SIEMENS

Datenblatt

Security Manager



Security Manager ist ein cloudbasiertes Angebot innerhalb von Building X, das Zutrittskontrollanlagen um Cloud-Dienste erweitert.

- Identity and Access Management
- PACS-Privileggruppen
- Sicherheits-Selbstverwaltungsportal
- Mitgliedschaftsüberprüfung für Sicherheitsgruppen
- Berechtigungsnachweis-Management
- Sicherheitsüberwachung und Insights Dashboards
- Drucken und Kodieren von Sicherheitskarten
- Verbinden Sie vor Ort befindliche Zugangskontrollsysteme
- PACS SDK
- SALTO Nebula verwalten

buildingx.siemens.com

Funktionen

Anbindung von lokalen Zutrittskontrollanlagen *(Konnektivität – Physikalische Zutrittskontrollanlagen)*

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 *(Connectivity – Physical Access Control Systems (PACS)*

Verwenden Sie das PACS-SDK, um die Integration von Zutrittskontrollanlagen von Drittanbietern freizugeben.

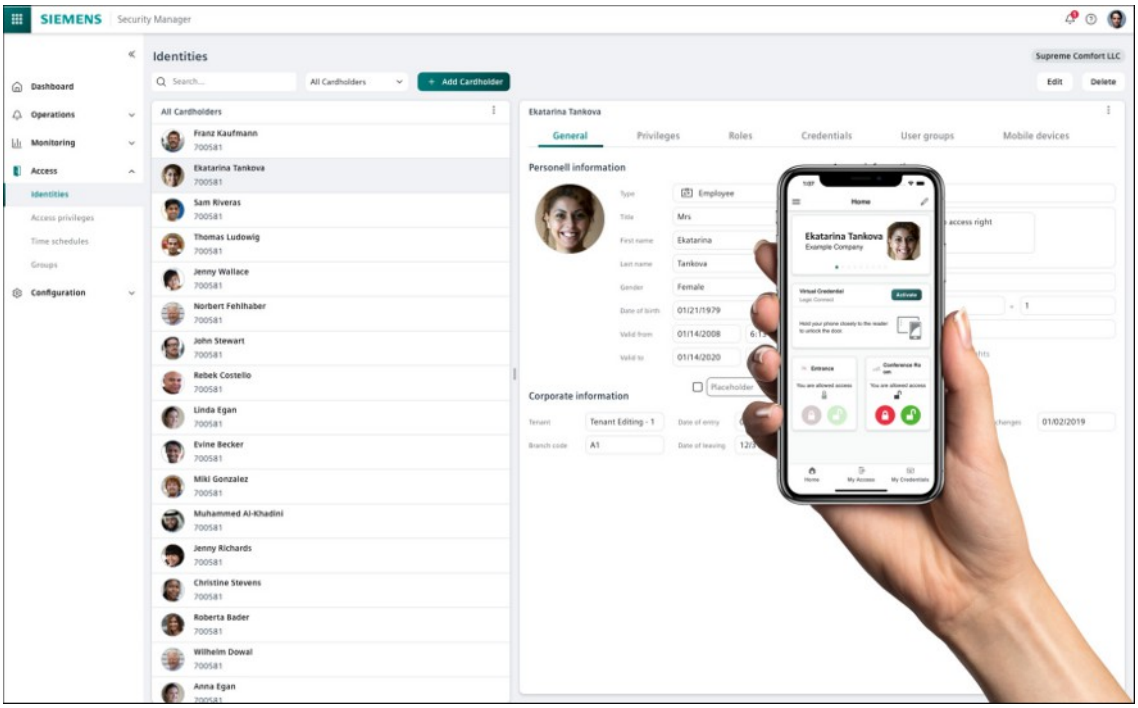
SALTO Nebula verwalten *(Konnektivität – SALTO Nebula Online-/Offline-Zugangspunkt)*

Servicetechniker konfigurieren SALTO-Zugangspunkte und Zugangspunktgruppen mit dem gesamten Funktionsumfang direkt in SALTO Nebula, während der Sicherheitsmanager eine eigene, schreibgeschützte SALTO-Verbindungsansicht für die Zuweisung von Partitionen verwaltet.

