MATRIX Software 3000

- Zutrittskontrollsoftware für die Anbindung von Online- und Mechatronik-Zutrittskomponenten in der Betriebsart Offline und Access on Card (AoC)
- Client/Serverarchitektur mit browserbasierter Bedienoberfläche
- Umfangreiche Auswertmöglichkeiten
- Scharf-/Unscharfschalten von Einbruchmeldeanlagen
- Berechtigung über Zutrittsprofile und Einzelberechtigungen

Die MATRIX Software 3000 Zutrittskontrolle ist eine hochmoderne Softwareplattform zur Steuerung und Verwaltung von Zutrittsabläufen in Gebäuden und der Gebäudeperipherie.

Systemübersicht

Das MATRIX Software 3000 Zutrittskontrollsystem unterstützt nahezu jeden Sicherheitsanspruch und kann für eine einfache Türsteuerung über Schließplan genauso eingesetzt werden wie für die Abbildung komplexer Sicherheitssituationen, beispielsweise mit Aufzugssteuerung oder Schleusenverwaltung.
MATRIX verwaltet und steuert dabei „Offline“-Mechatronik-Komponenten in den Betriebsarten Offline und Access on Card (AoC) genauso wie verkabelte Online-Zutrittsleser in einem übersichtlichen Gesamtsystem.
MATRIX Zutrittskontrolle ermöglicht ein effizientes Management der Zutrittsberechtigungen auf Basis von festen Zutrittsprofilen oder Einzelberechtigungen, die Personen bzw. Personengruppen zugeordnet werden. Über Zutrittsprofile sind allgemeine Änderungen schnell an zentraler Stelle durchführbar.
Individuelle Zutrittsanforderungen lassen sich ergänzend über Einzelberechtigungen abbilden und einzelnen Personen zuordnen.
MATRIX ist vollständig browserbasiert, was Installation und Wartung wesentlich erleichtert. Einmal installiert ist das System von jedem gewünschten Rechner im Netzwerk aus erreichbar.

Bearbeitungsdialoge und Daten sind multilingual. Alle Funktionen werden nach einem einheitlichen Bedienkonzept über eine ergonomische Bedienoberfläche verwaltet.
Auswertungen von Protokollen können detailliert angezeigt oder in Listen selektiert werden.

Funktionen

Die Zutrittskontrollsoftware MATRIX entspricht der DIN EN60839-11-1 und ist mit modernster objektorientierter Java Technologie ausgestattet.
Die Software ist ausgelegt für 2.000 Personalstammsätze und die Nutzung beliebig vieler Zutrittskontrollzentralen, Ausweisleser sowie MATRIX Schließzylinder, Türbeschläge und Offline-Wandleser in der Betriebsart Offline und AoC (Access on Card).
Die Software ist voll browserfähig und bietet eine ergonomisch sehr gut gestaltete Bedienoberfläche mit integrierter Verwaltung sämtlicher Zutrittskontrollkomponenten. Alle Funktionen werden nach einem durchgängig einheitlichen Bedienkonzept verwaltet.
Bei einer Anbindung an Einbruchmeldeanlagen können mit MATRIX Software 3000 Sicherungsbereiche sowie Berechtigungen zum Scharf- und Unscharfschalten einfach und schnell konfiguriert werden. Dabei können auch VdS-konforme Anforderungen berücksichtigt werden.
Verschiedene Assistenten und eine Schließplanmatrix erlauben es, bedienergeführt eine große Anzahl von externen Komponenten fehlerfrei und vollständig zu parametrieren, sowie schnell und übersichtlich in Betrieb zu nehmen.

Die Software bietet benutzerabhängige umfangreiche Protokollier- und Auswertemöglichkeiten.

