SIEMENS

Datenblatt

Security Manager

Security Manager / Building Access Add-Ons sind cloudbasierte Angebote innerhalb von Building X, mit denen Zutrittskontrollsysteme durch Cloud-Dienste ergänzt werden.

- Essential Identity and Access Management
- Standard Identity and Access Management
- Sicherheits-Selbstverwaltungsportal
- Berechtigungsnachweis-Management
- Sicherheitsalarm und Aufgabenverwaltung
- Sicherheitsüberwachung und Insights Dashboards
- Drucken und Kodieren von Sicherheitskarten
- Verwalten der Cloud-basierte Zugangskontrolle
- Verbinden Sie ACC-AP Tür-Controller
- Verbinden Sie vor Ort befindliche Zugangskontrollsysteme
- PACS SDK
- Data Setup
- Activity Log

URL

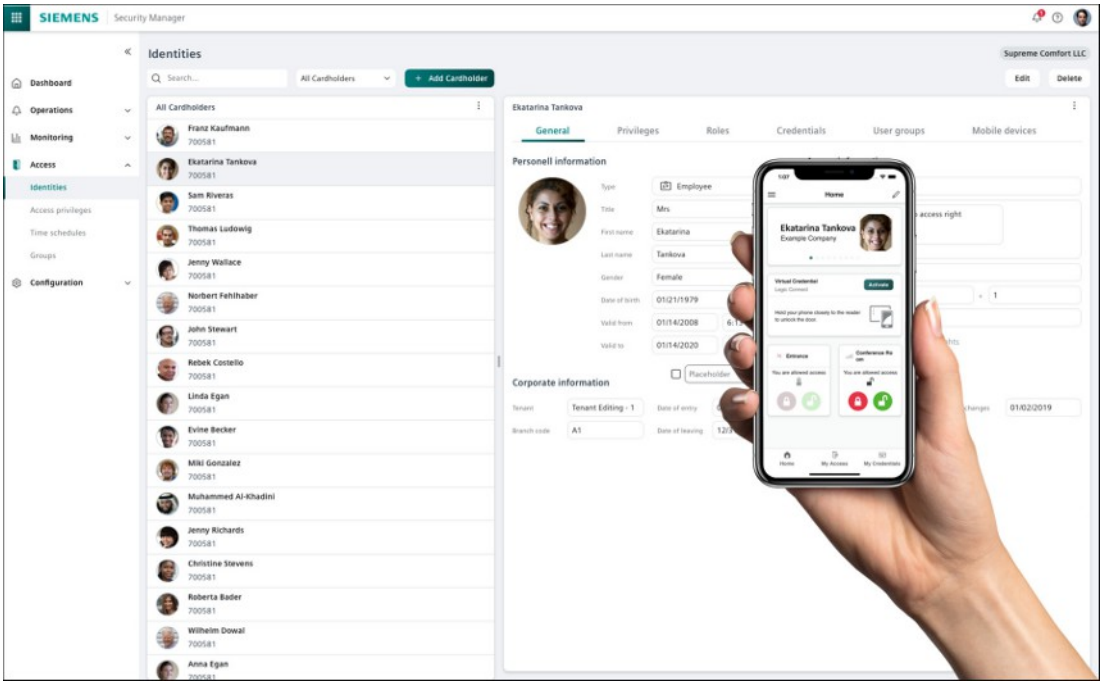
securitymanager.siemens.com

Funktionen

Essential Identity and Access Management

Verwalten Sie Identitäten auf Basis des festgelegten Grundidentitätstyps (einschließlich allgemeiner Identitätsinformationen), weisen Sie Zutrittsberechtigungen und Berechtigungsnachweise zu, verwalten und weisen Sie Sicherheitsgruppen zu und verwalten Sie mobile Geräte.

