Bosch Introduces Access Management System 3.0 That Integrates With Other Security Solutions

Published on 6 Jul 2020

Today’s market wants access control systems that are always available, scalable, and integrated with other security solutions like video and intrusion systems to ensure the highest security and safety levels. At the same time, these systems must be easy to configure and use. With the introduction of the Access Management System 3.0, Bosch meets all of these requirements.

Always available for security

Access Management System 3.0 is designed to be available at all times. Its resilient design includes a Master Access Controller (MAC) as an additional layer of defense between the server and the access controllers.
If the server fails, the MAC takes over, ensuring continuous communication across controllers while sharing necessary information from the card readers. In addition, access control functionalities that involve multiple access readers, such as anti-passback and guard tour can continue to perform.

The anti-passback functionality is an important feature to ensure a high level of security. It prevents a cardholder from passing a card to another person enabling an unauthorized entry. Guard tour is a safety functionality offered to security guards, which uses access readers as checkpoints along a defined route at specified times.

### Threat level management

The different threat levels can make all doors open, or all doors blocked, or a mix of open and blocked.

Any deviation of sequence or timing causes an alarm in the Access Management System. Immediate notifications to colleagues or first responders increase the safety of security guards. In the rare event that both the Access Management System 3.0 server and the MAC fail, cardholders can still enter and leave areas with their badges because the database is stored directly on the Access Management Controllers (AMCs).

Thanks to this offline capability, it is possible to save millions of events even during downtimes, ensuring the continuous availability of the system. Access Management System 3.0 offers up to 15 configurable threat levels such as lockdown, controlled lockdown, or evacuation, which means safety measures can be initiated quickly in critical situations such as fire or security breach.

The threat level state is activated by one of three triggers: operator workstation, external contact such as an emergency button, or specially configured “emergency” cards that are presented to a reader. The different threat levels can make all doors open, or all doors blocked, or a mix of open...
and blocked.

**Scalable and future-proof**

Users can start small and add extra capacity whenever necessary. The Access Management System 3.0 software can be expanded up to 10,000 doors and 200,000 cardholders. The software is offered in three pre-configured software bundles from medium to large organizations: Lite (max. 144 doors), Plus (max. 512 doors), and Professional (max. 10,000 doors). All bundles support up to 200,000 cardholders.

No hardware needs replacing when expanding; users only require software upgrades and possibly additional controllers, readers, and cards. So, increasing the system is also cost-efficient. Customers who work with the software solution Access Professional Edition (APE) from Bosch can migrate to the Access Management System 3.0 by using the new importer/exporter tool. Together with regular updates to data security enhancements, these features make the system a future-proof investment - suitable for office and government buildings, retail environments, educational institutions, and more.

**Easy configuration and operation**

*Access Management System 3.0 also has trusted digital certificates for mutual authentication*

Configuration is easy: Users can import existing floor maps into the system, and drag and drop icons on the map to represent controllers, doors, and building objects. User onboarding is straightforward. For example, enrollment and assignment of access profiles are all implemented in one dialog manager.

Operation is smooth: The graphical user interface (GUI) is simple and easy to understand. The dark color scheme of the GUI reduces eye-strain and fatigue, so operators stay fresh and alert.
Access Management System 3.0 offers protection against cybercrime and loss of personal data. The database, as well as the communication between the server and access controllers, is encrypted at all stages through the support of the secure Open Supervised Device Protocol (OSDP) v2 protocol. Access Management System 3.0 also has trusted digital certificates for mutual authentication between the server and client to prevent tampering by unauthorized clients and uses secure design principles such as “secure-by-default” and “principle of least privilege.”

Integration with third-party solutions

Access Management System 3.0 is ideal as a standalone solution to meet today’s access control needs. It integrates seamlessly with Bosch B Series and G Series intrusion control panels as well as with video systems such as Bosch Video Management System or third-party systems like Milestone’s XProtect for increased security and enhanced situational awareness.

Integration with Bosch Video Management System (version 10.1 and higher) offers manual video verification to increase the security level at doors. The operator can visually verify whether the person at the door matches the registered person in the database. If so, the operator allows the person to enter. Bosch Video Management System integration also enables searching for cardholder events and events at doors.

With the searching functionality, it is possible to quickly check who has entered an area and at what time. Moreover, access commands and events can be handled in Bosch Video Management System, making the operation of the integrated system most efficient.

Intrusion control panels integration

B and G Series intrusion control panels integrate seamlessly into Access Management System
3.0 for efficient authorization management and a central overview of all access and intrusion events. With central user management, operators can add, delete, and modify intrusion-related user passcodes and authorizations directly into the system, as well as organize users by groups or functionalities.

The integrated command and control functionality enables operators to arm and disarm intrusion panels directly in the Access Management System 3.0 user interface as well as to see states of the areas (e.g. “armed”, “ready to arm”) and detectors (e.g. “motion detected”) on the system map. This provides operators with a central overview of all access and intrusion states, allowing them to easily and remotely handle intrusion events.

Bosch Access Management System 3.0 is available for sale and makes access management simple, scalable, and always available.
You may also be interested in...

**Automatic Gates: Making The Right Investment For Access Control**

The experience of the COVID-19 pandemic has made us all more conscious of who is coming and going from our property. Whether it is a family... 

**Facial Recognition: Contactless Solutions For A Safe, Post-pandemic World**

Facial recognition technology has come a long way since it first came to market several years ago. Initially plagued with technical challenge...

**Thermal Cameras And Smart Cities: Preventing COVID-19 In Public Places**

With the pandemic still in full swing and no certainty as to when exactly it will come to an end, the world has been battling anxiety for mo...