Planungshinweise

Systemvoraussetzungen: MATRIX Server

- **Microsoft® Windows® kompatibler PC**
- **Prozessor (Intel-Core-i5-Serie, Intel Xeon oder vergleichbar) / Hauptspeicher**
  - Aktueller Prozessor (< 2 Jahre) mit min. 4 Kernen und min. 3 GHz
  - bis 1.000 Personen: >= 8 GB
  - bis 2.000 Personen: >= 16 GB
- **Betriebssysteme**
  - Windows 10 Pro (64-Bit) [(1)]
  - Windows 11 Pro (64-Bit)
  - Windows Server 2012 (R2) [(2)]
  - Windows Server 2016 [(2)]
  - Windows Server 2019 Standard [(2)]
  - Windows Server 2022 Standard [(2)]

Hinweis:

- Jeweils nur mit aktuellem Servicepack.
- Windows 10 und neuer: Um ein unkontrolliertes Beenden von MATRIX zu vermeiden muss unter *Energieoptionen > Netzschalterverhalten ändern* der Schnellstart deaktiviert werden.

[(1)] evolo Programmer Service: Keine Unterstützung für Version 1507 (2015) und 1511 (2017)

[(2)] Keine Nutzung der Client-Software-Module (Desktop Reader Manager, evolo Programmer Service, XS-Manager) direkt auf Server-Betriebssystemen möglich. Diese werden auf dem aufrufenden Client-Rechner installiert, an dem die entsprechende Funktion genutzt werden soll und stehen daher nur in Betriebssystemen für Client-Rechner zur Verfügung.

- **Datenbanken**
  - H2 (Interne Datenhaltung bis 1000 Personen)
  - MS SQL Server 2016 (Lizenzpflichtig)
  - MS SQL Server 2017 (Lizenzpflichtig)
  - MS SQL Server Express 2019 (kostenlose Lizenz; wird standardmäßig mit MATRIX installiert
  - MS SQL Server 2019 (Lizenzpflichtig)
  - MS SQL-Server 2022 (Lizenzpflichtig)

Hinweise:

- MS SQL Server (bzw. Express) jeweils nur mit aktuellem Servicepack!
- Systemvoraussetzungen MS SQL Server (bzw. Express) beachten.
  - MS SQL Server Express ist limitiert auf max. 10 GB Datenbankgröße. Es werden auch bei Rechnern mit höherer Ausstattung maximal 1 GB Hauptspeicher und 1 Prozessor (4 Kerne) verwendet.
  - Ab 5.000 Personen wird MS SQL Server Standard-Edition oder höher empfohlen. (nur MATRIX Software 5000 und Zeitwirtschaft)
- **Festplattengröße**
  - Anwendung und Datenbank-Installation benötigt 6 GB, hinzu kommt die Kapazität zur Datenspeicherung (bei MS SQL Server Express max. 10 GB)
- **Schnittstellen**
  - TCP/IP, Ethernet (Ports zur Kommunikation mit Webbrowsern und externen Geräten müssen offen sein)
  - Freier USB-Port für Lizenz-Dongle (entfällt bei Dongle-freier Lizensierung über E-Licence)
- **MATRIX OPC-Server**
  - Betriebssystem: Windows 10 Professional (64-Bit)

Systemvoraussetzung: Client-PC (Browser-Client)

- **Browser**
  - Jeder für Mozilla Firefox, Google Chrome oder Microsoft Edge geeignete PC. Die Browser müssen jeweils auf einem aktuellen Versionsstand sein.
- **Schnittstellen**
  - USB für Maus und ggf. für PC-Leser (USB-Bekanntmachungsleser)
  - TCP/IP, Ethernet
- **Bildschirm**
  - Auflösung von mind. 1366 x 768, empfohlen Full-HD 1920 x 1080
  - Für Alarmmonitor mind. 1600 x 900, empfohlen Full-HD 1920 x 1080
- **Anzeige generierter PDF-Dokumente**
  - Für die Anzeige generierter PDF-Dokumente ist ein PDF-Reader notwendig
- **Anzeige generierter PDF-Dokumente**
  - Für die Anzeige generierter PDF-Dokumente ist ein PDF-Reader notwendig

Erforderliche Portfreischaltungen in der Firewall

Je nachdem welche Geräte bzw. Funktionalität genutzt wird, müssen folgende ein- und ausgehenden Ports auf dem Server ("MATRIX-Server") in der Firewall freigeschaltet sein. Es handelt sich um die bei der Installation vorgeschlagenen Standardwerte. Wenn durch den Einrichter des Systems abweichende Ports definiert werden, müssen stattdessen diese freigeschaltet werden.

