IndigoVision

Nedap AEOS Integration

Administrator's Guide

This manual was published on Wednesday, August 21, 2019.

Document ID: IU-IM-MAN033-2

Legal Considerations

Laws that can vary from country to country may prohibit camera surveillance. Please ensure that the relevant laws are fully understood for the particular country or region in which you will be operating this equipment. IndigoVision Ltd. accepts no liability for improper or illegal use of this product.

Copyright

Save as otherwise agreed with IndigoVision Limited and/or IndigoVision, Inc., this manual is provided without express representation and/or warranty of any kind. To the fullest extent permitted by applicable laws, IndigoVision Limited and IndigoVision, Inc. disclaim all implied representations, warranties, conditions and/or obligations of every kind in respect of this manual. Accordingly, save as otherwise agreed with IndigoVision Limited and/or IndigoVision, Inc., this manual is provided on an “as is”, “with all faults” and “as available” basis. Please contact IndigoVision Limited (either by post or by e-mail at technical.support@indigovision.com) with any suggested corrections and/or improvements to this manual.

Save as otherwise agreed with IndigoVision Limited and/or IndigoVision, Inc., the liability of IndigoVision Limited and IndigoVision, Inc. for any loss (other than death or personal injury) arising as a result of any negligent act or omission by IndigoVision Limited and/or IndigoVision, Inc. in connection with this manual and/or as a result of any use of or reliance on this manual is excluded to the fullest extent permitted by applicable laws.

Contact address

IndigoVision Limited

Charles Darwin House,
The Edinburgh Technopole,
Edinburgh,
EH26 0PY

TABLE OF CONTENTS

1 ABOUT THIS GUIDE

This guide is provided for system administrators integrating the Nedap AEOS system with the IndigoVision Control Center suite.

Safety notices

This guide uses the following formats for safety notices:

⚠ **Warning** *Indicates a hazardous situation which, if not avoided, could result in death or serious injury.*

⚠ **Caution** *Indicates a hazardous situation which, if not avoided, could result in moderate injury, damage the product, or lead to loss of data.*

Notice *Indicates a hazardous situation which, if not avoided, may seriously impair operations.*

💡 *Additional information relating to the current section.*

References

The following documents are referenced in this document:

- Control Center Help

  Start* > *IndigoVision* > *Control Center* > *Control Center Help

  Located on the Control Center workstation, by default
- IndigoVision Control Center Installation Guide

  Located on the Control Center CD.
- Integration Modules http://www.indigovision.com/products/Integration
- AEOS Socket Interface User Manual, version 19.

  Located within the ***Nedap AEOS installation media* > *Additional Programs* > *Socket Interface***
- AEOS Generic Event Descriptions, version 19.

  Located within the ***Nedap AEOS installation media* > *Additional Programs* > *Socket Interface***
- AEOS User Manual

  Located within the ***Nedap AEOS installation* > *User Manual***

2 OVERVIEW

The Nedap AEOS Integration allows alarms from a Nedap AEOS system to integrate into IndigoVision Control Center suite.

This document explains how to install and configure the Nedap AEOS Integration.

Compatibility

Please ensure you have properly installed, configured, and licensed the Nedap AEOS system.

System requirements

You can install Nedap AEOS Integration on the following Windows® Operating Systems with latest service packs applied:

- Windows® Server 2016
- Windows® Server 2012 R2
- Windows® Server 2012
- Windows® Server 2008 R2
- Windows® 10 (64-bit) version 1607 or later
- Windows® 8.1 (64-bit)
- Windows® 7 (64-bit)

If a firewall is enabled on your system, ensure that you add the Nedap AEOS Integration executable **IndigoVision.IntegrationCore.exe** to the list of exceptions.

Nedap AEOS requirements

The Nedap AEOS Integration is compatible and has been tested with Nedap AEOS Pro 2019.1.2.

► For supported Nedap AEOS event types, *see "Event numbers" on page 25*.

You can install the Nedap AEOS Integration on either the same machine as the Nedap AEOS, or on a different machine. If installing on a remote machine, ensure that both are configured to use the same time zone.

Licensing

The Nedap AEOS Integration is a licensed product, which you can install on a physical or virtual machine.

► For more information, *see "License the integration" on page 9*

3 INSTALLATION

This section describes how to install the Nedap AEOS Integration.

Before you install the Nedap AEOS, you must first configure the Nedap AEOS system:

1. Ensure that Nedap AEOS is running on the Nedap AEOS machine.
2. Create a new AEOS user dedicated for the Nedap AEOS Integration. The user must be part of a role with the following permissions:
   - Configuration, Socketconnection, Commands
   - Configuration, Socketconnection, Events
   - ► For more information on configuring a user for use with the AEOS Socket interface, see AEOS Socket Interface User Manual

To install the Nedap AEOS Integration:

1. Download the Nedap AEOS Integration from the support section of the IndigoVision website.
   - ► For more information, *see "References" on page 6*
2. Run the ***setup.exe*** file and follow the on-screen instructions. The Nedap AEOS Integration is installed to:

   C:\Program Files (x86)\IndigoVision\Integration\Nedap AEOS

   by default.
3. If the Microsoft .NET 4.7.2 Framework or later is not installed, then you are prompted to install it.
4. Once the installation is complete, request and install a software license for the Nedap AEOS Integration using the License Manager tool.
   - ► For more information, *see "License the integration" on page 9*
5. Configure the Nedap AEOS Integration.
   - ► For more information, *see "Configuration" on page 11*

License the integration

You must have a valid license that allows the IndigoVision Nedap AEOS Integration to run on a specific machine.

You can manage the software license using the License Manager tool, which is installed as part of the Nedap AEOS Integration standard installation.

1. Create a Client to Vendor file (c2v) that contains a fingerprint of the machine. This is then sent to IndigoVision Order Management.
2. Apply a Vendor to Client file (v2c) provided by IndigoVision.

You can transfer a license from one machine to another using the License Manager tool.

4 CONFIGURATION

To integrate Nedap AEOS alarm events into the IndigoVision Alarm Server, or remotely control Nedap AEOS doors using Control Center relays, perform the following steps:

1. Configure the Nedap AEOS Integration.
2. Configure IndigoVision Control Center.

Configure the Nedap AEOS Integration

The Integration Configuration Tool can be used to configure the events and system settings for the Nedap AEOS Integration:

1. Run the Integration Configuration Tool for Nedap AEOS Integration.

   Start > All Programs > IndigoVision Nedap AEOS Integration > Configure Nedap AEOS Integration
2. Optionally provide the System Alarm Server IP for System Events.
   - System Events report the status of the Nedap AEOS Integration and its connection to Nedap AEOS.
3. Provide the Integration IP of the Nedap AEOS Integration.
   - When the IndigoVision Nedap AEOS Integration is installed on a machine with multiple network adapters or multiple IP addresses, the Integration IP must be specified.
   - This must be the IP of the External System configured in Control Center.
4. If the System Alarm Server IP for System Events was provided, configure System Events.
   - Integration Online and Offline
   - Nedap AEOS Online and Offline
5. Provide the host of the Nedap AEOS server. This can be an IP address or host name.
6. Provide the port number for the AEOS interface service. This is configured as 8035 for the default Nedap AEOS installation.

