BIS - Access Engine (ACE) 5.0

- Distributed access control system with graphical alarm management
- Seamless integration and interaction with video, fire, intrusion and PA/VA systems via the common BIS platform
- High resilience thanks to a 4-tier system architecture and redundant deployment of critical components
- Integration of third-party products via open and secure protocols and an SDK
- Efficient enrollment process that makes onboarding faster and more secure

Access control has become one of today's most important technologies for increasing the security of people, property, and assets. The BIS Access Engine and sophisticated controller products provide a wide range of access control features.
Combine the basic Access Engine package with optional features to build a customized access control system to meet your exact needs. Then use the Building Integration System software to integrate the Access Engine with your intrusion detection and video security equipment.

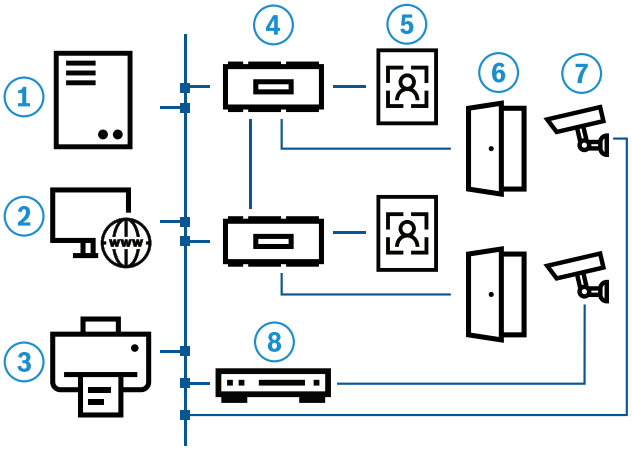
System overview

The Access Engine (ACE) software, in conjunction with Bosch access hardware, is a complete access control system within the Building Integration System (BIS). It encompasses all the essential features of any standalone access control system, plus a wide range of optional enhancements.

Like the other BIS engines, the ACE takes full advantage of all the extra BIS features, such as interactive location maps and action plans for powerful, fully integrated alarm management. Alarm messages and access control events can be displayed with graphical location information and workflow instructions.

ACE uses the standard BIS user interfaces and their flexibility of customization. Additionally ACE offers specific access configuration interfaces for cardholders, access hardware and access rules.

The main benefit of the Building Integration System family is the integration of a wide variety of security and safety systems on the same premises. By combining ACE with other BIS engines (e.g. Automation and Video) you can design smart security solutions tailored exactly to the requirements of your tender.
The Access Engine runs on a single-workstation, in a client-server system, or within a distributed environment with a central server and local or regional servers.
In the distributed multi-server environment all devices, cardholders and authorizations can be managed from the top-level server.
To ensure highest data security and integrity, BIS ACE can manage high-security RS485 controllers with OSDP v2 protocol for authenticated encrypted communication and reader supervision.

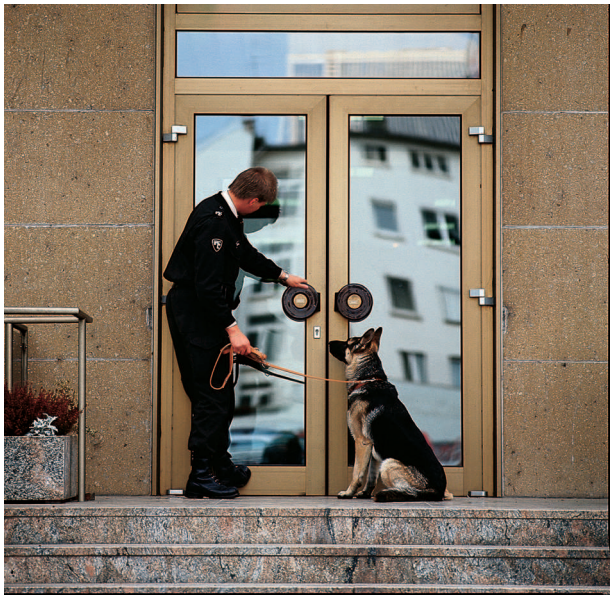


Pos.	Description (single-server system)
1	Central BIS server with Access Engine and Video Engine SW
2	Multiple workstations for alarm management or enrollment
3	Enrollment devices such as card printer, signature scanner, enrollment reader, camera for ID photos
4	Access controllers
5	Access readers
6	Door strikes
7	IP camera
8	Digital Video Recorder e.g. DIVAR for alarm recording

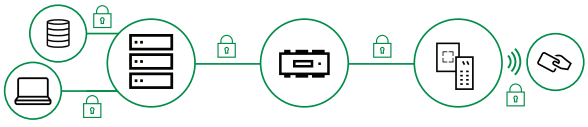
Functions

The Access Engine basic package, in combination with AMC access controllers, offers the following features:

- A wide range of intuitive, template door models allowing fast and easy hardware configuration (e.g. standard door, turnstile, elevator with time & attendance readers etc.).
- The door-model configuration dialog generates a wiring plan for the hardware installer.
- Smooth onboarding process, including card and biometric enrollment.
- Customizable dialogs to collect only the necessary personal information.
- Time models for time-based access control, including the definition of special days, recurring public holidays, etc.
- Time models for automatic activation/deactivation of cardholder accounts, PIN codes etc.
- Time models for automatic activation/deactivation of system settings, such as setting an office door to stay unlocked from 9am to 5pm
- Additional PIN code for arming /disarming intruder alarms.
- Temporary blocking / unblocking of cardholders, either manually or time-controlled.
- Blacklisting of cards.
- Anti-passback.
- Access area balancing, including access sequence checking, provides a means of limiting the number of people in a given area, automatically arming/ disarming alarms if an area is empty/not empty, and generating muster lists.
- N-Persons authorization will grant access at a door only when a defined number (N) of authorized cardholders present their badges to a correspondingly configured reader. The setting can be made reader by reader, and from 2 to N (unlimited) persons.
- Mantrap feature for managing two cooperating doors with two pairs of readers; recommended for high security levels, e.g. entrances to server rooms or research departments.
- Guard tour: a state-of-the-art patrol tracking system using existing access control readers, access-sequence and access-time checking. Any violation of patrol sequence or timing causes an alarm, which is then tracked by BIS's sophisticated alarm management features. Guard tour reports can be generated from the BIS event log.



- Random screening feature: Cardholders accessing or leaving the site can be stopped at random and directed to security personnel for closer inspection. Cards belonging to designated "VIPs" can be excluded from random screening.
- Visitor management: Visitors' cards can be tracked and handled separately as regards their validity periods and the possible need for an escort.
- Interface for arming/disarming an IDS (Intrusion Detection System) including authorization handling and card assignment.

- Web-based import and export of cardholder data stored in third party systems or on a directory server, such as Microsoft Active Directory or Apache Directory.
- All personal information, including photos and signatures, are stored in a secure SQL database.
- Threat-Level Management to preconfigure up to 15 scenarios including Lock Out and Evacuation situations.
- Elevator interface for controlling up to 64 floors via an elevator-internal card reader, and for the assignment of floor authorizations to cardholders.
- Interface to destination management systems able to authorize up to 255 floors with front and back door in an elevator system.
- Interface for importing personnel data from an HR system or exporting such information from ACE to such a system.
- Improved card personalization for importing cardholder images and creating customized corporate badge designs printable on standard card printers.
- Remote door unlock feature e.g. by mouse click on an icon in a BIS interactive location map.
- Creation of logical areas, e.g. single rooms, groups of rooms, whole floors or parking lots, to which special access control points can be assigned.
- Flexible alarm management for a huge range of alarm conditions (e.g. denied access, tamper-detection, badge blacklisted, duress alarm, etc.) optionally combinable with BIS features such as interactive location maps and action plans.
- Utilization of the Bosch controller family's digital, monitored I/Os for additional control and monitoring functions, including intrusion- and tamper-detection.
- Communication between the local access controllers and the readers is secured by OSDP V2 (OSDP Secure Channel).
- Communication between the main access control system and the local access controllers is secured by DTLS (with AES-256 encryption).
- 
- Detailed logging of access events and alarms for legal compliance and forensic investigation.
  - Audit trail for changes to master records and authorizations, including creation, modification and deletion of records.
  - Integrated reporting with filtering capability.
- Support for up to eight different card formats simultaneously.
- Bulk editing of authorizations and other data.

Video verification

Video verification extends the security level of your access control system through video technology. When a reader is in video verification mode the cardholder is not admitted directly. Instead the reader performs a request for entrance which appears as a message on the operator's screen.
An Action Plan (see BIS optional accessories) shows the operator the cardholder’s image as stored in the ACE database in conjunction with a live image from a camera near the entrance/reader that sent the request. The operator compares both images and decides whether or not to open the door.