Webserver und Datenbank (Muss)

- Port 8443 für den Webserver mit SSL-Verschlüsselung (empfohlen)
- Port 8080 für den Webserver ohne SSL-Verschlüsselung (nicht empfohlen)

- Port 1433 für MS SQL-Server Datenbank (lokale Verwendung oder zu externem DB Server)
- Hinweis: Für H2 ist keine Port-Freischaltung notwendig

Geräte in MATRIX
Die jeweiligen Ports müssen nur für die Gerätetypen freigeschaltet werden, die in der Kundeninstallation tatsächlich eingesetzt werden.
Server (Muss)
- Port 3000 für Buchungen und Ereignisse (eingehend)

Tischleser 91 08 / Desktop Reader Manager Software
- Port 3501 für Kommandos und Konfigurationen
  - MATRIX-Server (ausgehend)
  - Bedien-Client (eingehend)
- Port 3010 für Alive-Meldungen
  - MATRIX-Server (eingehend)
  - Bedien-Client (ausgehend)
- Port 8000
  - lokale Kommunikation (DRM zu DCC 3.0-Schnittstelle)
- Port 18080 für das Übernehmen der Ausweisnummer in MATRIX
  - Bedien-Client (eingehend)

Access Manager (AM 92 xx TP4 Controller)
- Port 3001 für Kommandos und Konfigurationen (ausgehend)
- Port 3002 für Kommunikation zwischen den Controllern
- Port 23 für Telnet-Kommunikation mit den Controllern
- Port 22 für den Firmware-Download über FTP (K7-Controller)

Zeiterfassungsterminals (96 20 / 97 20)
- Port 30464 für Kommandos zu den Terminals (ein- und ausgehend - UDP)
- Port 22 für FTP-Kommunikation
- Port 8443 für die Web-GUI der Terminals

evolo Komponenten / evolo Programmer Service
- Port 3502 für Kommandos und Konfigurationen
  - MATRIX-Server (ausgehend)
  - Bedien-Client (eingehend)

evolo wireless Gateway 90 40
- Port 9000 für Kommandos und Konfigurationen (ausgehend)
- Port 443 für die Web-GUI des wireless Gateway

Hinweise zur Security
Die Infrastruktur des Betreibernetzwerkes hat großen Einfluss auf die zusätzliche Sicherheit. Wir empfehlen daher dringend, den Zugriff auf den MATRIX-Server soweit wie möglich einzuschränken. Beispielsweise sollte bei sehr hohen Sicherheitsanforderungen MATRIX nur in einem geschützten internen Netz zur Verfügung gestellt werden. Wenn MATRIX im öffentlichen Netz verfügbar sein soll (z.B. Self Service mit Smartphone), müssen vom Betreiber zusätzliche Sicherheitsmaßnahmen, wie z.B. Zugang über VPN (Virtual Private Network) ergriffen werden.

Hinweis zur Datensicherung
Es wird empfohlen, eine regelmäßige Datensicherung durchzuführen (z.B. Datensicherung auf dem Server oder externer Harddisk oder Tape-Streamer)

Hinweis zum verwendeten Webserver
Als Webserver wird der Apache Tomcat verwendet und mit der MATRIX-Installationsroutine mitinstalliert (muss nicht vorab installiert werden!). Es wird eine eigene Instanz verwendet und als MATRIX Tomcat Dienst registriert.

Hinweis zu Dongle-freier Lizenz in Server-Clustern
Das Dongle-freie Lizenz-Konzept basiert auf diversen Hardware-Parametern und weiteren Faktoren. Wenn sich diese ändern, muss eine manuelle Relizenzierung vorgenommen werden.