   ► For more information on configuring the AEOS interface service port within Nedap AEOS, see AEOS Socket Interface User Manual
7. Provide the ***User*** and ***Password*** for the AEOS User that the Nedap AEOS Integration will use to connect to Nedap AEOS.

   ► For more information on the requirements for the AEOS User, *see "Installation" on page 9*
8. Specify the IndigoVision Alarm Servers that will receive events
   - Each Alarm Server supports up to 10,000 detectors.
   - If you require more than 10,000 Nedap AEOS alarms to be configured, or the Alarm Server has detectors for other sources configured (such as Advanced Analytics or Digital Input detectors), then you can split the configuration of Nedap AEOS alarms across multiple Alarm Servers.

9. Configure the Nedap AEOS event mappings for each Alarm Server.
   - The Nedap AEOS event configuration file for the Alarm Server opens in a new window.

   ► For more information, *see "Nedap AEOS event configuration files" on page 12*
10. Optionally, select Enable Relay Actions and Configure Relay Actions.

    ► For more information, *see "Remote control of doors" on page 13*
11. Click ***Finish*** to close the dialog and save your settings.
12. Click ***Yes*** to restart the service, or restart it manually using the Windows Services Utility.

Nedap AEOS event configuration files

This section covers the configuration for Nedap AEOS events that are sent from the Nedap AEOS system to the IndigoVision Control Center suite to activate detectors.

Nedap AEOS event configuration files contain information for mapping each Nedap AEOS event received from the Nedap AEOS system to the IndigoVision Control Center suite. A file must be configured for each Alarm Server.

There is one mapping entry per line in the mapping file. Each entry is a comma-separated pair.

Figure 1: Example of a Nedap AEOS event configuration file

```
# This file contains the ToIv mapping of Nedap AEOS events to IndigoVision
# external event input numbers.
#
# Each entry consists of three comma separated elements:
#
# Input Number, Nedap AEOS Event, Optional Description
#
# 1. The first element of each entry, InputNumber, is the positive integer
#    corresponding to the External Event input in the Alarm Server.
#
# 2. The second element, Nedap AEOS Event, describes the details of the event
#    within Nedap AEOS.
#
#    The Nedap AEOS event consists of 3 to 5 parts:
#        - Source:Event Number:AEpu Hostname
#        - Source:Event Number:AEpu Hostname:Behaviour Component
#        - Source:Event Number:AEpu Hostname:Behaviour Component:Sub Component
#
#    Source: Where the event originated. Typically "AEOS".
#
#    Event Number: 4-digit number for the type of event. For more details on the
#       Event Numbers, refer to the IndigoVision Nedap AEOS Integration Admin
#       Guide.
#
#    AEpu Hostname: The hostname for the AEpu that either triggered the event or
#       is connected to the Behaviour Component that triggered the event.
#
#    Behaviour Component (Optional): The Behaviour Component that triggered the
#       event. Not required if the event originated from an AEpu (for example an
#       AEpu becomes unreachable on the network).
```

```
#
#    Sub Component (Optional): Some events may include Sub Components, such as
#       named inputs, connected to a Behaviour Component.
#
# 3. An optional third field, separated by another comma can be added with
#    a description of the event mapping.
# Examples:
# 10, AEOS:1061:aepu-000da00b4706
# 11, AEOS:1005:aepu-000da00b4706:Entrance Door
# 12, AEOS:1142:aepu-000da00b4706:IntrusionComponent:PIR
# Example of an event with the optional description:
# 13, AEOS:1127:aepu-086m3trs2j8:TestDoor, Unassigned badge
# Example of an event with Unicode characters:
# 14, AEOS:1005:aepu-000da00b4706:Indigo☺Door
# The Nedap AEOS event cannot contain the characters '\', '{', '}' or ','.
# The following octal escape codes can be used to represent these characters.
# Character '\': => \134
# Character '{': => \173
# Character '}': => \175
# Character ',': => \054
# Example using octal escape codes when a door is called "Door, Front"
# 15, AEOS:1012:aepu-086m3trs2j8:Door\054 Front
```

Octal escape codes are required to configure Nedap AEOS events with special characters, such as comma and backslash.

Remote control of doors

The Nedap AEOS Integration allows operators to control doors from Control Center using relays. This feature needs to be enabled and configured using the Integration Configuration tool.

► For more information, *see "Configure the Nedap AEOS Integration" on page 11*

The installation provides a default Relay actions from IndigoVision configuration file (***FromIvRelays.conf***).

There is one mapping entry per line in the mapping file. Each entry is a comma-separated pair.

Figure 2: Example of a FromIvRelays configuration file

```
# This file maps IndigoVision external relay outputs to actions within the
# Nedap AEOS system.

# The following formats are used to define the relay outputs:
#
# Output Number, ACTION:AEpu Hostname:Behaviour Component, Optional Description
#
# 1. The first element of each entry, Output Number, is the positive integer
#    corresponding to the External Relay in Control Center.
#
# 2. The second element describes the action to be performed within Nedap AEOS.
#    It consists of 3 parts
#        ACTION:AEpu Hostname:Behaviour Component
#
```

```
#ACTION: The action to perform on the named door. Possible values:
#    LOCK         - A relay with the LOCK action configured will lock the
#                   associated Behaviour Component on relay activation and
#                   activate access control again on relay deactivation.
#
#    UNLOCK       - A relay with the UNLOCK action configured will unlock
#                   the associated Behaviour Component on relay activation
#                   and activate access control again on relay deactivation.
#
#   PROVIDE_ACCESS  -  A relay with the PROVIDE_ACCESS action configured will
#                      unlock the Behaviour Component on relay activation for
#                      the unlock time configured in Nedap AEOS. Relay deactivations
#                      are not supported.
#
#AEpu Hostname: The host name for the AEpu that is connected to the AEbc Component
#that should receive the action.
#
#Behaviour Component: The AEbc Component that should receive the action.
#
#
# Examples:
# 1, LOCK:aepu-000da00b4706:Entrance Door
# 2, UNLOCK:aepu-000da00b4706:Middle Door
# 3, PROVIDE_ACCESS:aepu-000da00b4706:Exit Door
#
# Example of an action with the optional description:
# 4, LOCK:aepu-086m3trs2j8:TestDoor, Lock/unlock the test door
#
# Example of an action with Unicode characters:
# 5, PROVIDE_ACCESS:aepu-000da00b4706:Indigo☺Door
#
# The AEpuName and AEbcName cannot contain the characters ':', '\', '{', '}', ','
# or leading or trailing whitespace.
# The following octal escape codes can be used to represent these characters.
# Character ':': => \072
# Character '\': => \134
# Character '{': => \173
# Character '}': => \175
# Character ',': => \054
#
# Example using octal escape codes when a door is called "Door, Front"
# 4, LOCK:aepu-086m3trs2j8:Door\054 Front
```

Configure IndigoVision Control Center

Zones and detectors must be created in Control Center for the configured Nedap AEOS events. If the Integration Online, Integration Offline, Nedap AEOS Offline or Nedap AEOS Online system events have been specified, then they must be configured in Control Center. Additionally, external relays must be configured for each relay number mapped to Nedap AEOS actions.

