SIEMENS

Datenblatt

Security Manager - Mobile



Security Manager / Mobile Access ist ein cloud-basiertes Angebot innerhalb von Building X, mit dem Sie Türen mithilfe Ihres Smartphones öffnen können.

- Virtueller Berechtigungsnachweis für Kartenlesegeräte
- Apple Wallet Berechtigungsnachweis
- Google Wallet Berechtigungsnachweis
- Anmeldedaten für SALTO-Zugangspunkte
- Mobile App SDK
- Vor-Ort-Virtual Credentials für SIPORT
- Mobile Ausweisverwaltung
- Foto-Upload
- Verbinden Sie vor Ort befindliche Zugangskontrollsysteme
- SALTO Nebula verwalten

URL

buildingx.siemens.com

iOS: https://apps.apple.com/app/building-x-access/id1483078094

Android: https://play.google.com/store/apps/details?id=com.siemens.accessmobile&hl=gsw

Funktionen

Mobiler Aoo SDK *(Zugang - Virtueller Ausweis für Kartenleser)*

Verwenden Sie das Mobile App SDK, um Funktionen für den mobilen Zugriff in Ihre eigene mobile App zu integrieren

Verwaltung mobiler Zugangsdaten *(Virtual Credential for Card Readers)*

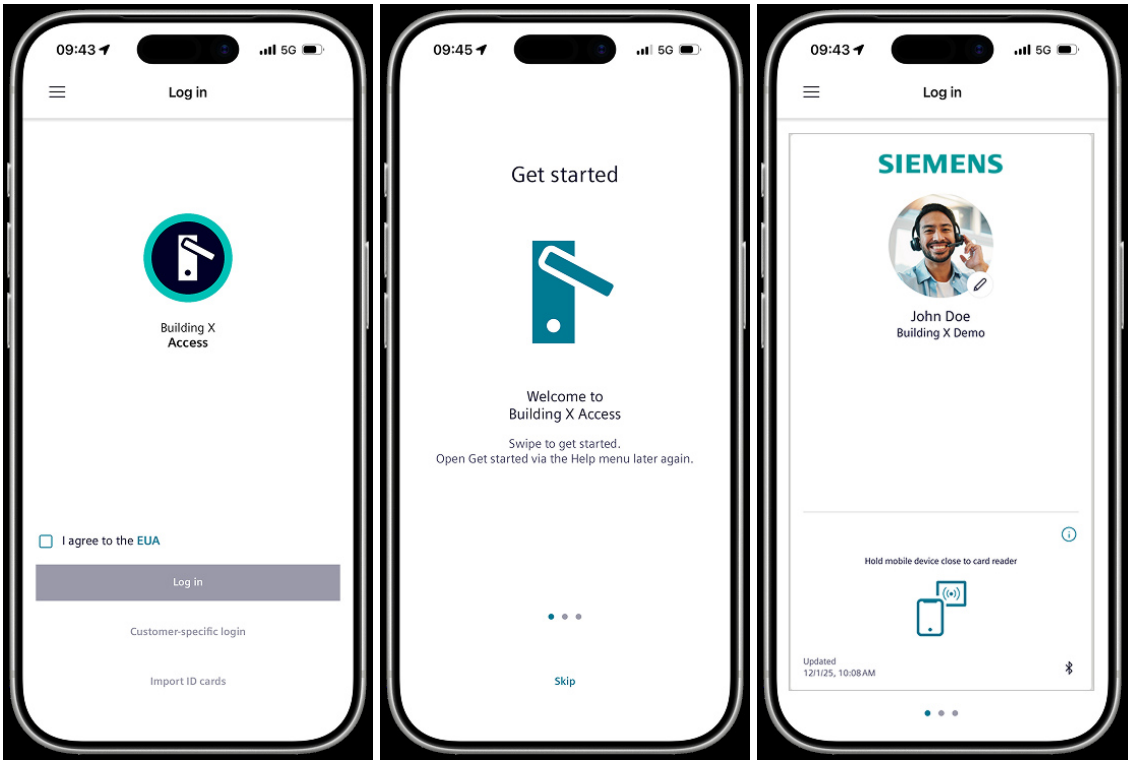
Der Servicetechniker kann Folgendes konfigurieren:

- Wie viele mobile Berechtigungsnachweise können einer Identität zugewiesen werden
- Wie viele mobile Zugangsdaten können gleichzeitig aktiviert werden
- Wie viele mobile Geräte können von einem Nutzer gleichzeitig aktiviert werden, um zusätzliche Kosten zu vermeiden

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.
- Schützen Sie hochsensible Schlüssel, indem Sie den Zugriff und die Konfiguration auf eine dedizierte Benutzerrolle beschränken.

Virtuelle Zugangsberechtigung für Kartenlesegeräte *(Virtual Credential for Card Readers)*



Verwendung des Smartphones des Kunden zum Öffnen von Türen, die durch einen LEGIC Connect-fähigen Kartenleser gesichert sind, der entweder an einen SiPass- oder SIPORT-Controller oder an einen mit der Cloud verbundenen ACC-AP-Türcontroller angeschlossen ist.

Es gelten die folgenden Bedingungen:

- Ein Nutzer kann die Geräte bis zu dreimal pro Jahr ohne zusätzliche Kosten wechseln.
- Die Deaktivierung und Reaktivierung eines Geräts verursacht keine zusätzlichen Kosten.
- Die Meldung eines gestohlenen Geräts und seine Reaktivierung nach dem Wiederauffinden verursachen keine zusätzlichen Kosten.

- Das Deaktivieren und erneute Aktivieren der Option "Virtuelle Berechtigungsnachweise aktivieren" im Sicherheitsmanager / Identitäten erzeugt neue virtuelle Berechtigungsnachweise für alle Geräte des Benutzers, was zu zusätzlichen Kosten führt.

Lokale virtuelle Zugangsdaten für SIPORT *(Virtual Credential for Card Readers)*

Unterstützung von virtuellen Anmeldedaten vor Ort durch Offline-Import für SIPORT-Kunden.

Porträtfoto über das Smartphone hochladen *(virtueller Ausweis für Kartenlesegeräte)*

Mit der Building X Access-App können Nutzer ganz einfach ein neues Profilbild hochladen und ihr Foto in der App, im Identitätsmanagement und auf gedruckten Zugangsausweisen anzeigen lassen.

