

AEOS: powerful authorization possibilities

For companies using security management systems the way authorizations and access rights are handled is an important issue. Handling authorizations properly is essential because these define who has access where and at what time. AEOS has a unique authorization model to handle and manage the authorizations and access rights in your security management system. Additional features such as the Rule Engine and Security Level Management offer even more possibilities to manage authorizations.

In AEOS, **carriers** are persons or vehicles to which one or more identifiers can be issued. **Identifiers** can be badges, PIN codes, biometric characteristics or a combination of these.



Assigning and managing access rights

Contrary to what other security systems do, authorizations in AEOS are not assigned to identifiers but to carriers. This is a flexible method for the assignment and management of access rights, which is also less time consuming and a lot less susceptible to errors. The fact that authorizations are assigned to carriers makes it possible to handle multiple identifiers and to replace identifiers more easily. The unique AEOS authorization model allows the use of biometric verifiers, multiple templates and/or profiles, temporary authorizations and specific security conditions such as rules and security level management.

Authorization model

In AEOS, **carriers** are persons or vehicles to which one or more identifiers can be issued. **Identifiers** can be badges, PIN codes, biometric characteristics or a combination of these. Carriers can be given the right to use one or more **entrances** or entrance groups during a certain **time slot**. The authorizations in AEOS are defined by a combination of data: the carrier, the identifier(s) and the entrances with a **day/time schedule**. Those combinations are defined in a **template** that is easy to maintain and to assign to a carrier group. It is possible to assign multiple templates to one carrier. The template is a combination of a day/time schedule with an entrance (group). If none of the available templates match the authorizations you wish to assign to a specific carrier AEOS allows you to create a profile. A **profile** is a combination of an entrance (group) with a day/time schedule assigned to a single carrier.

Rule Engine

The AEOS authorization model has an additional feature that speeds up and simplifies authorization management: the Rule Engine. The Rule Engine can quickly and simply couple access authorizations for employees, vehicles, visitors or contractors to different attributes such as age, department or building. With just one click, authorizations can be applied to individuals or complete groups, locally or across the world. What's very unique is that the authorization can be updated as often as required, for example every hour. Access rights of employees leaving the company can automatically be blocked and authorizations of employees who change office location can immediately be switched to the relevant access rights for the new location.

Rule Engine case study

Imagine a large company with hundreds of employees. On a daily basis employees change function or office location, new employees join the company and others leave. All these personal data must be kept up to date in the access control system because access rights change along with these alterations. The security manager has to enter all the new and changed personal data into the access control system. Since this is a huge job, employee data and the accompanying access rights are hardly ever up to date, causing serious security risks. This can be avoided by importing the personal data from the Human Resources database and applying the AEOS Rule Engine. With the Rule Engine changes that were always done manually are now automated and executed error-free. This means that the authorizations are always up to date and security risks are reduced.

Security Level Management

Another additional feature in the AEOS security management system is to handle authorizations with Security Level Management. Security Level Management is used to create scenarios which give or deny particular groups of carriers access to certain zones in special situations, for example during crises or when dealing with various threat levels. Security level authorizations differ from the regular authorizations for entrance groups set by means of templates and profiles, but they are not an overall emergency scenario in which entrances (clustered in emergency groups) are all locked or unlocked. Security level authorizations are a refined type of access control, requiring alternative clustering of carrier groups, entrance groups and authorizations. Unlike regular authorizations, security level authorizations are not time-controlled. Security scenarios must be activated manually when they are needed, and deactivated manually when the situation returns to normal.

Features and Benefits

- Unique authorization model
- Authorizations assigned to carriers, allowing the use of multiple identifiers for one carrier
- Speedy and simplified authorization with the Rule Engine (product number: 8014205)
- Creation of security scenarios with Security Level Management (product number: 8015368)