Create a new external system

The IP address entered is the IP address of the host running the Nedap AEOS Integration. Refer to the Control Center online help about creating a new external system.

Create a new zone and external detector for Nedap AEOS events

You must create zones and detectors for the configured Nedap AEOS events using one of the following methods:

1. Manually create the zones and external detectors within Control Center.
   - Add a new zone for each unique alarm you want to report in Control Center.
   - Within the zone, create a new external detector for the external system. Specify the Input Number as the Activation Input Number configured for the event in the Nedap AEOS event configuration file of the Nedap AEOS Integration.
   - IndigoVision recommends that you configure the zone name description in Control Center to closely match the Nedap AEOS alarm name. This helps to ensure there is no confusion in correlating events.
2. Use the IndigoVision Import Alarm Sources tool to automatically create zones and detectors for each event within a Nedap AEOS event configuration file.
   - After you have edited the Nedap AEOS event configuration file, accessible through the Integration Configuration Tool, with all the supported events, configure an IndigoVision Alarm Server using the IndigoVision Import Alarm Sources tool.
   - You can download the Import Alarm Servers tool from the IndigoVision website.
   - Every time an event is added to Nedap AEOS event configuration file, run the tool again to create new zones and detectors.

Create external relays

Add a new external relay in Control Center for each relay action configured in the ***FromIvRelays.conf*** file.

► For more information about creating external relays, refer to the Control Center help.

5 TROUBLESHOOTING

This chapter provides troubleshooting information for the Nedap AEOS Integration.

Service does not start

If the IndigoVision Nedap AEOS Integration does not start properly from Windows Services, then open the most recent log file and look at the latest two messages marked as `FATAL`.

If no `FATAL` level log messages are available:

1. Open Windows **Event Viewer**
2. Navigate to ***Windows Logs > Application***
3. Find one or more events logged at `ERROR` level and with ***Source*** `IndigoVision IntegrationCore Service`

The ***General*** field describes why the service is not starting.

Unable to connect to the Nedap AEOS socket interface service

If you are unable to connect to the Nedap AEOS system server, check the following:

1. Check the log file for `ERROR` level messages and follow the advice in the error message.
2. If the log files contain errors related to connection failures:
   - Ensure that the Server Port and Server Host have been correctly configured.
   - ► For more information on how to specify the Server Port and Server Host within the Nedap AEOS Integration, *see "Configure the Nedap AEOS Integration" on page 11*
   - ► For more information on how to configure the port used by the Nedap AEOS Socket interface, see AEOS Socket Interface User Manual
   - Ensure that the firewalls on the machine running the Nedap AEOS Integration and also the machine running Nedap AEOS are both configured to allow TCP connections for the Server Port.
   - If using a host name, ensure that DNS is correctly configured or provide the IP address of the machine running Nedap AEOS.
3. If you see an error message such as:

   ```
   [NedapAEOSIntegration.Aeos.StartupManager]: Login failed. The maximum number of
   concurrent logins for this user has been reached. Please log out from another
   session.
   ```

   This indicates there is one or more existing sessions for that user, such as within a browser or another service and the user cannot login again. Either terminate one of the existing sessions or configure the user to have a higher number of permitted sessions.

You can remove existing sessions from ***AEOS > Management > Maintain connected users***.

4. If you see a login error message similar to the following:

```
[NedapAEOSIntegration.Aeos.StartupManager]: Login failed. The user does not have a
valid configuration for use with the Nedap AEOS Integration.
```

   This indicates that the user does not have the necessary Socket interface permissions as stated within the Installation section of this document.

   ► For more information on configuring a user for use with the AEOS Socket interface, see AEOS Socket Interface User Manual

5. If no error messages are seen, enable INFO level logging and check for messages stating that the connection has been made successfully.

```
[NedapAEOSIntegration.Connection.AeosConnectionManager]: The connection to AEOS
interface service has been fully established.
```

   ► For more information, *see "Logging configuration" on page 23*

Alarms not appearing in Control Center

If alarms are not appearing in Control Center, then the following end-to-end check for a single alarm may help you to determine the source of the problem:

1. Verify that the Nedap AEOS Integration is running.
2. Enable `INFO` level logging.

   ► For more information, *see "Logging configuration" on page 23*.

   This enables the Nedap AEOS Integration to log all alarms and events received from the monitored system, not only those that are mapped in the event configuration file.

3. If the Nedap AEOS Integration cannot contact the Alarm Server, you will see a log message similar to the following:

```
[ERROR][IntegrationCore.Core.Event.BindingKit]: Failed to send ToIv event.
```

4. Ensure that the Alarm Server is online, and that the firewall is not blocking communication. Refer to the IndigoVision Control Center Installation Guide for more information about IndigoVision Firewall Requirements.

   ► For more information, *see "References" on page 6*.

5. Inspect the log file for messages showing that the event has been received:

```
[INFO ][NedapAEOSIntegration.ToIv.GenericEventHandler]: Received AEOS Generic
Event 'AEOS:1005:aepu-000da00b4706:Entrance Door'.
```

   a. If the event is within the log file, then look for a log message confirming that the event has been sent to the Alarm Server:

```
[INFO][IntegrationCore.Core.Event.BindingKit]: ToIv stateless event sent to
Alarm Server '10.1.219.11' with external input number '104' from IP
'10.1.219.1'. UTC time of the event was '03/12/2018 11:16:23'.
```

   If you see the above log message, then the Integration has successfully processed the event, however it the alarm or detector may not configured correctly, in which case progress to steps 6 & 7.

   If you do not see the log message confirming that the message was sent, then the event is not correctly configured to forward this event to the IndigoVision system, in which case you will see a log message similar to the following:

```
2018-08-30 10:42:08,335 [INFO ][IntegrationCore.Core.EventManager]: ToIv event
'AEOS:1005:aepu-000da00b4706:Entrance Door' is not configured to send to any
Alarm Server.
```

   The event can be configured using the Integration Configuration Tool.