SSL Zertifikat Zertifizierungsstelle
Um ein SSL Zertifikat für eine sichere Verschlüsselung zu erhalten muss ein „Certificate Signing Request" (CSR) (englisch für „Zertifikatsanforderung") bei einer Zertifizierungsstelle gestellt werden. Jeder Anbieter von SSL Zertifikaten unterstützt den Antragsteller beim Erstellen des CSR. Das Zertifikat muss im Format PKCS12 oder JKS vorliegen.
Die CSR ist die Vorstufe eines SSL Zertifikats und wird benötigt, um ein SSL Zertifikat bei einer Zertifizierungsstelle zu beantragen. Um eine CSR zu erzeugen, müssen Sie ein Schlüsselpaar für Ihren Server erstellen, bestehend aus einem privaten Schlüssel (Private Key) und der CSR. Die CSR enthält Informationen zum Antragssteller und der Domain, die verschlüsselt werden soll, sowie den öffentlichen Schlüssel (Public Key). Der private Schlüssel verbleibt bei Ihnen und darf nicht veröffentlicht werden. Das Zertifikat ist später untrennbar mit dem privaten Schlüssel verbunden. Dieser sollte daher gut aufbewahrt und zusätzlich z.B. auf einem externen Datenträger gesichert werden.

Allgemeiner Hinweis
Alle genannten Systemvoraussetzungen beziehen sich auf MATRIX Softwareversion 4.1

Im Lieferumfang enthaltene Teile

Anzahl	Komponente
1	Software via Download
1	Lizenzkey zur Autorisierung der Software

Technische Daten

Systemgröße	Wertebereiche bis 9999 möglich für alle wesentlichen Systemtabellen (Begrenzungen durch die Peripherie müssen beachtet werden)
Anzahl Ausweise	2000
Benutzergruppen/ -verwaltung	Beliebig viele Benutzer mit Aktivitätsprotokollierung möglich; Zugriff auf alle Module und Funktionen als Voll- oder Lesezugriff definierbar; Menü passt sich den Rechten dynamisch an
Datensicherung	Automatisierte Datensicherung und Wiederherstellungsfunktion bei Nutzung der H2-oder integrierten SQL-Datenbank
Personaldaten	Import oder Export mittels CSV-Dateien
Datenhaltungsgrenzen	Individuelle Festlegung der Datenhaltungsgrenzen
Assistenten	Dialoggeführte Unterstützung zur schnellen Definition von Zutrittskontrollkomponenten
Serviceinformationen	Als Textdatei, optimiert zur Weiterleitung an den Support zur Fehlerbehebung
Logdateien	Zugriff auf die in den Komponenten erzeugten Protokolle möglich
Listen	Vordefinierte Listen und eigene Definition von dynamischen Listen für Personaldaten im PDF-Format oder als CSV-Datei
PIN Code	1- bis 6-stelliger PIN-Code Möglichkeit für unterschiedliche PIN-Codes: (Zutritt, Bedrohungs-PIN-Code, Scharf-/Unscharfschalten)
Zutrittskalender	Basis für die Zutrittskontrolle der Personen und zur Türsteuerung; inkl. Sondertagsteuerung
Tagestypen u. Sondertage	Definition eigener Sondertage bei Abweichungen vom normalen Kalender
Personalsatz	Personalnummer: bis 255 Zeichen, numerisch/alphanumerisch; Erfassung der wesentlichen personenbezogenen Daten übersichtlich in einer Maske; Integrierte Ausweis- und Berechtigungsverwaltung
Abteilungen	Zuordnung der Stammsätze zu Abteilungen, zur Gruppierung von Personen über Abteilungsname und Nummer
Ausweise	Mehrere Ausweise pro Person definierbar; Unterstützung von Ersatzausweise; Flexible Berechtigung der Ausweise mittels Profile und Einzelberechtigungen
PC-Leser	Einlesen der Ausweiskodierung mittels optionalem PC-Leser effizient und fehlerfrei möglich
Zutrittsprofile	Zusammenfassung von Zutrittsrechten für z. B. bestimmte Mitarbeitergruppen zur schnellen Vergabe von Rechten
Einzelberechtigungen	Zuordnung weiterer, individueller Zutrittsrechte zu einem vergebenen Profil vereinfacht die Behandlung temporärer Ausnahmefälle
Zutrittswochenpläne für Mitarbeiterberechtigung	Jedem Wochentag wird ein Zutrittsprogramm zugeordnet, bei Sondertagen wird automatisch das Ersatzzutrittsprogramm berücksichtigt
Zutrittsprogramme	Vier Zeitintervalle pro Tag je Tür
Türwochenpläne	Zusammenfassung der Türtagesprogramme zu Wochenplänen mit Ausnahmeregeln für Sondertage
Türtagesprogramme	4 Intervalle je Tag, z. B. für: • Buchung berechtigt • Türdaueröffnung • Unterdrückung der Zutrittsprotokollierung • Anforderung der PIN-Eingabe zusätzlich zur Ausweisbuchung
Türstatusüberwachung	Eingangskontakte und Relais zur Steuerung und Überwachung; Definition der Entriegelungsimpulsdauer, erlaubte Türoffenzeit und Alarmdauer möglich