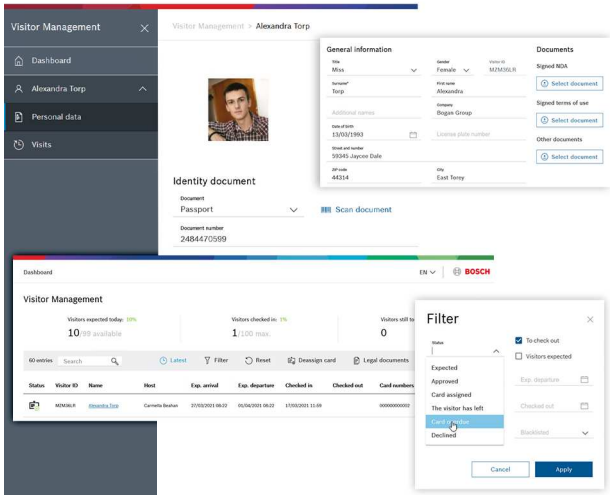
Parking lot management

This feature allows the definition and use of the door model “parking lot” which contains the control of two barriers for entrance and exit and their traffic lights, which prevent access when the lot has reached maximum capacity.
Access to parking lots can be regulated by long-range reader and ID card, or by camera and license plate. Each parking lot can be divided into logical areas, with a maximum number of cars defined for each. Authorization to pass the barrier and park in a logical area can be assigned to cardholders in the standard dialogs. Load-balancing of the parking lots is also possible, with current capacity information displayed on the operator’s screen. Load balancing of cars (parking lots) and persons (access areas) is handled separately, so that it is possible to track the location of both cardholder and car simultaneously.

Visitor Management

- Pre-register appointments in the system, to shorten processing time.
- Allow visitors to create their own profiles in kiosk mode, to avoid queues at reception.
- Use a dashboard to monitor the day's expected visits, how many visitors are on the premises, which credentials are in use, and which credentials still need to be collected.

- Set expiration dates on visitor profiles and their attachments to comply with national data privacy regulations, such as European GDPR.



Integration of intrusion panels
Permissions to operate Bosch B and G Series intrusion panels can be assigned to cardholders centrally, allowing them to arm and disarm intrusion-controlled areas.
With the appropriate authorization, a cardholder can disarm an area and unlock its door with a single card swipe at a simple reader.

Access control for disease control

- New contactless fingerprint and face-recognition readers eliminate a dangerous source of contamination. For even higher security, the system can optionally demand a contactless card or a further biometric credential for authentication.
- Access sequence control helps enforce one-way crowd flow - reducing the risk of the infection by eliminating face-to-face encounters.
- ACE's threat-level management provides ways to switch instantaneously from one crowd-flow scheme to another, in case of emergency.
- ACE's access-control areas are ideal for quickly implementing hygienic restrictions on the number of persons in a defined space.
- Contactless readers eliminate the need for physical elevator buttons.
- Contactless arming and disarming of intrusion areas further reduces contamination sources.
- The use of mobile phones for access promotes hygiene by reducing the number of shared physical credentials - a cooperative solution developed with partners **HID** and **STiD**.
- License-plate recognition systems reduce the need for manned control booths, keypads and buttons; or for reaching outside the vehicle with physical credentials.

Accessories for BIS Access Engine

Extended parking management
Provides management of guest parking, including the generation of parking vouchers and notification about visitors who overstay their scheduled appointments.

Application Programming Interface
A software development kit (SDK) to integrate Access Engine with third-party applications such as Identity Management, Time & Attendance and advanced Visitor Management systems.

Integration of key cabinets
Integration of **Deister** and **Kemas** key cabinets for securing physical keys and monitoring their usage. Available in certain countries only.

Integration of wireless online locks
Integration of **SimonsVoss SmartIntego** wireless online locks (lock cylinders, door handles and padlocks) for doors, which require medium-level security, such as offices and classrooms. Available in certain countries only.

Integration of remote offline locks
Integration of **OSS-SO compliant offline locks** or **Normbau (Pegasys)** offline locks for remote doors, which connection via cabling is not possible due to distance, construction conditions or cost. The offline locking system consists of software, hardware and accessories. The hardware is freely available on the open market from Bosch partners. The software license enables a number of dialogs in BIS and ACE. Available in certain countries only.

Increasing access control capacity
ACE scales easily to the growing needs of your sites. Additional MAC (Main Access Controller) licenses enable you to increase geographical coverage or performance. A growing number of staff or visitors can be accommodated by additional cardholder licenses. Licenses to increase the number of entrances are available in steps of 32, 128 or 512. An entrance in this sense is equivalent to an ACE door model, making it easy to calculate requirements.
Example: Your site has 2 main entrances with an entry and an exit reader each, 26 office doors with entrance reader and 1 mantrap for the server room. The total number of door models/entrances is 29, irrespective of the number of readers involved. A total of 32 entrances is already covered by the ACE basic package license.

Installation/configuration notes

Access Engine in figures

The following maxima apply to the reference system described below.