   ► For more information on how to configure events, *see "Configure the Nedap AEOS Integration" on page 11*

b. If there are no messages confirming that the event has been received then it may not have been received within Nedap AEOS, or the event is not correctly configured within Nedap AEOS.

6. Verify that you have:
   - created corresponding zones and external detectors
   - set the zones
   - enabled external detectors in Control Center

   In ***Setup***, select the relevant site in the ***Alarms*** tab of the Site Explorer, then:

   a. Select the ***External Systems*** tab. Ensure that you have created an External System with the IP address of the PC running the Nedap AEOS Integration.

   b. Select the ***Zones*** tab. Ensure that you have created a zone containing an external detector with the Input Number as the external input number configured for the event.

   c. Ensure that the zone belongs to the nominated Alarm Server.

   Right-click the zone, then select ***Properties*** > ***Zone***.
7. Ensure that the Alarm Server containing the zones and detectors for Nedap AEOS alarms is the same Alarm Server that is configured using the Integration Configuration Tool.
8. Verify that the System user is authorized to write to the log file regardless of the current login user's authorization.

Activations have the incorrect time in Control Center

If you see incorrect activation times for detectors within Control Center, the time zones for Nedap AEOS Integration and Nedap AEOS do not match.

The machine running the Nedap AEOS Integration must be configured to use the same time zone as the machine running Nedap AEOS and AEpu controllers. You should adjust the time zone within the Windows **Date & Time settings**.

Nedap AEOS Integration is slow to start

If no internet access is available, a standard security check causes the Nedap AEOS Integration service to start slowly, taking up to one minute.

To resolve this, disable ***Check for publisher's certificate revocation***, which is typically found in the ***Advanced*** tab of Internet Options. However, this must be disabled for the Windows user running the service, which by default is Local System.

To disable ***Check for publisher's certificate revocation*** for the Local System user, edit the registry key:

1. Start the Windows **Registry Editor** (Regedit.exe).
2. Navigate to ***HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\WinTrust\TrustProviders\Software Publishing***.
3. Double-click ***State***.
4. Set the ***Value*** data to `23e00` for hexadecimal or `146944` in decimal.
5. Click ***OK***.
6. Quit Registry Editor.

Optionally, perform the same steps for the default registry key: ***HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing***.

If you have configured a different user to run the service, disable ***Check for publisher's certificate revocation*** for that user.

If you are able to log into Windows with this user account, use the method described to disable the option.

Unable to control a door in Control Center

Do the following if you see this error:

```
Failed to perform action RelayName: Activate
```

- Verify that the IndigoVision Nedap AEOS Integration Module is running and online.
- Verify that ***EnableFromIvRelays*** in the System Configuration file is set to true.
- Check ***FromIvRelays.conf*** to ensure that the relay output number configured matches the external relay within Control Center.

If you get a completion message within Control Center but the action is not being performed on the Nedap AEOS Behaviour Component, do the following:

1. Enable INFO level logging.

   ► For more information, *see "Logging configuration" on page 23*

   This allows the Integration Module to log all relay actions sent to Nedap AEOS.
2. Verify that the Integration Module is sending relay actions to the Nedap AEOS by activating the relay and then checking the logs for messages relating to success or failure.

   For example:

   ```
   2019-07-23
   15:30:43,520[INFO][NedapAEOSIntegration.Connection.AeosConnectionManager]:
   Performing LOCK on Door on AEpu: aepu-000da00b4706
   ```

If the Integration Module reports an unsupported command, verify that the named Behaviour Component is an Access Point.

If the Integration Module reports an unreachable AEpu or Behaviour Component, verify that both are correct in ***FromIvRelays.conf*** and that both are online.

If the Integration Module reports any other error or no errors, refer to the Nedap AEOS User Manual.

Unable to temporarily unlock a door from Control Center

The ***PROVIDE_ACCESS*** action only works if the access point has access control activated. Locking or unlocking a door using relays deactivates access control for the access point. To activate access control for an access point, deactivate a ***LOCK*** or ***UNLOCK*** relay targeting the access point or do the following:

1. Open the Nedap AEOS client in a browser (`https://<Nedap Aeos Machine Hostname/IP Address>:8443/main`).
2. Navigate to ***Entrance > Access point > (De)activate access control***.
3. Find the access point using the search functions.

   ► For more information, refer to the AEOS User Manual.
4. Tick the box to the left of the access point in the list.

5. Select the ***Access Control Activated*** radio button at the bottom of the page.
6. Click ***Set***.

A LOGGING CONFIGURATION

Logging is configured with a separate file, which allows you to customize logging and to manage backup log files.

You need only to change this file when you require more detail on events received, or as advised by IndigoVision.

To access this file, navigate to the following location:

Start > All Programs > IndigoVision Nedap AEOS Integration > Logging Configuration for Nedap AEOS Integration

To adjust the logging level, modify ***level*** in the root section. You can change this to one of the following values:

- **DEBUG**: Verbose logs with comprehensive details on operations.
- **INFO**: Details successful events and behavior as well as all warnings and errors.
- **WARN**: All messages logged are warning or error messages that indicate that the Nedap AEOS Integration is functioning incorrectly and may require action.
- **ERROR**: Only capture messages where a failure has occurred and may require action.
- **FATAL**: Critical errors where the Nedap AEOS Integration cannot continue.

For example, to increase the default logging level to include confirmation of events sent successfully:

```
<level value="INFO"/>
```

You can customize the retention of log files by editing the following values:

- ***maximumFileSize***: The size of individual log files before a new file is created.
- ***maxSizeRollBackups***: The number of backup files kept. Older files are removed when this limit is reached and new files are required.

IndigoVision recommends that you do not change any other settings unless advised to by IndigoVision.

B EVENT NUMBERS

Events received from Nedap AEOS will contain an Event Number that identified the type of event. This number is used within the event mapping.

To help identify the events of interest, the following table provides a list of supported events within Nedap AEOS with a description. If you receive an event with an Event Number not listed here, view the AEOS Generic Event Descriptions document, which is located within the ***Nedap AEOS installation media > Additional Programs > Socket Interface***.