Raumzonen	Zusammenfassung von Ausweislesern zu Raumzonen mit Sicherheitsoptionen, z. B. • Zutrittswiederholsperre (Antipassback) • Doppelnutzungssperre • Raumzonenwechselkontrolle
Spezielle Zutrittsoptionen	• Schleusensteuerung • Aufzugssteuerung • Scharf/Unscharfschalten von Einbruchmeldeanlagen • Anwesenheitstableau zur Visualisierung des Anwesenheitsstatus von Personen in einem bestimmten Umfeld
Fernwirken manuelle Türsteuerung	Türtableau zur Visualisierung und Steuerung einzelner oder aller Türen • kurzzeitig öffnen • Daueröffnung aktiveren und beenden

Bestellinformationen

MATRIX Software 3000
Zutrittskontrollsoftware für Online- und Offline-Komponenten, Access on Card, max. 2000 Mitarbeiter-Stammsätze, keine Erweiterungen möglich
Bestellnummer **F.01U.569.235** App.Schl. **6250** Vepos **1300**

Zubehör

Nachbestellung MATRIX Software CD
Kostenpflichtig bei CD-Nachbestellung (bitte Donglenummer angeben)
Bestellnummer **F.01U.569.261** App.Schl. **6250** Vepos **1603**

Nachbestellung MATRIX Lizenz Dongle
Ersatz-Dongle für eine bestehende Installation (Dongle-/Lizenzkeynummer wird zwingend benötigt). Die alte bestehende Lizenznummer wird in der Lizenzdatenbank auf inaktiv/gesperrt gesetzt.
Bestellnummer **F.01U.569.263** App.Schl. **6250** Vepos **1605**

MATRIX Lizenz-Dongle (anstatt E-Licence)
USB-Lizenz-Dongle als Alternative zur Lizenzierung mit E-Licence
Bestellnummer **F.01U.649.066** App.Schl. **6250** Vepos **9066**

Software-Optionen

E-License
Dongle-freie Verwaltung (gekoppelt an MAC-Adresse), wird nur für die Erweiterung von Bestandssystemen mit USB-Lizenzdongle benötigt
Bestellnummer **F.01U.569.256** App.Schl. **6250** Vepos **1520**

Update MATRIX Software 3000
Update auf nächst höhere Version (bei Sprung über mehrere Versionen bitte entsprechend mehrfach bestellen)
Bestellnummer **F.01U.569.258** App.Schl. **6250** Vepos **1600**

Upgrade MATRIX Variante
Upgrade von MATRIX Software 3000 auf MATRIX Software 5000 (inkl. 500 Mitarbeiter), zzgl. weitere Mitarbeiter, zzgl. Upgradepreise für Versionssprünge, zzgl. neuer Optionen für MATRIX Software 5000
Bestellnummer **F.01U.569.260** App.Schl. **6250** Vepos **1602**

Lizenzerneuerung MATRIX
Lizenzerneuerung bei Verlust. Lizenzdatei, die im Lieferumfang des bestellten Softwarepaketes oder im Lieferumfang einer Erweiterung enthalten ist.
Bestellnummer **F.01U.569.262** App.Schl. **6250** Vepos **1604**

Vertreten von:

Europe, Middle East, Africa:
Bosch Security Systems B.V.
P.O. Box 80002
5600 JB Eindhoven, The Netherlands
Phone: + 31 40 2577 284
www.boschsecurity.com/xc/en/contact/
www.boschsecurity.com

Germany:
Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Tel.: +49 (0)89 6290 0
Fax:+49 (0)89 6290 1020
de.securitysystems@bosch.com
www.boschsecurity.com