Standard Identity and Access Management



Verwalten Sie neu erstellte oder importierte Identitäten:

- Verwalten von Identitäten auf der Grundlage des generischen Standardidentitätstyps
- Verwalten von Identitäten über mehrere verbundene PACS-Systeme hinweg
- Verwalten von mobilen Geräte
- Berechtigungsnachweise zuweisen
- Zugriffsberechtigungen zuweisen
- Verwalten und Zuweisen von Sicherheitsgruppen
- Import von Identitäten über eine CSV-Datei
- Definieren Sie einen eindeutigen Identifikator für Identitäten (z. B. Mitarbeiter-ID, E-Mail)

Sicherheits-Selbstverwaltungsportal

- Bereitstellung eines vordefinierten Workflows für die Zugriffsgenehmigung, um die Selbstverwaltung der Mitarbeiter zu ermöglichen. Konfiguration von Genehmigern und der Sichtbarkeit im Self-Service pro Zugangsgruppe.
- Ermöglicht LCB- und DSC-geschulten Ingenieuren die Gestaltung von Self-Service- und anpassbaren Workflows (einschließlich der Gestaltung von Wizard-Formularen über einen UI-Editor) für das physische Identitäts- und Zugangsmanagement. PDF-Dateien können in benutzerdefinierten Workflows verwendet werden. Die Dateien können hochgeladen und in der Antragserstellung, "Meine Anträge" und "Meine Genehmigungen" angezeigt werden.
- Konfigurieren Sie Delegationen für Genehmigende und Anforderer: Für jede Delegation kann eine Dauer konfiguriert werden, ein Enddatum ist optional. Die Delegierten werden per E-Mail informiert, wenn eine Delegation eingerichtet oder aktualisiert wird.
- Selbstbedienungsbenutzer können ganz einfach ein neues Profilbild hochladen und sehen ihr Foto in der Building X Access-App, im Identitätsmanagement und auf gedruckten Zugangsausweisen.

Mitgliedschaftsüberprüfung für Sicherheitsgruppen

Sobald ein Benutzer als Eigentümer einer Sicherheitsgruppe konfiguriert ist, kann die Überprüfung der Mitgliedschaft in den Self-Services gestartet werden. Jede Bewertung wird im Aktivitätsprotokoll und unter Meine Anfragen gespeichert.

Berechtigungsnachweis-Management

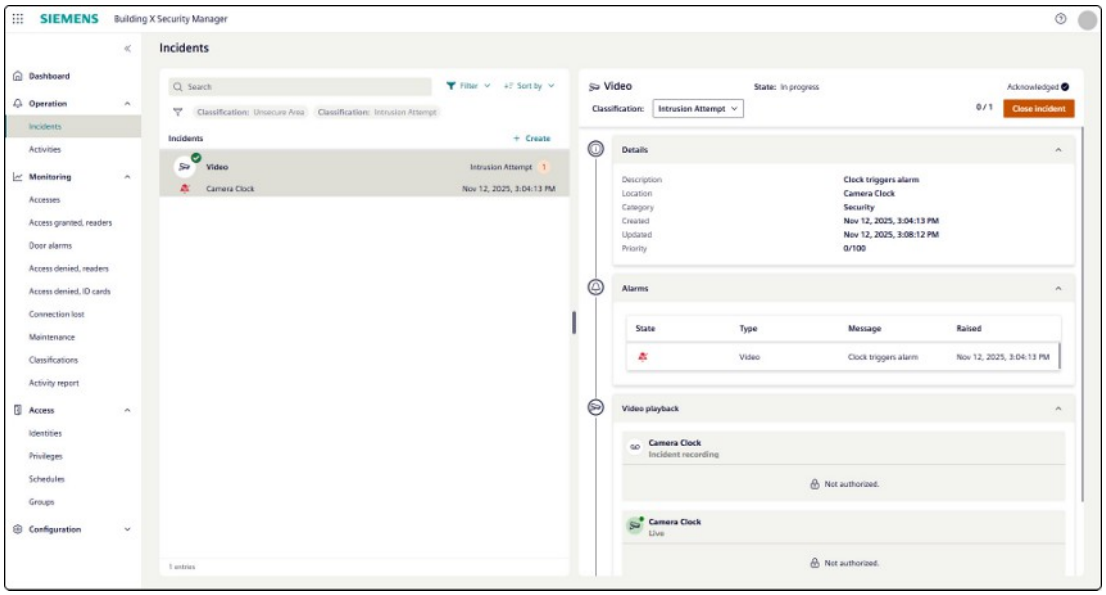
Der Servicetechniker kann Folgendes konfigurieren:

- Wie viele physische Berechtigungsnachweise können einer Identität zugewiesen werden
- Wie viele physische Berechtigungsnachweise können gleichzeitig aktiviert werden

Security Manager kann virtuelle IDs und virtuelle Zugangsdaten aktivieren/deaktivieren:

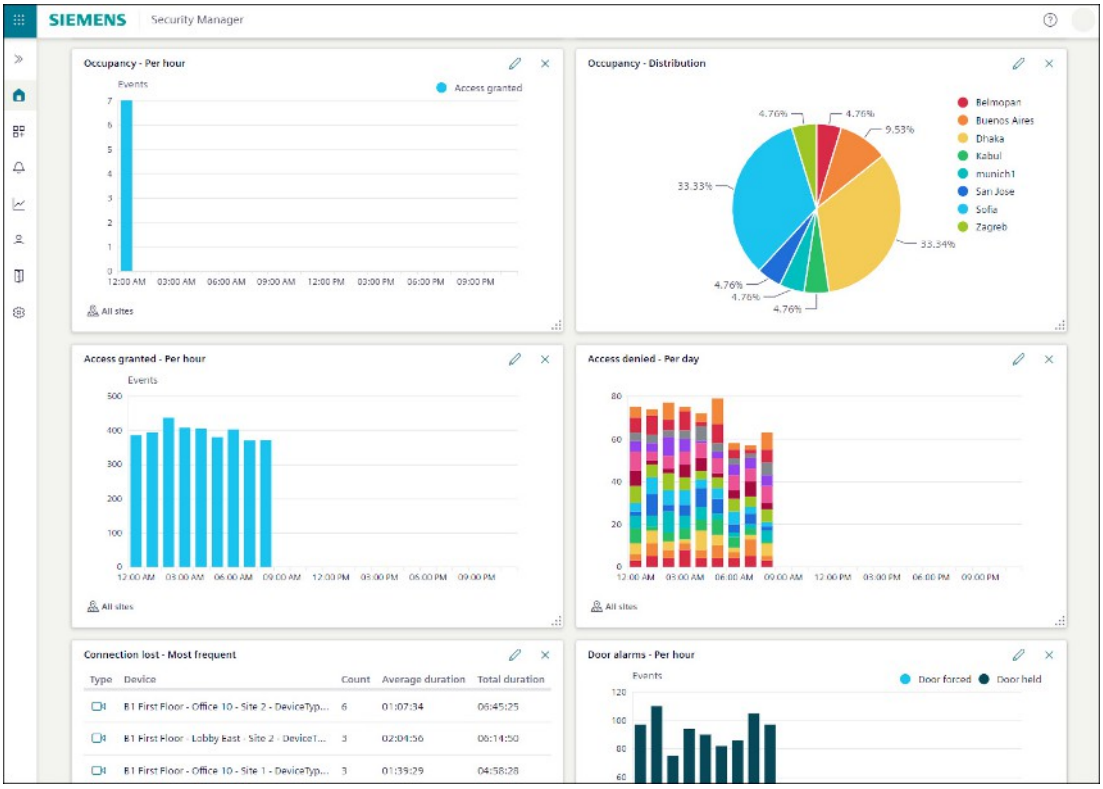
- Mit dem Flag "Enable virtual ID card in Building X Access app" kann die virtuelle ID-Karte (Ausweis) für eine bestimmte Identität aktiviert oder deaktiviert werden. Wenn sie aktiviert ist, zeigt die Building X Access-App dem Benutzer die virtuelle ID-Karte sowie alle verfügbaren digitalen Schlüssel an. Ist sie deaktiviert, werden der virtuelle Ausweis und alle digitalen Schlüssel ausgeblendet, und der Zugang zu den Türen ist nicht möglich.