Hinweis: Es gelten die folgenden Bedingungen:

- Jedes Berechtigungsrecht kann bis zu 100 cloudbasierten SALTO-Schlössern oder Zugangspunktgruppen oder einer beliebigen Kombination aus beiden zugewiesen werden. Pro Berechtigung wird der Zugriff auf bis zu 10.000 cloudbasierte Schlösser gewährt.
- Jede Identität kann bis zu 5 Berechtigungen umfassen.
- 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 Berechtigungen pro Identität erhöht werden

Identitäts- und Zugriffsmanagement *(Physisches Identitäts- und Zugriffsmanagement)*



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
- Identitäten aktivieren und deaktivieren
- 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)

PACS-Berechtigungsgruppen *(Physikalisches Identitäts- und Zugriffsmanagement)*

SiPass Sync Agent 3.x bestimmt Security Manager als das massgebliche System für die Verwaltung der Zugriffsrechte. Zugriffsgruppen werden von SiPass mit Security Manager synchronisiert und sind in SiPass schreibgeschützt. Alle Zuweisungen und Änderungen müssen im Security Manager vorgenommen werden, wo die Zugriffsgruppen als Security Manager-Gruppen mit den zugehörigen Zugriffsebenen verwaltet werden. Der Sync Agent stellt sicher, dass Änderungen, wie z. B. das Löschen von Gruppen oder leere Gruppen, in SiPass widergespiegelt werden, und sorgt so für eine zentrale, konsistente und aktuelle Verwaltung von Berechtigungen auf allen Systemen.

Zugangsdaten-Verwaltung *(Physical Identity & Access 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.

Sicherheits-Self-Service-Portal *(Sicherheits-Self-Service-Portal)*

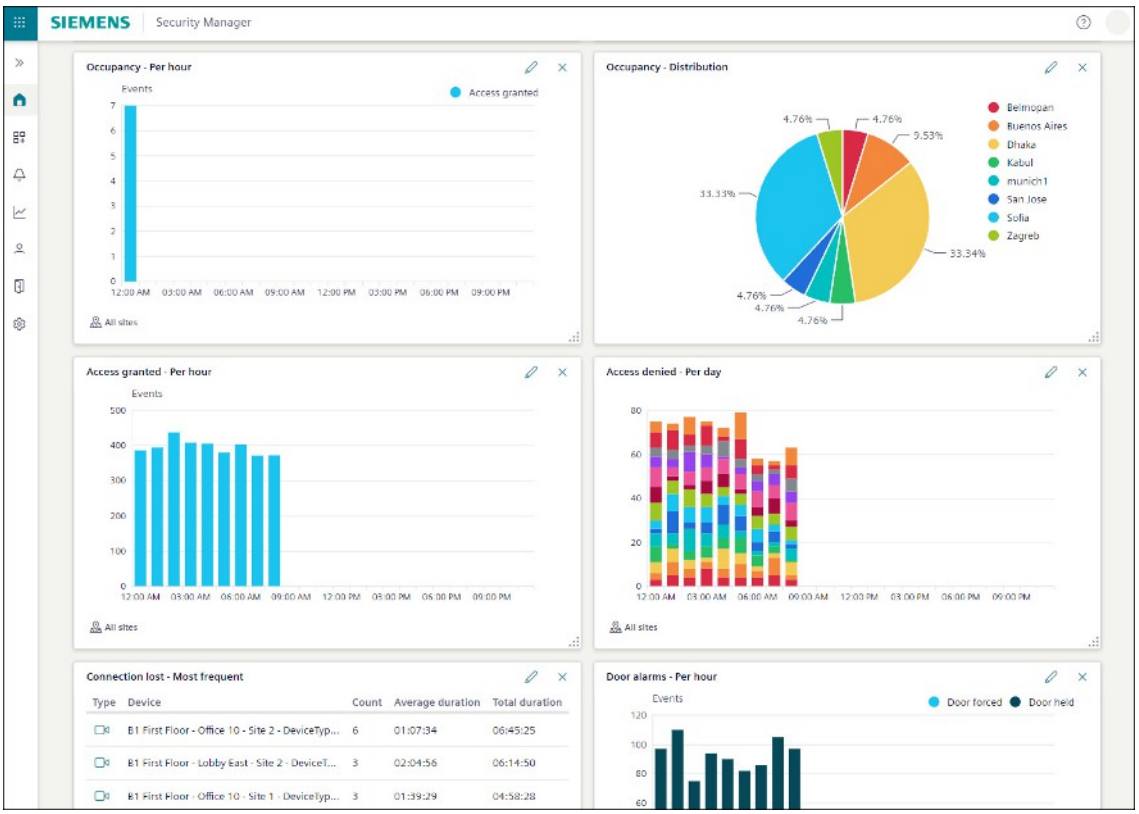
- Bereitstellung eines vordefinierten Workflows für die Zugriffsgenehmigung, um die Selbstverwaltung der Mitarbeiter zu ermöglichen. Konfiguration von Genehmigern und der Sichtbarkeit im Self-Service pro Zugangsgruppe.
- Über den Arbeitsablauf „Karte verloren“ können Benutzer den Verlust ihrer Karte melden, woraufhin diese umgehend deaktiviert wird. Nutzer haben ein Zeitfenster von 5 Tagen, um den Antrag zurückzuziehen und ihre Karte wieder zu aktivieren, falls sie diese wiederfinden. Andernfalls bleiben die Zugangsdaten gesperrt und es müssen neue angelegt werden.

