SIEMENS

Datenblatt

Security Manager

Security Manager / Intrusion Detection sind cloudbasierte Angebote innerhalb von Building X, die zur Fernüberwachung und -bedienung von Siveillance Intrusion-Systemen verwendet werden.

- Essentielle Identitäts- und Zugangsverwaltung und Scharf-/Unscharfschaltung
- Standard-Identitäts- und -Zugangsverwaltung sowie Scharf-/Unscharfschaltung
- Sicherheits-Selbstverwaltungsportal
- Mitgliedschaftsüberprüfung für Sicherheitsgruppen
- Berechtigungsnachweis-Management
- Sicherheitsalarm-Management
- Sicherheitsüberwachung und Insights Dashboards
- Verbindung von On-Prem Siveillance Intrusion Systems
- Keypad NXT Edge
- Activity Log

URL

securitymanager.siemens.com

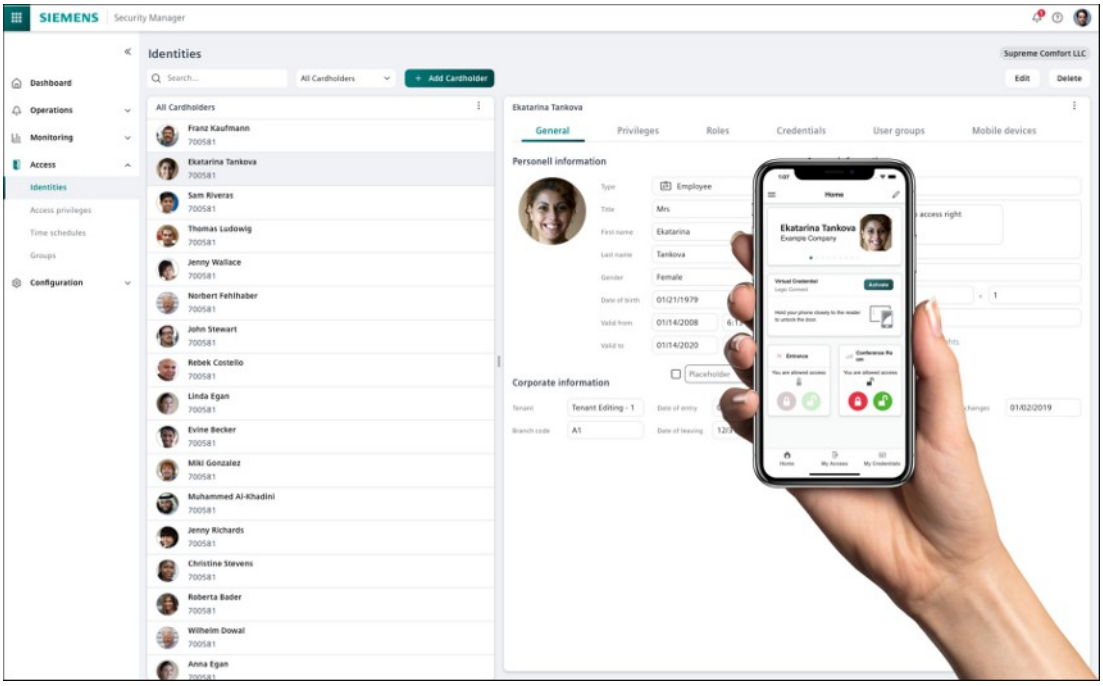
Funktionen

Essential Identity and Access Management

Verwalten von Identitäten auf Basis des festgelegten Basisidentitätstyps (inkl. allgemeiner Identitätsinformationen), Zuweisen von Zugriffs- und Aktivierungs-/Deaktivierungsrechten und Berechtigungsnachweisen, Verwalten und Zuweisen von Sicherheitsgruppen, Verwalten mobiler Geräte.