Events 1000-1099

Event type number	Version	Event description
1000		Unknown AEOS event Event is received that is not known by AEOS
1001		Access point locked The access point has entered the ‘locked’ state.
1002		Access point normal The access point has entered the ‘normal’ state.
1003		Access point unlocked The access point has entered the ‘unlocked’ state.
1004		Authorization service IO event Fired by an access point in case there was an I/O error during a call to an authorization service.
1005		Direct door alarm start Door has been forced opened (alarm, no legal action)
1006		Direct door alarm end Door is closed after 1005
1007		Door open too long start Door is longer open than the specified ‘Door Open alarm time’
1008		Door open too long end Door is closed after 1007
1009		Lock supervisor normal Supervising function of lock output returns to normal (no sabotage)
1010		Lock supervisor shortcut Lock output is shortcut (alarm, sabotage)
1011		Lock supervisor open Lock output is open (alarm, sabotage)
1012		Door manual unlock start Input activated that manual unlock on Access Point
1013		Door manual unlock end Input released after 1012
1014		No authorization service

Event type number	Version	Event description
		Fired by an access point in case there were no authorization services available during an authorization request.
1015		Authorized badge access Authorized badge has been accessed to Access Point
1034		Input contact changed, passive Input has been changed to passive state
1035		Input contact changed, active Input has been changed to active state
1036		Input contact changed, sabotage open Connection to input is open (alarm, sabotage)
1037		Input contact changed, sabotage shortcut Connection to input is shortcut (alarm, sabotage)
1040		Behavior test mode start Test mode activated at AEmon for this AEbc
1041		Behavior test mode end End of test mode for this AEbc
1042		Device connected Device (AEbc or part of AEbc) has been discovered by AEpu
1043		Device disconnected A software device (AEbc or part of AEbc) has been lost by AEpu
1044		Device network operational Network connection recovered after lost (1045)
1045		Device network not operational Network connection lost with device
1046		AEPack discovered AEpack (hardware) been discovered by AEpu
1047		AEPack removed Before discovered AEpack (hardware) has been lost (removed)
1048		AutomaticUnlockEvent begin Unlock output is been activated by the Automatic Unlock Schedule
1049		AutomaticUnlockEvent end End of 1048, Unlock output is deactivated (after Unlock time)
1050		EmergencyUnlockedEvent begin Unlock output has been activated by the Emergency Unlock Input
1051		EmergencyUnlockedEvent end End of 1050, Unlock output is deactivated (after Unlock time)
1058		DeviceIOEvent Aepack recovered
1059		DeviceIOEvent Aepack failed
1060		AEpuStatusEvent reachable (Generated by AEOS Server) AEpu has been reached by AEOS server (lookup server)
1061		AEpuStatusEvent unreachable (Generated by AEOS Server) AEpu has not been reached any longer by AEOS server (lookup server)

Event type number	Version	Event description
1062		AccessPointModificationFailedEvent LOCK Action to set access point to this state failed
1063		AccessPointModificationFailedEvent NORMAL Action to set access point to this state failed
1064		AccessPointModificationFailedEvent UNLOCK Action to set access point to this state failed
1065		AccessPointModificationFailedEvent NOTIFY_ENTRANCE_ASSIGNMENT
1066		AccessPointModificationFailedEvent NOTIFY_ENTRANCE_REMOVAL
1067		AccessPointModificationFailedEvent SET_RELATED_ENTRANCE Action to set access point to this state failed, access point cannot be linked to Entrance ID
1068		AccessPointModificationFailedEvent REMOVE_RELATED_ENTRANCE Action to set access point to this state failed, Entrance ID cannot be removed from access point
1069		AccessPointModificationFailedEvent SET_SCHEDULES Action to set access point to this state failed, Time Schedules cannot be set
1070		AccessPointModificationFailedEvent REMOVE_SCHEDULES Action to set access point to this state failed, Time Schedules cannot be removed
1071		AccessPointModificationFailedEvent SET_RELATED_ENTRANCE_AND_SCHEDULES
1072		AccessPointModificationFailedEvent EMERGENCY_UNLOCK Action to set access point to this state failed
1073		AccessPointModificationFailedEvent EMERGENCY_LOCK Action to set access point to this state failed
1074		AccessPointModificationQuitEvent LOCK Action to set access point to this state stopped after having failed for a predefined number of retries.
1075		AccessPointModificationQuitEvent NORMAL Action to set access point to this state stopped after having failed for a predefined number of retries.
1076		AccessPointModificationQuitEvent UNLOCK Action to set access point to this state stopped after having failed for a predefined number of retries.
1077		AccessPointModificationQuitEvent NOTIFY_ENTRANCE_ASSIGNMENT Action to set access point to this state stopped after having failed for a predefined number of retries.
1078		AccessPointModificationQuitEvent NOTIFY_ENTRANCE_REMOVAL Action to set access point to this state stopped after having failed for a predefined number of retries.
1079		AccessPointModificationQuitEvent SET_RELATED_ENTRANCE Action to set access point to this state stopped after having failed for a predefined number of retries.
1080		AccessPointModificationQuitEvent REMOVE_RELATED_ENTRANCE Action to set access point to this state stopped after having failed for a predefined number of retries.
1081		AccessPointModificationQuitEvent SET_SCHEDULES

Event type number	Version	Event description
		Action to set access point to this state stopped after having failed for a predefined number of retries.
1082		AccessPointModificationQuitEvent REMOVE_SCHEDULES Action to set access point to this state stopped after having failed for a predefined number of retries.
1083		AccessPointModificationQuitEvent SET_RELATED_ENTRANCE_AND_SCHEDULES Action to set access point to this state stopped after having failed for a predefined number of retries.
1084		AccessPointModificationQuitEvent EMERGENCY_UNLOCK Action to set access point to this state stopped after having failed for a predefined number of retries.
1085		AccessPointModificationQuitEvent EMERGENCY_LOCK Action to set access point to this state stopped after having failed for a predefined number of retries.
1086		BooleanStateChangedEvent True Toggle output has been set to True
1087		BooleanStateChangedEvent False Toggle output has been set to False
1092		InhibitInputSabotagedEvent begin Inhibit input (set AEbc to state Inhibit) is sabotaged (alarm, sabotage)
1093		InhibitInputSabotagedEvent end End of 1092
1094		InhibitEvent begin Inhibit input is been activated (set AEbc to state inhibit)
1095		InhibitEvent end End of 1094
1099		Sequence Error Generated by SMA when there is an error in the sequence of event numbers. This event is not generated from AEOS.