Anmeldedaten für SALTO-Zugangspunkte *(Anmeldedaten für SALTO-Zugangspunkte)*

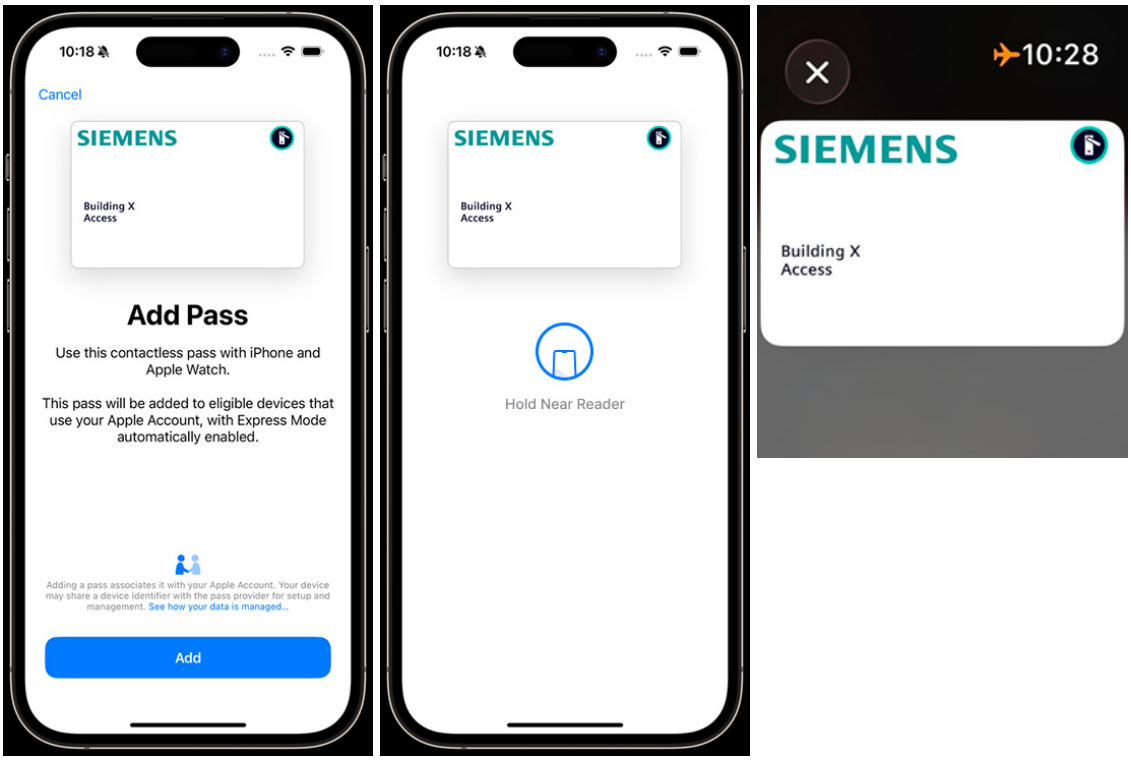
Verwendung des Smartphones des Kunden oder einer physischen Karte zum Öffnen von Türen, die mit SALTO Smartlocks gesichert sind.

Es gelten die folgenden Bedingungen:

- Ein Nutzer kann die Geräte bis zu dreimal pro Jahr ohne zusätzliche Kosten wechseln.
- Die Deaktivierung und Reaktivierung eines Geräts verursacht keine zusätzlichen Kosten.
- Die Meldung eines gestohlenen Geräts und seine Reaktivierung nach dem Wiederauffinden verursachen keine zusätzlichen Kosten.

Apple Wallet-Zugangsdaten *(Apple Wallet-Zugangsdaten)*

iPhone: Apple Watch:



Apple Wallet ermöglicht den sofortigen Zugriff, wenn der Nutzer sein iPhone oder seine Apple Watch in die Nähe eines kompatiblen Kartenlesegeräts hält. Die Verzögerung, die bei Bluetooth Low Energy (BLE) Systemen auftritt, entfällt.

Für die Nutzung des Dienstes mit Apple Wallet sind zusätzliche Geschäftsbedingungen erforderlich, die im Voraus unterzeichnet werden müssen. Für weitere Informationen wenden Sie sich bitte an request.securitymanager.si@siemens.com.

Google Wallet-Anmeldedaten *(Google Wallet-Anmeldedaten)*

Android-Nutzer können ihre Zugangsdaten zu Google Wallet hinzufügen und Türen direkt vom Sperrbildschirm aus öffnen, ohne die Building X starten oder gar geöffnet lassen zu müssen, während Sicherheitsmanager die zentrale Kontrolle über die Aktivierung, Sperrung und Wiederaufnahme dieser Zugangsdaten auf allen Geräten einer Identität behalten.

Für die Nutzung des Dienstes mit Apple Wallet sind zusätzliche Geschäftsbedingungen erforderlich, die im Voraus unterzeichnet werden müssen. Für weitere Informationen wenden Sie sich bitte an *request.securitymanager.si@siemens.com*.

ACC-AP-Controller verbinden *(Verbindung – Cloud-basierte Zugangskontrolle)*

Schliessen Sie bis zu 10 Türen über Building X Devices an einen ACC-AP-AP-Controller an.

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.
- Jede Identität kann bis zu 5 Berechtigungen umfassen.
- Jedes Privileg umfasst einen Zeitplan.
- Eine Access-Point-Gruppe kann bis zu 100 Access Points umfassen.