Max. number of active cards per system	400,000
Max. number of readers per server	10,000
Max. number of MACs (Master Access Controllers) per server	40
Max. number of access authorizations per MAC	1,000
Max. number of AMCs per MAC	125 For high-performance systems: 60
Max. number of access authorizations per ACE	40,000
Max. number of divisions per ACE	400
Max. number of guard tours per ACE	200
Max. number of simultaneous guard tours	8
Max. number of B/G intrusion panels for cardholder synchronization with ACE	500

Reference systems for server and client

	Server system (with no client running)	Client system
CPU	Intel Xeon E-2144G @ 3,6 GHz (4 cores, 8 logical)	Intel Core i7-8700 @ 3,2 GHz (6 cores, 12 logical)
RAM	32 GB (2667 MHz)	8 GB (2667 MHz)
GPU	Integrated graphics from CPU	Intel UHD Graphics 630 (4GB GPU memory)
System disk	NVMe Write speed: 1440MB/s Read speed: 2250MB/s Average response time 10ms	SSD disk
Disk where AMS is installed	SSD Write speed: 1000MB/s Read speed: 1100MB/s Average response time 10ms	
Operating system	Microsoft Server 2019 Standard Edition	Microsoft 10 Pro Edition

Browser versions for web-based add-in programs

Web Browser	Version
Google Chrome	112 or higher
Microsoft Edge	111 or higher
Mozilla Firefox	102 or higher

Technical specifications

See the specifications for the respective version of the BIS Basic Package.

Ordering information

BIS-FACE-API50 License for API
BIS Access Engine license for API
Order number **BIS-FACE-API50 | F.01U.415.274**

BIS-FACE-BPA50 Basic license
Basic license for BIS Access Engine
Order number **BIS-FACE-BPA50 | F.01U.415.273**

BIS-FACE-OFFL50 License for offline basic package
License for offline basic package (ACE)
Order number **BIS-FACE-OFFL50 | F.01U.415.275**

BIS-FACE-PRK50 License for carpark management
License for carpark management (ACE)
Order number **BIS-FACE-PRK50 | F.01U.415.277**

BIS-FACE-VISWEB50 License for visitor management
License for visitor management (ACE)
Order number **BIS-FACE-VISWEB50 | F.01U.415.276**

BIS-XACE-100C50 License for 100 ID cards
License for 100 ID cards (ACE)
Order number **BIS-XACE-100C50 | F.01U.415.290**

BIS-XACE-10KC50 License for 10,000 ID cards
License for 10,000 ID cards (ACE)
Order number **BIS-XACE-10KC50 | F.01U.415.292**

BIS-XACE-10MC50 License for 10 MAC
License for 10 MAC (ACE)
Order number **BIS-XACE-10MC50 | F.01U.415.285**

BIS-XACE-128D50 License for 128 doors
License for 128 doors (ACE)
Order number **BIS-XACE-128D50 | F.01U.415.288**

BIS-XACE-1KC50 License for 1,000 ID cards
License for 1,000 ID cards
Order number **BIS-XACE-1KC50 | F.01U.415.291**

BIS-XACE-1KEY50 License for 1 key cabinet
License for 1 key cabinet
Order number **BIS-XACE-1KEY50 | F.01U.415.295**

BIS-XACE-1MAC50 License for 1 MAC
License for 1 MAC
Order number **BIS-XACE-1MAC50 | F.01U.415.284**

BIS-XACE-25OF50 License for 25 offline doors
License for 25 offline doors
Order number **BIS-XACE-25OF50 | F.01U.415.286**

BIS-XACE-25ON50 License for 25 wireless online doors
License for 25 wireless online doors
Order number **BIS-XACE-25ON50 | F.01U.415.294**

BIS-XACE-32DR50 License for 32 doors
License for 32 doors
Order number **BIS-XACE-32DR50 | F.01U.415.287**

BIS-XACE-50KC50 License for 50,000 ID cards
License for 50,000 ID cards
Order number **BIS-XACE-50KC50 | F.01U.415.293**

BIS-XACE-512D50 License for 512 doors
License for 512 doors
Order number **BIS-XACE-512D50 | F.01U.415.289**

BIS-XACE-25OS50 License for 25 OSS-SO offline doors
License for 25 OSS-SO offline doors
Order number **BIS-XACE-25OS50 | F.01U.415.309**

Represented by:

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

North America:
Bosch Security Systems, LLC
130 Perinton Parkway
Fairport, New York, 14450, USA
Phone: +1 800 289 0096
Fax: +1 585 223 9180
onlinehelp@us.bosch.com
www.boschsecurity.com

Asia-Pacific:
Robert Bosch (SEA) Pte Ltd, Security Systems
11 Bishan Street 21
Singapore 573943
Phone: +65 6571 2808
Fax: +65 6571 2699
www.boschsecurity.com/xc/en/contact/
www.boschsecurity.com