  Selbstbedienungsbenutzer können ganz einfach ein neues Profilbild hochladen und sehen ihr Foto in der Building X Access-App, im Identitätsmanagement und auf gedruckten Zugangsausweisen.
- 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.
- E-Mail-Benachrichtigungen im Workflow halten Antragsteller, Genehmiger und Beauftragte während des gesamten Workflow-Lebenszyklus auf dem Laufenden, indem sie relevante Informationen zum Antrag, Statusaktualisierungen, Genehmigungsentscheidungen und direkten Zugriff auf die entsprechenden Workflow-Aufgaben bereitstellen.
- Ermöglicht LCB- und DSC-geschulten Ingenieuren die Gestaltung von Self-Service- und anpassbaren Workflows (einschließlich der Gestaltung von Wizard-Formularen über einen UI-Editor und gemappten Tabellen) 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.

Überprüfung der Gruppenmitgliedschaft in Sicherheitsgruppen *(Sicherheits-Self-Service-Portal)*

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.

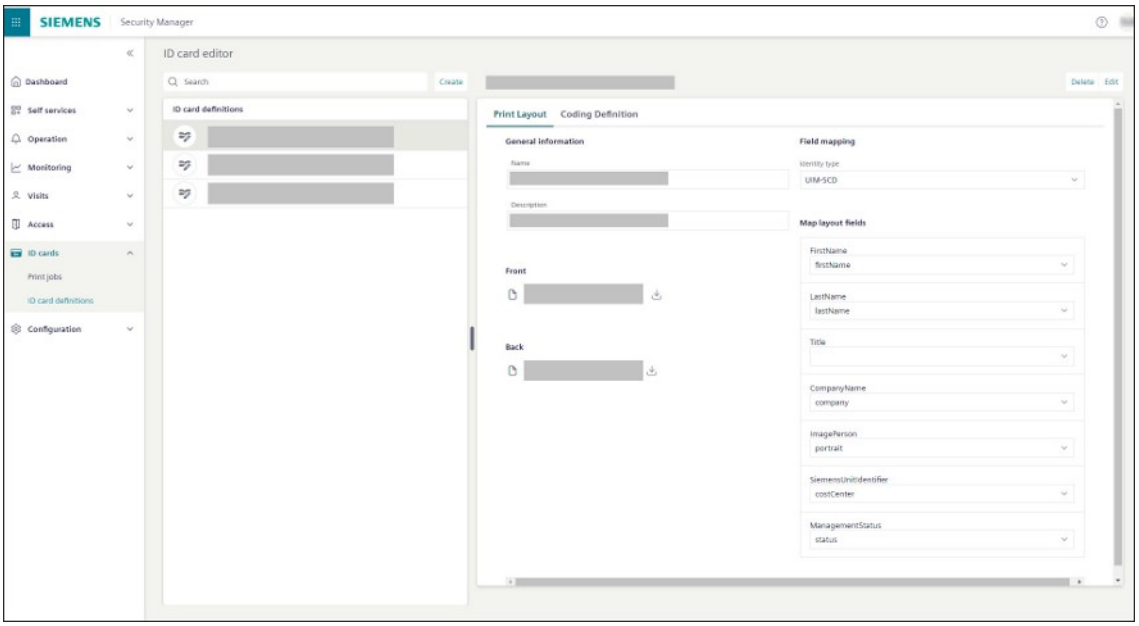
Dashboards für Sicherheitsüberwachung und Einblicke *(Dashboards für Sicherheitsüberwachung und Einblicke)*