Hinweis: Derzeit ist es möglich, einer einzigen Identität im Security Manager mehrere Zugriffsrechte zuzuweisen, die mit verschiedenen Siveillance Intrusion Advanced / Pro Berechtigungsgruppen verbunden sind. Aufgrund von Systembeschränkungen in Siveillance Intrusion kann jedoch nur eine Berechtigungsgruppe pro System für einen Benutzer zu einem bestimmten Zeitpunkt aktiv sein. Die zuletzt in Security Manager zugewiesene Berechtigung hat Vorrang und wird mit Siveillance Intrusion synchronisiert.

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 Siveillance Intrusion-Systeme hinweg
- Verwalten von mobilen Geräte
- Berechtigungsnachweise zuweisen
- Zuweisung von Zugangs- und Aktivierungs-/Deaktivierungsberechtigungen
- Verwalten und Zuweisen von Sicherheitsgruppen
- Import von Identitäten über eine CSV-Datei

Hinweis: Derzeit ist es möglich, einer einzigen Identität im Security Manager mehrere Zugriffsrechte zuzuweisen, die mit verschiedenen Siveillance Intrusion Advanced / Pro Berechtigungsgruppen verbunden sind. Aufgrund von Systembeschränkungen in Siveillance Intrusion kann jedoch nur eine Berechtigungsgruppe pro System für einen Benutzer zu einem bestimmten Zeitpunkt aktiv sein. Die zuletzt in Security Manager zugewiesene Berechtigung hat Vorrang und wird mit Siveillance Intrusion synchronisiert.

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.
- Konfigurieren Sie Delegationen für Approver: 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.

Berechtigungsnachweis-Management

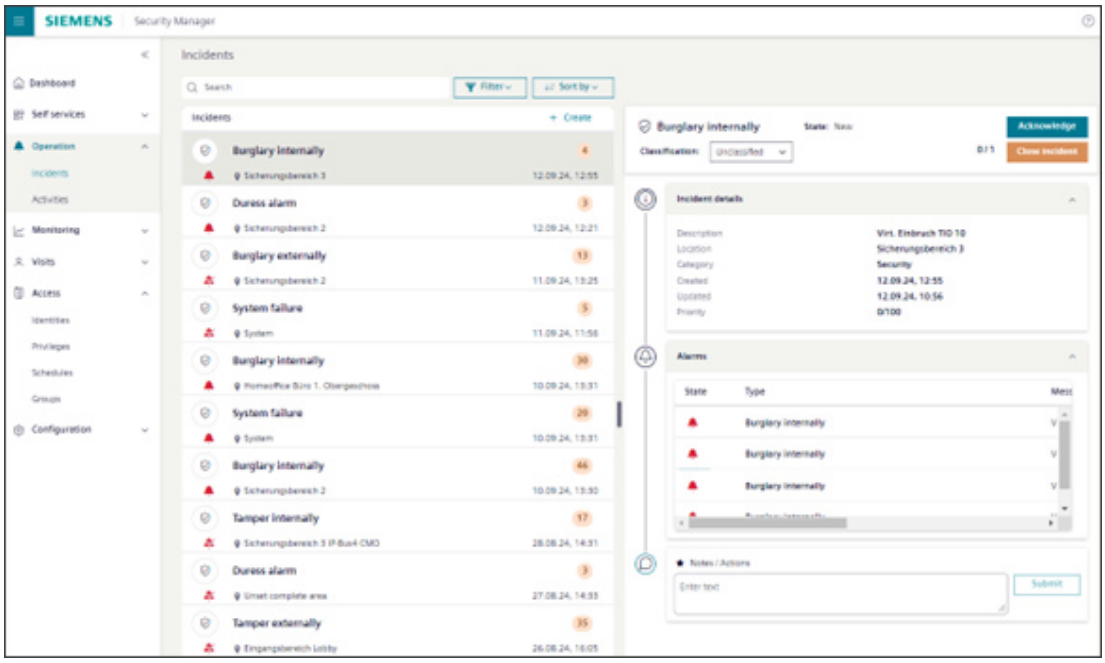
Der Servicetechniker kann Folgendes konfigurieren:

- 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:

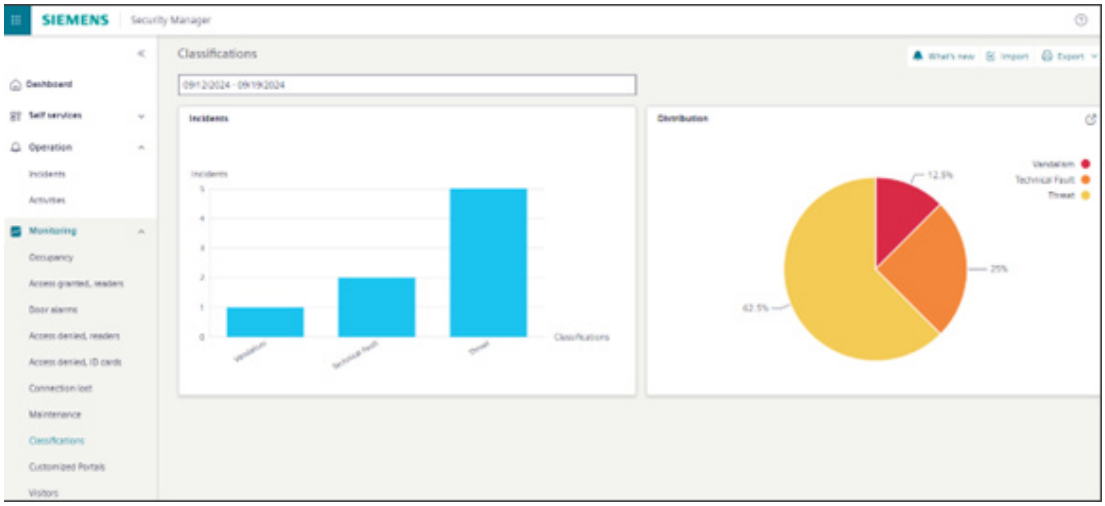
- Mit dem Flag "Enable virtual ID card in Building X Access app" kann die virtuelle ID-Karte (Ausweis) für eine bestimmte Identität aktiviert oder deaktiviert werden. Wenn sie aktiviert ist, zeigt die Building X Access-App dem Benutzer die virtuelle ID-Karte sowie alle verfügbaren digitalen Schlüssel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

Security Alarm and Task Management



- Alarme, die am selben Ort auftreten, zu einem Sicherheitsauftrag zusammenfassen.

Security Monitoring and Insights Dashboards



- Klassifizierte Anzahl von Incidents anzeigen

Connect On-Prem Siveillance Intrusion Systems

Verbindung zu Siveillance Intrusion Advanced und PRO über den Cloud Agent zur Synchronisierung von Berechtigungsnachweisen, Berechtigungen und Identitäten sowie das Senden von Daten an die Building X Punkt- und Alarmvertikale.

Keypad NXT Edge

Verwaltung der HMI SW für Siveillance Intrusion, die auf X200, X300 oder Connect SW läuft, und Bereitstellung der Remote-Client-Funktionalität über Building X.