Events 1100-1199

Event type number	Version	Event description
1103		InputSabotagedEvent begin Input is sabotaged (alarm, sabotage)
1104		InputSabotagedEvent end End of 1103
1105		NoBookingEvent Booking contact has not been activated inside the ‘Booking time out time’
1106		CCFailureEvent, Slide not opened Card Collector CC100 slide is not been opened after card is been thrown in
1107		CCFailureEvent, Slide opened to long Failure in Card Collector CC100 device

Event type number	Version	Event description
1108		CCillegalCardInsertedEvent Card inserted in the card collector is not the same for which the card collector was opened
1109		AntennaMonitorAlarmEvent, is sabotaged Antenna has been sabotaged (alarm, sabotage)
1110		AntennaMonitorAlarmEvent, no alarm End of 1109
1111		ThresholdGuardAlarmEvent, Level is lower than threshold Threshold value has been exceeded to a lower value than specified
1112		ThresholdGuardAlarmEvent, Level is equal or higher than threshold Threshold value has been exceeded to a higher value than specified
1113		ApbGrantAccessEvent, soft ABP APB failed, in case of soft APB Access granted
1114		ApbGrantAccessEvent, Zone Manager was not available APB failed, because the APB Zone Manager couldn't be reached
1115		ApbCarrierResetEvent, One person is reset by the system APB level for one person has been by reset from the AEOS server
1116		ApbCarrierResetEvent, More than one person is reset by the system Same as 1115, but for more than one person
1117		ApbCarrierResetEvent, One person is reset by a user APB level for one person has been by reset by a user
1118		ApbCarrierResetEvent, More than one person is reset by the a user Same as 1117, but for more than one person
1119		BadgeNoAccessEvent, verification has no result Unauthorized badge, Verification error (for example PIN code fault)
1120		BadgeNoAccessEvent, verification alarm Unauthorized badge, Verification alarm (for example PIN last digit entered twice)
1121		BadgeNoAccessEvent, authorization has no result Unauthorized badge
1122		BadgeNoAccessEvent, verification invalid Unauthorized badge, Verification is invalid
1123		BadgeNoAccessEvent, verification aborted Unauthorized badge, Verification is aborted by the user
1124		BadgeNoAccessEvent, internal error (i) // impossible
1125		BadgeNoAccessEvent, internal error (e) // impossible
1126		BadgeNoAccessEvent, internal error (w) // impossible
1127		BadgeNoAccessEvent, unassigned badge Unauthorized badge, badge is not assigned to a carrier
1128		BadgeNoAccessEvent, outside schedule Unauthorized badge, badge is offered to antenna outside valid day / time schedule
1129		BadgeNoAccessEvent, not valid yet/anymore Unauthorized badge, badge is not valid (begin date, end date)
1130		BadgeNoAccessEvent, internal error // invalid (nonexistent) schedule

Event type number	Version	Event description
1131		BadgeNoAccessEvent, no authorization for this entrance Unauthorized badge, badge has no authorization for this entrance
1132		BadgeNoAccessEvent, APB invalid direction Unauthorized badge, direction for APB is wrong
1133		BadgeNoAccessEvent, APB request from unknown entrance Unauthorized badge
1134		BadgeNoAccessEvent, APB auth. req. already running Unauthorized badge, for this carrier there is already an APB authorization request running (for example, if this badge has been offered to another entrance while the first entrance is still not booked)
1135		BadgeNoAccessEvent, APB illegal presence Unauthorized badge
1136		BadgeNoAccessEvent, APB unavailable zone manager Unauthorized badge, because the APBZoneManager isn't available
1137		BadgeNoAccessEvent, APB incorrect configured AEpu Unauthorized badge because APB was not correctly configured
1138		VerificationAlarmEvent
1139		InvalidVerificationEvent
1140		InvalidVerifierEvent
1141		NoAccessControlServiceEvent
1142	1.5	ZoneChangedEvent, Burglary, active IntrusionDetection: Zone for Burglar is set to active This event is generated by an intrusion component, while the system is not armed.
1143	1.5	ZoneChangedEvent, Burglary, passive IntrusionDetection: Zone for Burglar is set to passive
1144	1.5	ZoneChangedEvent, Walk-in/out, active IntrusionDetection: Zone for Walk-In/Out is set to active
1145	1.5	ZoneChangedEvent, Walk-in/out, passive IntrusionDetection: Zone for Walk-In/Out is set to passive
1146	1.5	ZoneChangedEvent, Fire, active IntrusionDetection: Zone for Fire is set to active
1147	1.5	ZoneChangedEvent, Fire, passive IntrusionDetection: Zone for Fire is set to passive
1148	1.5	ZoneChangedEvent, Technical, active IntrusionDetection: Zone for Technical is set to active
1149	1.5	ZoneChangedEvent, Technical, passive IntrusionDetection: Zone for Technical is set to passive
1150	1.5	ZoneChangedEvent, System switch, active IntrusionDetection: Zone for SystemSwitch is set to active
1151	1.5	ZoneChangedEvent, System switch, passive IntrusionDetection: Zone for SystemSwitch is set to passive
1152	1.5	ZoneChangedEvent, Reset alarm, active IntrusionDetection: Zone for ResetAlarm is set to active

Event type number	Version	Event description
1153	1.5	ZoneChangedEvent, Reset alarm, passive IntrusionDetection: Zone for ResetAlarm is set to passive
1154	1.5	ZoneChangedEvent, Sabotage, active IntrusionDetection: Sabotage output is active
1155	1.5	ZoneChangedEvent, Sabotage, passive IntrusionDetection: Sabotage output is passive
1160		InputSabotagedEvent, Sabotaged open
1161		InputSabotagedEvent, Sabotaged shortcut
1174		StateChangedEvent, Burglary alarm, active IntrusionDetection state for Burglary alarm has changed to active
1175		StateChangedEvent, Burglary alarm, passive IntrusionDetection state for Burglary alarm has changed to passive
1176		StateChangedEvent, Sabotage alarm, active IntrusionDetection state for Sabotage alarm has changed to active
1177		StateChangedEvent, Sabotage alarm, passive IntrusionDetection state for Sabotage alarm has changed to passive
1178		StateChangedEvent, Fire alarm, active IntrusionDetection state for Fire alarm has changed to active
1179		StateChangedEvent, Fire alarm, passive IntrusionDetection state for Fire alarm has changed to passive
1180		StateChangedEvent, Technical alarm, active IntrusionDetection state for Technical alarm has changed to active
1181		StateChangedEvent, Technical alarm, passive IntrusionDetection state for Technical alarm has changed to passive
1182		StateChangedEvent, Zone ignored, active IntrusionDetection state for ignoring zone alarm has changed to active
1183		StateChangedEvent, Zone ignored, passive IntrusionDetection state for ignoring zone alarm has changed to passive
1184		StateChangedEvent, Buzzer, active IntrusionDetection Buzzer is set to active
1185		StateChangedEvent, Buzzer, passive IntrusionDetection Buzzer is set to passive
1186		StateChangedEvent, Alarm signal, active IntrusionDetection Alarm signal is set to active
1187		StateChangedEvent, Alarm signal, passive IntrusionDetection Alarm signal set to passive
1188		StateChangedEvent, Fire alarm signal, active IntrusionDetection Fire alarm signal is set to active
1189		StateChangedEvent, Fire alarm signal, passive IntrusionDetection Fire alarm signal is set to passive
1190		StateChangedEvent, System ON, active IntrusionDetection System ON is set to active

