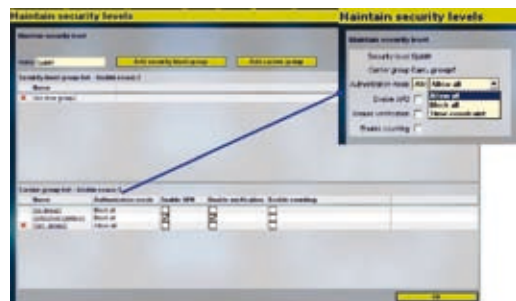


Security Procedures Support

Securing your buildings and premises involves a host of different aspects. In most organizations, a security manager puts the appropriate security measures in place by drawing up a Security Policy or Plan. Nedap's AEOS Security Management system can help implement this policy with its wide range of features geared towards specific security issues. These include automated responses to freely definable security breaches, security scenarios that can be activated at the touch of a button, and the ability to trace violations and automatically blacklist people and block their access.

- Response to events, actions, expiries
- Security Level Management
- Blacklist & Violations management
- E-mail, SMS, Pager interface
- Fully integrated into AEOS



Security Policy

Events and alarms generated by the security management system require a rapid and adequate response. AEOS provides several instruments that can help the security manager react appropriately. AEOS can generate automatic responses to various freely definable events, switch to a different access mode (security level scenario) at the touch of a button, or keep track of the number of violations a carrier has committed. The server software needed for such functions includes [Responses](#), [Security Level Management](#) and [Violations & Blacklist](#).

Responses

The Responses functionality allows security managers to ensure that a particular event automatically triggers a particular action. It is designed to raise the alarm or notify key people when an attempt is made to tamper with authorizations. The responses option makes it possible to respond to events, actions or expiries. The response itself may be the triggering of an alarm or notification of one or more people by e-mail or text message.

Response to event

Response to Event allows you to define a response to a particular occurrence (which is also recorded in the event monitor). For example, if an invalid badge is presented (event), a video link is activated (response). Or, if a person exceeds a permitted presence time (event), he or she is given a violation (response).

Response to Action

Response to Action allows you to define an action, such as a change to a person's data, which will either trigger an alarm or generate an automatic e-mail or text message to the person, the person's contact or a freely definable group of persons.

Response to Expiry

Response to Expiry allows you to define a response to a validity date that is nearly or already expired, regarding an individual's photo or authorizations for instance. The response will either trigger an alarm or alert the person, the person's contact or a freely definable group of persons by e-mail or text message.

Security Level Management

The automatic responses described above are intended to deal with minor breaches of your security system. In case of a serious security incident, you may need to take more drastic measures. AEOS Security Level Management allows you to pre-define any number of security scenarios that can be activated in a matter of seconds. In an emergency situation, you can switch to a different access mode and retain full control, so you continue to determine who has access to your premises. For example, you can pre-define the authorizations and carrier groups that will apply in case of a strike, a fire alarm, an open day or a visitor tour of the building. Switch to the appropriate scenario and restore your normal authorization scenario as soon as the „all clear“ is given.

Security Level Management is ideal for large companies operating in various locations, regions or countries; organizations with large and complex employee and visitor flows; and businesses that require extra security because of the hazardous or valuable commodities they deal with.

Violations and Blacklist

If your company enforces a code of conduct as part of its security policy, you can record violations of this code in AEOS. Violations & Blacklist management will help you to implement your company's safety & security regulations in your security management system. AEOS allows you to set an unlimited number of violations categories and corresponding sanctions. Sanctions may, for instance, include barring someone from entering the company's premises. An overview is available of the date, time and place of each violation recorded for a particular employee, visitor, contractor or vehicle. It is freely definable when somebody is to be blacklisted, which makes AEOS Violations & Blacklist Management a very supportive tool to enforce your Security Policy.

Features

- Responses to events, user actions, expiries
- Automatic alarms, e-mail and text messages
- Number of responses: unlimited
- Freely definable Security Scenarios
- Blacklist and Violations are freely definable
- Number of Security Levels: unlimited
- Number of Security Scenarios: unlimited