Die Inbetriebnahme der Geräte und die gerätespezifischen Einstellungen müssen in SALTO Nebula vorgenommen werden. Die aktuelle Liste der unterstützten SALTO Nebula-Geräte finden Sie unter: https://support.saltosystems.com/nebula/user-guide/installer/device-overview

Building X *(virtuelle Berechtigungsnachweise für Kartenlesegeräte, Apple Wallet-Berechtigungsnachweise)*

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

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

	Virtueller Berechtigungsnachweis für Kartenlesegeräte
Voraussetzung	Für die Verwendung mit PACS muss das folgende Abo aktiv sein: ● Connectivity – Physical Access Control Systems (PACS)
Funktionen	
Building X Platform	✓
Mobile App SDK	✓
Mobile Ausweisverwaltung	✓
Virtueller Berechtigungsnachweis für Kartenlesegeräte	✓
Vor-Ort-Virtual Credentials für SIPORT	✓
Bedingungen	
Abometriken	pro Gerät und 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

	Apple Wallet Berechtigungsnachweis
Voraussetzung	Für die Verwendung mit PACS muss das folgende Abo aktiv sein: ● Connectivity – Physical Access Control Systems (PACS)
Funktionen	
Building X Platform	✓
Apple Wallet Berechtigungsnachweis	✓
Bedingungen	
Abometriken	pro 1 Apple-ID-Benutzer 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

	Google Wallet Berechtigungsnachweis
Voraussetzung	Für die Verwendung mit PACS muss das folgende Abo aktiv sein: ● Connectivity – Physical Access Control Systems (PACS)
Funktionen	
Building X Platform	✓
Google Wallet Berechtigungsnachweis	✓
Bedingungen	
Abometriken	pro 1 Apple-ID-Benutzer pro Jahr erworben werden
Abodauer	Jährliche, automatische Verlängerung
Abrechnungszeit	Jährlich, Vorauszahlung

	Google Wallet Berechtigungsnachweis
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

	Anmeldedaten für SALTO-Zugangspunkte
Voraussetzung	Eines der folgenden Abos muss aktiv sein: • Connectivity: SALTO Nebula Online-Zugangspunkt • Connectivity: SALTO Nebula Offline-Zugangspunkt
Funktionen	
Building X Platform	✓
Anmeldedaten für SALTO-Zugangspunkte	✓
Bedingungen	
Abometriken	pro 1 Google-ID-Benutzer 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

	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

Das Abo für Security Manager / Mobile Access 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**

	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 und der Funktion für virtuelle Zugangsdaten validiert: ● Autec: XMP-TMC2170+XMP-TMC2180+XMP-TMC3070, XMP-TMC3080 ● Elatec: Secustos SQ80 Legic, Secustos SQ80 K Legic, Secustos MU20 LEGIC, Secustos MU20 K LEGIC ● Acre: AR10S-MF+AR40S-MF+AR20M-MF, AR50M-MF ● Apple Wallet Credential wird von allen ECP2-zertifizierten Kartenlesern unterstützt
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

	Liste von unterstützten verbundenen Geräten
	● 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 und der Funktion für virtuelle Zugangsdaten validiert: ● Autec: XMP-TMC2170+XMP-TMC2180+XMP-TMC3070, XMP-TMC3080 ● Apple Wallet Credential wird von allen ECP2-zertifizierten Kartenlesern unterstützt
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.

Mobile Geräte

Für die Installation der mobilen App ist iOS 16.0 und höher oder Android 10 und höher erforderlich.

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 / Mobile Access Datenblatt	www.siemens.com/buildingx/data-sheet/de/security-manager-mobile-access
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.

