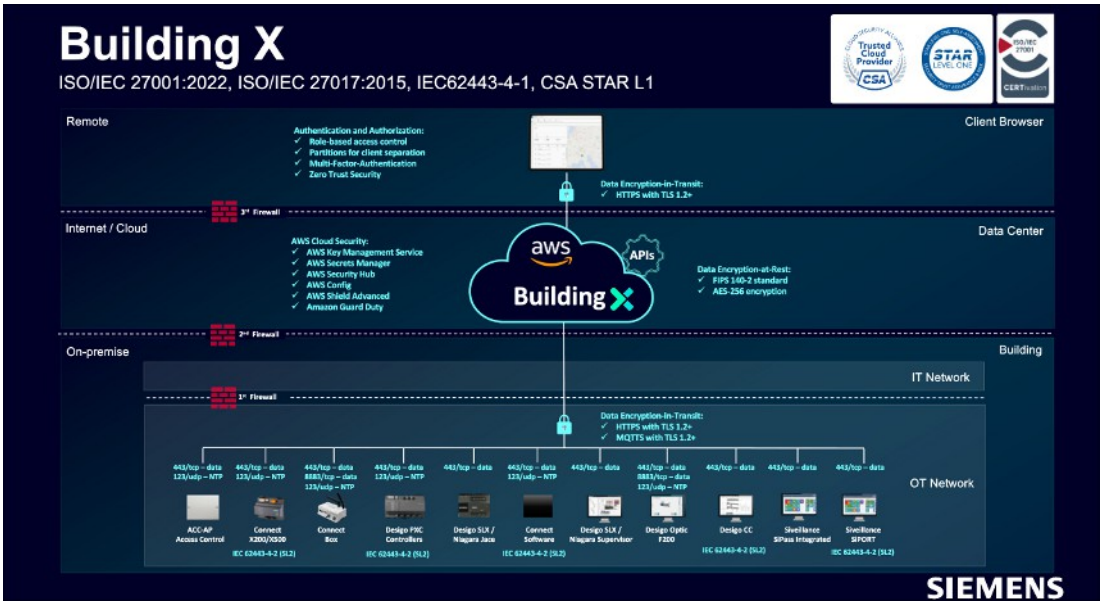
2) Produktdokumentation im Rahmen eines Benutzerdefinierten Abos

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

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 vom ordnungsgemäßen Funktionieren der Angebote abhängig ist; und

b) das Ergebnis der Verarbeitung von Daten durch die Nutzung der Angebote außerhalb der Kontrolle von Siemens liegt.

Servicelevel-Vereinbarung

Siemens ist gehalten, bei einem kommerziell zumutbaren Aufwand die Cloud-Dienste während eines jeden Monats bei einer Laufzeit von 98% verfügbar zu machen.

Ausnahmen:

a) Geplante Ausfallzeiten, vereinbarte Ausfallzeiten, Routine- und Notwartung,
b) Cyberangriffe,
c) öffentliche, Dritt- und/oder Kundschafts-Internet- und Kommunikationsnetzwerke,
d) Daten, Software, Hardware, Telekommunikation, Infrastruktur, Leistung, Build-Packs oder Netzwerkeinrichtungen anderer Hersteller als Siemens,
e) Nachlässigkeit seitens Kundschaft oder Nutzern beim Einsatz der Cloud-Dienste und/oder durch Nichteinhaltung der Anweisungen veröffentlicher Dokumentation,
f) Systemkonfigurationen und Plattformen anderer Hersteller, nicht unterstützt durch Siemens,
g) Systemadministration, Aktionen, Befehle und Dateiübermittlungen von Kundschaft oder Nutzern,
h) Änderungen durch andere Parteien als Siemens,
i) nicht autorisierter Zugriff über Kundenanmeldeinformationen und/oder
j) alle weiteren, beliebigen Ausfälle ausserhalb der Kontrolle von Siemens.

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

Dokument-ID	A6V14152435_de--
Ausgabe	16.12.2025