Event type number	Version	Event description
1191		StateChangedEvent, System ON, passive IntrusionDetection System ON is set to passive
1192		StateChangedEvent, System NOT OK, active IntrusionDetection System NOT OK is set to active
1193		StateChangedEvent, System NOT OK, passive IntrusionDetection System NOT OK is set to passive
1194		StateChangedEvent, Reset fire, active IntrusionDetection Reset fire is set to active
1195		StateChangedEvent, Reset fire, passive IntrusionDetection Reset fire is set to passive
1196		ProvideAccessEvent
1197		StateChangedEvent, Panic alarm, active IntrusionDetection Panic alarm has changed to active
1198		StateChangedEvent, Panic alarm, passive IntrusionDetection Panic alarm has changed to passive
1199	2.2.2	BadgeNoAccessEvent, person is blocked (blacklisted) Unauthorized badge, person is blocked (blacklisted)

Events 1200-1299

Event type number	Version	Event description
1200		BadgeNoAccessEvent, verification device does not know carrier Unauthorized badge, Verification is not available for this carrier
1201		BadgeNoAccessEvent, no authorization for this entrance
1202		BadgeNoAccessEvent, person is blocked Unauthorized badge, person is blocked
1207		BadgeNoAccessEvent, authorization is not yet valid
1208		BadgeNoAccessEvent, authorization has expired
1209		PowerSupplyInputAlarmEvent, Accu Capacity is lower than threshold PowerMonitoring detects that Battery Capacity (Accu) goes below specified value
1210		PowerSupplyInputAlarmEvent, Accu Capacity is equal or higher than threshold PowerMonitoring detects that Battery Capacity (Accu) exceeds specified value
1211		PowerSupplyInputAlarmEvent, Vraw is lower than threshold PowerMonitoring detects that Vraw (input voltage for Power Supply) goes below specified value
1212		PowerSupplyInputAlarmEvent, Vraw is equal or higher than threshold PowerMonitoring detects that Vraw (input voltage for Power Supply) exceeds specified value
1213		PowerSupplyInputAlarmEvent, Temperature is lower than threshold PowerMonitoring detects that Temperature of Power Supply goes below specified value
1214		PowerSupplyInputAlarmEvent, Temperature is equal or higher than threshold PowerMonitoring detects that Temperature of Power Supply exceeds specified value

Event type number	Version	Event description
1215		PowerSupplyInputAlarmEvent, Vaccu is lower than threshold PowerMonitoring detects that Battery Voltage (Accu) goes below specified value
1216		PowerSupplyInputAlarmEvent, Vaccu is equal or higher than threshold PowerMonitoring detects that Battery Voltage (Accu) exceeds specified value
1217		PowerSupplyInputAlarmEvent, Vout is lower than threshold PowerMonitoring detects that Output Voltage of PowerSupply goes below specified value
1218		PowerSupplyInputAlarmEvent, Vout is equal or higher than threshold PowerMonitoring detects that Output Voltage of PowerSupply exceeds specified value
1219		PowerSupplyInputAlarmEvent, Iout is lower than threshold PowerMonitoring detects that Output Current of PowerSupply goes below specified value
1220		PowerSupplyInputAlarmEvent, Iout is equal or higher than threshold PowerMonitoring detects that Output Current of PowerSupply exceeds specified value
1221		PowerSupplyStateChangeEvent, Mains + Emergency PowerMonitoring detects that Mains (230VAC) and Emergency (24VDC) are available at startup
1222		PowerSupplyStateChangeEvent, Mains + Battery PowerMonitoring detects that Mains (230VAC) and Battery (24VDC) are available at startup
1223		PowerSupplyStateChangeEvent, Mains PowerMonitoring detects that only Mains (230VAC) is available at startup
1224		PowerSupplyStateChangeEvent, Emergency PowerMonitoring detects that only Emergency (24VDC) is available at startup
1225		PowerSupplyStateChangeEvent, Battery PowerMonitoring detects that only Battery (24VDC) is available at startup
1226		PowerSupplyStateChangeEvent, Undefined PowerMonitoring undefined event
1227		CountGroupAlMostReachedMaximumEvent The Counter value for Group at the CountZoneManager exceeds the ‘high’ value
1228		CountGroupMaximumNoLongerReachedEvent The Counter value for Group at the CountZoneManager returns a value below ‘high’
1229		CountGroupMaximumReachedEvent The Counter value for Group at the CountZoneManager has reached the 'max’ value
1230		CountZoneAlMostReachedMaximumEvent The Counter value for Zone at the CountZoneManager exceeds the ‘high’ value
1231		CountZoneMaximumNoLongerReachedEvent The Counter value for Zone at the CountZoneManager returns a value below ‘high’
1232		CountZoneMaximumReachedEvent The Counter value for Zone at the CountZoneManager reaches the 'max’ value
1233		BadgeNoAccessEvent, Count: unknown person/vehicle Unauthorized badge, the person/vehicle is unknown at the CountZoneManager
1234		BadgeNoAccessEvent, Count: unknown entrance Unauthorized badge, the entrance for this badge reading is unknown at the CountZoneManager
1235		BadgeNoAccessEvent, Count: maximum is reached Unauthorized badge, the CountZoneManager detects that the maximum for Group or Zone has been reached

Event type number	Version	Event description
1236		BadgeNoAccessEvent, Count: invalid direction Unauthorized badge, the CountZoneManager detects an invalid direction for this movement
1237		BadgeNoAccessEvent, Count: unknown countgroup/zone combination Unauthorized badge, the CountZoneManager detects an unknown countgroup/zone combination
1238		BadgeNoAccessEvent, Count: unavailable count manager Unauthorized badge, the CountZoneManager isn't available
1239		AlarmSwitchedEvent, Alarm on
1240		AlarmSwitchedEvent, Alarm off
1241		AlarmSwitchedForcedEvent, Alarm on
1242		AlarmSwitchedForcedEvent, Alarm off
1243		AlarmSwitchTimeOutEvent, Alarm on
1244		AlarmSwitchTimeOutEvent, Alarm off
1245		AnalogMonitorAlarmEvent, Alarm off
1246		AnalogMonitorAlarmEvent, Above Maximum Value at AnalogqMonitor exceeds ‘high’ value
1247		AnalogMonitorAlarmEvent, Below Minimum Value at AnalogqMonitor returns below ‘high’ value
1248		AnalogMonitorAlarmEvent, Outside of measuring range Value at AnaloggMonitor is out of measuring range
1249		CounterMinAlarmEvent, Counter below minimum Counter value (Counter AEbc) tries to go below minimum value specified
1250		CounterMaxAlarmEvent, Counter above maximum Counter value (Counter AEbc) tries to go above maximum value specified
1251		CountGrantAccessEvent Counter value (Counter AEbc)
1252		Counter value (Counter AEbc) Counter value (Counter AEbc) is changed
1253		BadgeNoAccessEvent, verification no code Unauthorized badge, no verification data hasis been received
1254		SIAEvent IntrusionDetection (IntrusionGalaxy AEbc) event
1255		DeviceDiscoveryEvent AEpack has been detected at the AEbus ({0} with adress {1} discovered)
1256		DeviceRemovalEvent AEpack is been removed from the AEbus ({0} with adress {1} removed)
1257		AEpuApplicationStartedEvent AEpu application is started (or restarted)
1258		AEpuReloadedEvent AEpu is been reloaded with all carriers and time constraints for the entrances on this AEpu
1259		ResetAllCountersEvent All counters for the CountZoneManager are manually reset
1260		NetMonitorAlarmEvent