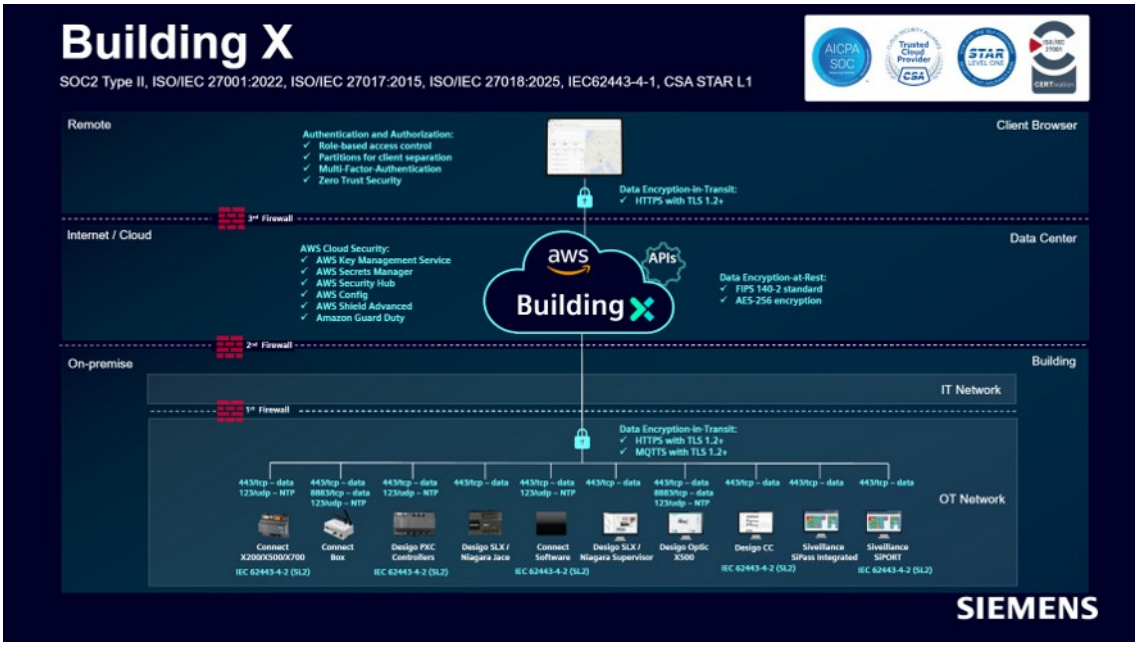
3) Technische Dokumente

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

Allgemeine Geschäftsbedingungen für die Nutzung der Apple Wallet-Funktionalität

1. Als Voraussetzung für die Nutzung der Apple-Wallet-Funktionalität erhält der Kunde die Pass-Through-Bedingungen von Apple (einschliesslich der Apple-Markenrichtlinien) und stimmt diesen mit der Legic Identsystems AG mit Sitz in CH-8620 Wetzikon, Schweiz, zu.
2. Der Kunde stellt sicher, dass keiner seiner Nutzer durch die Nutzung der Apple-Wallet-Funktionalität gegen eine Nutzungsvereinbarung verstößt und wird die Nutzungsvereinbarung bei Bedarf ändern.
3. Der Kunde stellt die relevanten Führungskräfte, Kundenbetreuer und Ingenieure für die Teilnahme an Besprechungen (persönlich, per Telefon oder per Videokonferenz) zur Verfügung, die von Apple angefordert und von Siemens dem Kunden von Zeit zu Zeit mitgeteilt werden.

Allgemeine Geschäftsbedingungen für die Nutzung der Google Wallet-Funktionalität

1. Als Voraussetzung für die Nutzung der Google Wallet-Funktion erhält der Kunde das separate Dokument mit den „Pass-Through-Bedingungen für teilnehmende Anbieter“ von Google und Siemens und erklärt sich damit einverstanden.
2. Der Kunde stellt sicher, dass keiner seiner Nutzer durch die Nutzung der Google-Wallet-Funktionalität gegen eine Nutzungsvereinbarung verstößt und wird die Nutzungsvereinbarung bei Bedarf ändern.

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 A6V15573372_de--
Ausgabe 22.09.2026