Sicherheitsalarm und Aufgabenverwaltung



- Bereitstellung von sofort einsetzbaren Standardarbeitsanweisungen (SOPs) zur Lösung von Sicherheitsaufgaben.
- Kombinieren Sie Alarme, die am selben Ort auftreten, zu einer einzigen Sicherheitsaufgabe.
- Warnmechanismus über E-Mail-Benachrichtigung

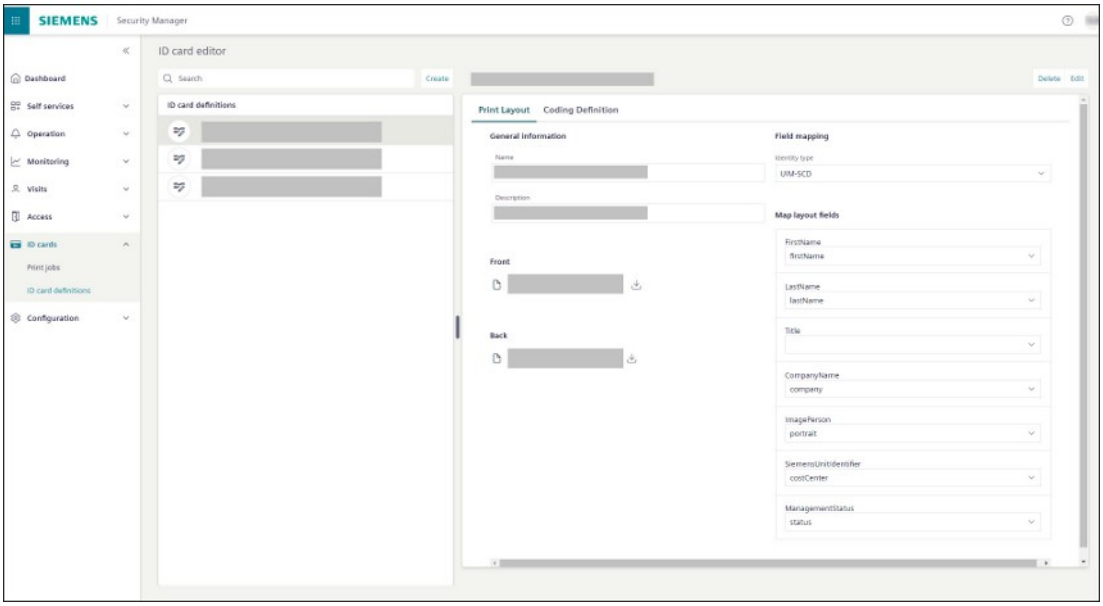
Sicherheitsüberwachung und Insights Dashboards



Erhalten Sie umsetzbare Erkenntnisse auf der Grundlage von Sicherheitsdaten:

- Visualisierung einzelner Zutrittsereignisse pro Gebäude/Standort
- Messung der Raum- oder Gebäudenutzung anhand der Anzahl der "zugangsberechtigten" Veranstaltungen
- Identifizierung von Wartungskandidaten oder Ausreißern bei der Auslastung als Indikatoren für Fehlfunktionen
- Zeigt den Systemstatus für an einen Edge Controller angeschlossene Lesegeräte und angeschlossene Kameras an.
- Automatisierte Berichte über mobile Zugangsdaten und Zugangsereignisse nach Region und Abteilung
- Gemeinsame Nutzung von benutzerdefinierten Dashboards
- Definierte Berichte konfigurieren

Karten drucken und kodieren



Drucken und Kodieren von Karten für die cloudbasierte Zutrittskontrolle mit Tür-Controller(ACC-AP):ACC-AP

- Vordefinierte Kartenlayouts und Kodierungsdefinitionen können von einem Inbetriebnahmetechniker ausgewählt werden.
- Die Kodierungsdefinitionen können von einem Inbetriebnahmetechniker konfiguriert werden.
- Lösen Sie den Druckauftrag über einen Workflow aus.
- Unterstützung der virtuellen SAM-Karte: Kodierung physischer Karten ohne ein physisches Secure Access Module (SAM) zur Speicherung der Schlüssel.

Verwalten der Cloud-basierte Zugangskontrolle

Verwalten Sie ACC-AP-Türsteuerungen in variable variable. Building X Security Manager Verwalten Sie intelligente Schlösser aus der SALTO XS+ Systemfamilie. Verwalten Sie Zugangsberechtigungen, Zeitpläne und Türen. Stellen Sie die SALTO-Cloud-basierten Schlösser auf den Büromodus ein.