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

<table>
<tr><th colspan="5">Security Manager / Intrusion Detection</th></tr>
<tr><th></th><th>Intrusion Detection - Essential</th><th>Intrusion Detection - Standard</th><th>Connectivity – Physical Intrusion Detection System</th><th>Intrusion Detection - Keypad NXT Edge</th></tr>
<tr><td>Voraussetzung</td><td colspan="2">Das folgende Abo muss aktiv sein:
Connectivity – Physical Intrusion Detection System</td><td colspan="2">-</td></tr>
<tr><td rowspan="2">Funktionen</td><td colspan="4">Benutzerverwaltung
Activity Log</td></tr>
<tr><td>Essentielles Identitäts- und Zugangsmanagement / Scharf- und Unscharfschaltung</td><td>• Standard Identitäts- und Zugangsverwaltung / Scharf- und Unscharfschaltung
• Sicherheits-Selbstverwaltungsportal
• Überprüfung der Mitgliedschaft für Sicherheitsgruppen
• Berechtigungs-Management Sicherheitsalarm und Task Management
• Sicherheitsüberwachung und Insights Dashboards</td><td>Verbindung von On-Prem Siveillance Intrusion Systems</td><td>Keypad NXT Edge</td></tr>
<tr><td>Abometriken</td><td colspan="4">pro 1 Intrusion-Bereich pro Jahr
Das Abo kann in Paketen von 1 Datenpunkten erworben Bereich</td></tr>
<tr><td>Abodauer</td><td colspan="4">Jährliche, automatische Verlängerung</td></tr>
<tr><td>Abrechnungszeit</td><td colspan="4">Jährlich, Vorauszahlung</td></tr>
<tr><td>Upscaling</td><td colspan="4">Gültig ab sofort, anteilige Abrechnung</td></tr>
<tr><td>Downscaling/ Kündigung</td><td colspan="4">Gültig zum Ende der Abolaufzeit</td></tr>
<tr><td>Angeschlossene Geräte</td><td colspan="4">Separat zu erwerben</td></tr>
<tr><td>Zugelassene Benutzer</td><td colspan="4">Bis zu 10.000; Erweiterte Nutzung</td></tr>
</table>

Das Abo für Security Manager / Intrusion Detection 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 von Einbruchsüberwachungsbereichen, 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
Siveillance Intrusion Advanced	Siveillance Intrusion Detection Panel Advanced 100 & 200, versorgt mit 230 VAC.
Siveillance Intrusion PRO	Siveillance Einbruchmeldezentrale PRO 300, PRO 400 und PRO 800, versorgt mit 230 VAC.

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 Manager / Intrusion Detection Datenblatt	www.siemens.com/buildingx/data-sheet/de/security-manager-intrusion-detection
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

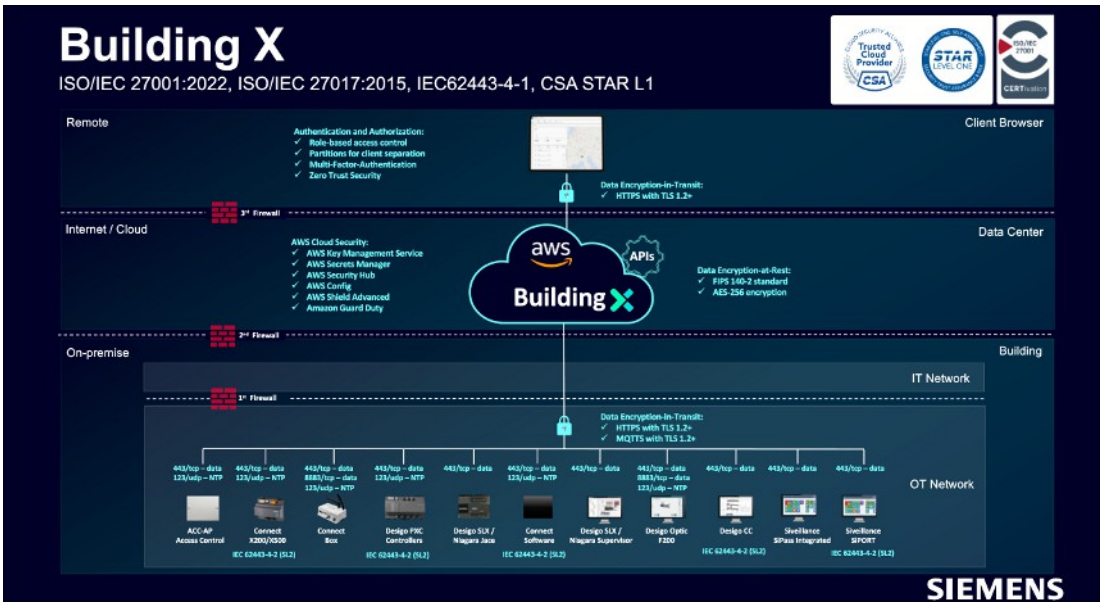
2) Produktdokumentation im Rahmen eines Benutzerdefinierten Abos

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	A6V16055141_de--
Ausgabe	16.12.2025