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.
- Visualisierung der Verwendung von Berechtigungsnachweisen an Türen/Lesern, um die Beiträge zu gewährten bzw. verweigerten Zutrittsereignissen zu bewerten
- Berichte zur Darstellung des Gesamtvolumens der Ausweisdruck- und Workflow-Anfragen
- Automatisierte Berichte über mobile Zugangsdaten und Zugangsereignisse nach Region und Abteilung
- Zeige die Anzahl der Identitäten und virtuellen Anmeldedaten pro Partition in den Widgets, der Überwachung und den Berichten an
- Widget zum Ablaufstatus von Zugangsdaten und Berichterstellung
- Gemeinsame Nutzung von benutzerdefinierten Dashboards
- Definierte Berichte konfigurieren

Karten drucken und codieren *(Verwaltung des Lebenszyklus von Sicherheitskarten)*



Karten für SiPass, SIPORT und SALTO Nebula drucken und codieren:

- 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.

Building X Platform

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

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

- Legen Sie je nach Bedarf fest, wie lange Aktivitätsprotokolle aufbewahrt werden sollen (z. B. 30, 90, 180 oder 365 Tage).
- Erweiterte Suchfunktionen, darunter strukturierte Filter, Freitextsuche und bedingte Operatoren wie „Gleich“ und „Nicht gleich“, um relevante Aktivitäten in großen Ereignismengen schnell zu finden
- Exportieren Sie Aktivitätsprotokolle in die Formate PDF und XLSX für Berichts-, Offline-Analyse-, Prüfungs- und Compliance-Zwecke unter Verwendung der aktuell ausgewählten Filter

Ask Building X

Ermöglicht es dem Benutzer, mit Hilfe von GenAI Fragen zu technischen Informationen über Building X in verschiedenen Sprachen zu stellen.

Abo

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

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

	Connectivity – Physical Access Control Systems (PACS)
Funktionen	
Verbinden Sie vor Ort befindliche Zugangskontrollsysteme	✓
PACS SDK	✓
Bedingungen	
Abometriken	pro 1 Tür pro Jahr 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

	Konnektivität – SALTO Nebula Online-Zugangspunkt
Funktionen	
SALTO Nebula verwalten	✓
Bedingungen	
Abometriken	pro 1 Tür pro Jahr 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

	Konnektivität – SALTO Nebula Offline-Zugangspunkt
Funktionen	
SALTO Nebula verwalten	✓
Bedingungen	
Abometriken	pro 1 Tür pro Jahr 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

	Physical Identity & Access Management (PIAM)
Voraussetzung	Für die Verwendung mit PACS muss das folgende Abo aktiv sein: Connectivity – Physical Access Control Systems (PACS)
Funktionen	
Building X Platform	✓
Identitäts- und Zugangsmanagement	✓

	Physical Identity & Access Management (PIAM)
PACS-Privileggruppen	✓
Berechtigungsnachweis-Management	✓
Bedingungen	
Abometriken	pro 1 Tür pro Jahr 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

	Sicherheits-Selbstverwaltungsportal
Voraussetzung	Für die Verwendung mit PACS muss das folgende Abo aktiv sein: Connectivity – Physical Access Control Systems (PACS)
Funktionen	
Building X Platform	✓
Sicherheits-Selbstverwaltungsportal	✓
Überprüfung der Mitgliedschaft für Sicherheitsgruppen	✓
Bedingungen	
Abometriken	pro 1 Tür pro Jahr 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