Hinweis: Bei Verwendung in Kombination mit SALTO-Schlössern gelten die folgenden Grenzwerte:

- Jedes Privileg kann nun bis zu 100 SALTO-Cloud-basierten Schlössern zugewiesen werden.
- Jede Identität kann bis zu 5 Berechtigungen haben, die den Zugang zu bis zu 500 Schlössern ermöglichen.
- Jedes Privileg umfasst einen Zeitplan. (Hinweis: Das Hinzufügen von mehr Zeitplänen pro Privileg reduziert die maximale Anzahl der zuweisbaren Privilegien pro Identität).
- Auf Anfrage kann das Limit auf 20 Privilegien pro Identität erweitert werden, was den Zugriff auf bis zu 2.000 SALTO-Cloud-basierte Schlösser ermöglicht.

Connect ACC-AP Door Controller

Verbinden Sie bis zu 10 Türen mit einem Tür-Controller ACC-AP über Building X Devices.

Verbinden Sie vor Ort befindliche Zugangskontrollsysteme

Anschluss an bis zu 5 SiPass- und SIPORT-Systeme. Anbindung von 3rd Party PACS über das PACS SDK. Exportierte Profilbilder aus SiPass- und SIPORT-Systemen können manuell über den Connection Manager importiert werden.

Hinweis: Sync Agent 2.x kann nicht auf Servern installiert werden, auf denen bereits ein anderer Siemens Building Connect Agent installiert ist.

PACS SDK

Verwenden Sie das PACS SDK, um Zutrittskontrollsysteme von Drittanbietern integrieren zu können.

Data Setup

Reichern Sie Datenpunkte aus der cloudbasierten Zutrittskontrolle mit ACC-AP-Türcontrollern oder aus SiPass/ SIPORT-Systemen über Building X Data Setup an. ACC-AP Building X Data Setup

Activity Log

Der Activity Log bietet eine überprüfbare Dokumentation der prüfungsrelevanten Aktionen, wobei sowohl vom Benutzer initiierte als auch systembedingte Änderungen erfasst werden.

Zu den derzeit verfolgten Aktivitäten gehören:

- Benutzeraktionen innerhalb der Punktvertikalen (z. B. Ändern von Punktwerten)
- Benutzeraktionen innerhalb der Benutzervertikale (z. B. Hinzufügen von Benutzern, Zuweisen von Gruppen)
- Vollständige Aktivitätsprotokolle von Security Manager
- Vollständige Aktivitätsprotokolle von Visitor Manager

Benutzerverwaltung

Bietet rollenbasierte Zugriffskontrolle. Die Kundschaft aktiviert das Abo in der Building X Accounts-Applikation. Benutzer und Rollenzuweisungen werden im Security Manager verwaltet (linker Navigationsbereich, Kategorie: Zutritt, Menübefehl: Identitäten).

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 Manager / Building Access Add-Ons								
	Physical Identity & Access Management (PIAM)	**Sicherheits-Selbstverwaltungsportal**	**Sicherheitsüberwachung und Insights Dashboards**	**Security Alarm & Task Management**	**Verwaltung des Lebenszyklus von Sicherheitskarten**	**Building Access - Essential**	**Connectivity – Physical Access Control Systems (PACS)**	**Connectivity – Cloud-based Access Control**
Voraussetzung	Die folgenden Abos müssen aktiv sein: ● Connectivity – Physical Access Control Systems (PACS) **Oder** die die folgenden Abos müssen aktiv sein: ● Connectivity – Cloud-based Access Control **und** Building Access - Essential					Eines der folgenden Abos muss aktiv sein: ● Connectivity – Physical Access Control Systems (PACS) ● Connectivity – Cloud-based Access Control	-	
Funktionen	Benutzerverwaltung Activity Log							
	Standard Identitäts- und Zugangsmanagement	Sicherheits-Selbstverwaltungsportal Überprüfung der Mitgliedschaft für Sicherheitsgruppen	Sicherheitsüberwachung und Insights Dashboards	Sicherheitsalarm und Aufgabenverwaltung	Drucken und Kodieren von Sicherheitskarten	Essential Identity and access management Verwalten der Cloud-basierte Zugangskontrolle	Verbinden Sie vor Ort befindliche Zugangskontrollsysteme PACS SDK	Connect ACC-AP door controller ACC-AP Data Setup
Abometriken	pro 1 Tür pro Jahr erworben werden Das Abo kann in Paketen von 1 Tür erworben werden							
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 Manager / Building Access Add-Ons 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.

Die Kundschaft kann die erforderlichen, verbundenen Geräte separat erstehen.

Mit einer erweiterten Nutzung kann die Kundschaft Partnern und Drittparteien den Zugriff und die Nutzung der Cloud-Dienste mit den in den Nutzungsbedingungen aufgeführten Rechten gewähren.

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.

Für kundenspezifische Anwendungsfälle wie beispielsweise bei einer sehr hohen Anzahl Türen und Identitäten pro Standort (z. B. mehr als 10.000 Identitäten und/oder 1.000 Türen), kann sich die Kundschaft für ein individuelles Abo an den zuständigen Vertriebspartner wenden.

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. 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.

	Liste von unterstützten verbundenen Geräten
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.

Unterstützte Software-Konnektivität von Drittanbietern

Der Cloud-Dienst ist zur Zeit mit den handelsüblicher Drittanbieter-Software kompatibel. Die Konnektivität für Software von Drittanbietern ermöglicht es dem Cloud-Dienst, Daten mit Software von Drittanbietern auszutauschen. Im Folgenden finden Sie eine Beschreibung der verfügbaren Drittanbieter-Software.

	Liste der unterstützten Software von Drittanbietern
Software-spezifische Verbindungen	● SDK für PACS von Drittanbietern ● Mobile App SDK

Der Kunde ist für die Drittsoftware am Standort und alle damit verbundenen Kosten für die Bereitstellung des Cloud-Dienstes gemäß der zugehörigen Dokumentation für die Drittsoftware 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 Manager / Building Access Add-Ons Datenblatt	www.siemens.com/buildingx/data-sheet/de/security-manager-building-access-add-ons

Allgemeine Vertragsdokumente	Links
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

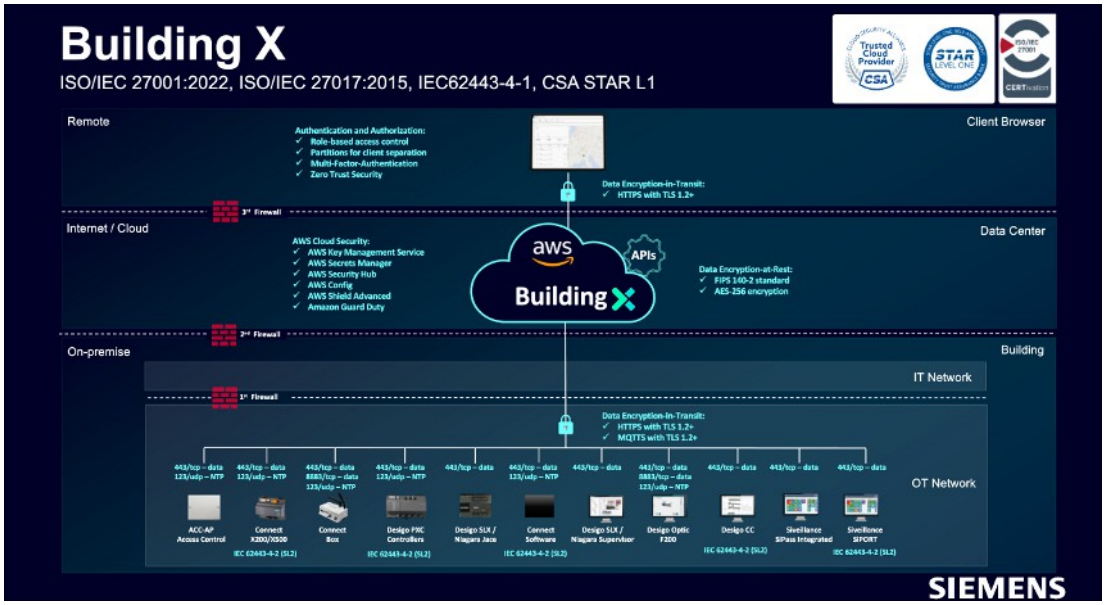
2) Produktdokumentation im Rahmen eines Benutzerdefinierten Abos

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

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 A6V13175246_de--
Ausgabe 16.12.2025