	Sicherheitsüberwachung und Insights Dashboards
Voraussetzung	Für die Verwendung mit PACS muss das folgende Abo aktiv sein: Connectivity – Physical Access Control Systems (PACS)
Funktionen	
Building X Platform	✓
Sicherheitsüberwachung und Insights Dashboards	✓
Bedingungen	
Abometriken	pro 1 Tür pro Jahr 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

	Verwaltung des Lebenszyklus von Sicherheitskarten
Voraussetzung	Für die Verwendung mit PACS muss das folgende Abo aktiv sein:

	Verwaltung des Lebenszyklus von Sicherheitskarten
	Connectivity – Physical Access Control Systems (PACS)
Funktionen	
Building X Platform	✓
Drucken und Kodieren von Sicherheitskarten	✓
Bedingungen	
Abometriken	pro 1 Tür pro Jahr 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 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

Alle Abos, die nicht über einen Online Store von Siemens erworben werden, sind benutzerdefinierte Abos. Bei einem benutzerdefinierten Abo werden die Einzelheiten zu Funktionen, Abometrik, Laufzeit, Abrechnung, Hoch- und Herunterskalierung, angeschlossenen Geräten sowie zulässigen Benutzenden in der Vereinbarung zwischen der Kundschaft und Siemens festgelegt.

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** ● 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:

	Liste von unterstützten verbundenen Geräten
	● 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) ● 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

	Liste von unterstützten verbundenen Geräten
	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.

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

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	www.siemens.com/buildingx/data-sheet/de/security-manager-building-access-add-ons
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.

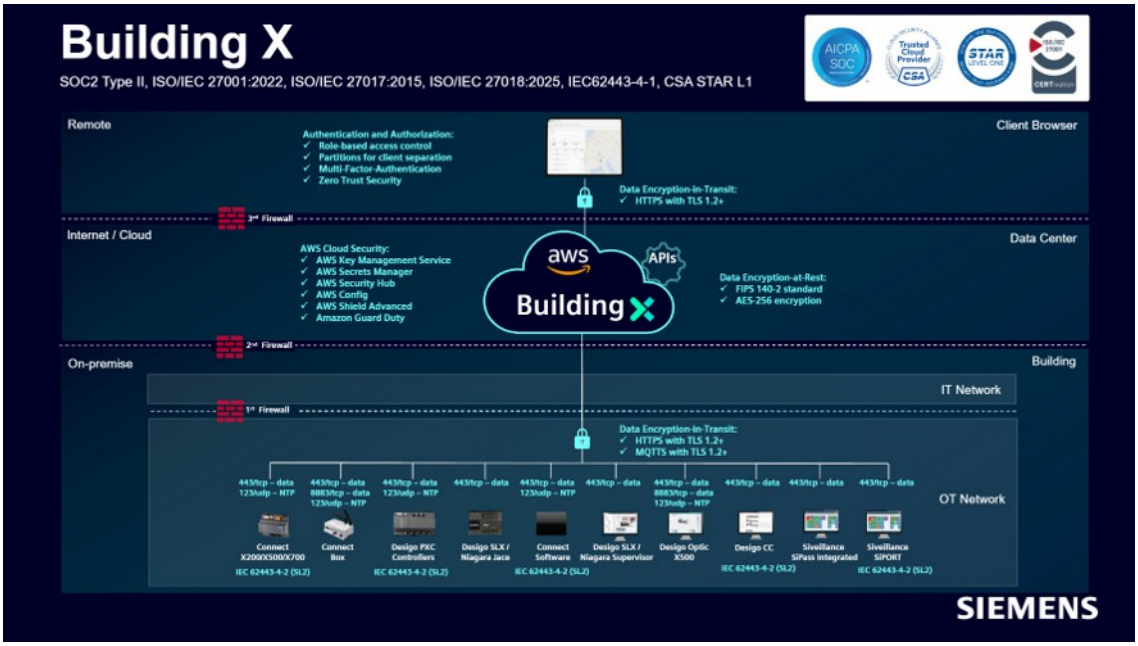
3) Technische Dokumente

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 A6V13175246_de--
Ausgabe 22.09.2026