Event type number	Version	Event description
		Network EndPoint as specified at NetworkMonitor AEbc cannot be reached
1261		NetMonitorAlarmEvent Network EndPoint as specified at NetworkMonitor AEbc is reachable again
1262		EduRegistrationBookingEvent Education registration booking event
1263		LoginEvent AEpu-login, status ok
1264		LoginEvent AEpu-login, status failed
1265		LoginFailedEvent AEpu-login failed
1266		IncorrectVerifierEvent Incorrect verifier E: {name} direction:{1}
1267		InsufficientAccessLevelEvent Insufficient accesslevel event
1269	2.1	ResetCountZoneEvent This event occurs when counting is enabled. A count zone can automatically be reset by a timed process.
1270	2.2	AEPackAltModeEvent, Alt-mode is set to ON This event is generated when an AEpack is put into the ALT-mode. You can do this by pressing the ALT-button for a fewsome seconds.
1271	2.2	AEPackAltModeEvent, Alt-mode is set to OFF
1272	2.2	ZoneChangedEvent, Fault, active IntrusionDetection: Fault output is active
1273	2.2	ZoneChangedEvent, Fault, passive IntrusionDetection: Fault output is passive
1274	2.2	ZoneChangedEvent, Not used, active IntrusionDetection: Not used output is active
1275	2.2	ZoneChangedEvent, Not used, passive IntrusionDetection: Not used output is passive
1276	2.2	ZoneChangedEvent, Panic alarm, active IntrusionDetection: Panic alarm output is active
1277	2.2	Panic alarm, passive IntrusionDetection: Panic alarm output is passive
1278	2.2	ZoneChangedEvent, BURGLARY_ZONE, Area is active, Input is active
1279	2.2	ZoneChangedEvent, BURGLARY_ZONE, Area is active, Input is passive
1280	2.2	ZoneChangedEvent, WALK_IN_OUT_ZONE, Area is active, Input is active
1281	2.2	ZoneChangedEvent, WALK_IN_OUT_ZONE, Area is active, Input is passive
1282	2.2	ZoneChangedEvent, FIRE_ZONE, Area is active, Input is active
1283	2.2	ZoneChangedEvent, FIRE_ZONE, Area is active, Input is passive
1284	2.2	ZoneChangedEvent, TECHNICAL_ZONE, Area is active, Input is active

Event type number	Version	Event description
1285	2.2	ZoneChangedEvent, TECHNICAL_ZONE, Area is active, Input is passive
1286	2.2	ZoneChangedEvent, SYSTEM_SWITCH_ZONE, Area is active, Input is active
1287	2.2	ZoneChangedEvent, SYSTEM_SWITCH_ZONE, Area is active, Input is passive
1288	2.2	ZoneChangedEvent, RESET_ALARM_ZONE, Area is active, Input is active
1289	2.2	ZoneChangedEvent, RESET_ALARM_ZONE, Area is active, Input is passive
1290	2.2	ZoneChangedEvent, SABOTAGE_ZONE, Area is active, Input is active
1291	2.2	ZoneChangedEvent, SABOTAGE_ZONE, Area is active, Input is passive
1292	2.2	ZoneChangedEvent, FAULT_ZONE, Area is active, Input is active
1293	2.2	ZoneChangedEvent, FAULT_ZONE, Area is active, Input is passive
1294	2.2	ZoneChangedEvent, NOT_USED_ZONE, Area is active, Input is active
1295	2.2	ZoneChangedEvent, NOT_USED_ZONE, Area is active, Input is passive
1296	2.2	ZoneChangedEvent, PANIC_ZONE, Area is active, Input is active
1297	2.2	ZoneChangedEvent, PANIC_ZONE, Area is active, Input is passive
1298	2.2	ZoneInhibitedEvent, BURGLARY_ZONE, Area is active, Input is active
1299	2.2	ZoneInhibitedEvent, BURGLARY_ZONE, Area is active, Input is passive

Events 1300-1399

Event type number	Version	Event description
1300	2.2	ZoneInhibitedEvent, WALK_IN_OUT_ZONE, Area is active, Input is active
1301	2.2	ZoneInhibitedEvent, WALK_IN_OUT_ZONE, Area is active, Input is passive
1302	2.2	ZoneInhibitedEvent, FIRE_ZONE, Area is active, Input is active
1303	2.2	ZoneInhibitedEvent, FIRE_ZONE, Area is active, Input is passive
1304	2.2	ZoneInhibitedEvent, TECHNICAL_ZONE, Area is active, Input is active
1305	2.2	ZoneInhibitedEvent, TECHNICAL_ZONE, Area is active, Input is passive
1306	2.2	ZoneInhibitedEvent, SYSTEM_SWITCH_ZONE, Area is active, Input is active
1307	2.2	ZoneInhibitedEvent, SYSTEM_SWITCH_ZONE, Area is active, Input is passive
1308	2.2	ZoneInhibitedEvent, RESET_ALARM_ZONE, Area is active, Input is active
1309	2.2	ZoneInhibitedEvent, RESET_ALARM_ZONE, Area is active, Input is passive
1310	2.2	ZoneInhibitedEvent, SABOTAGE_ZONE, Area is active, Input is active
1311	2.2	ZoneInhibitedEvent, SABOTAGE_ZONE, Area is active, Input is passive
1312	2.2	ZoneInhibitedEvent, FAULT_ZONE, Area is active, Input is active
1313	2.2	ZoneInhibitedEvent, FAULT_ZONE, Area is active, Input is passive
1314	2.2	ZoneInhibitedEvent, NOT_USED_ZONE, Area is active, Input is active
1315	2.2	ZoneInhibitedEvent, NOT_USED_ZONE, Area is active, Input is passive
1316	2.2	ZoneInhibitedEvent, PANIC_ZONE, Area is active, Input is active

Event type number	Version	Event description
1317	2.2	ZoneInhibitedEvent, PANIC_ZONE, Area is active, Input is passive
1318	2.2	ArmStateEvent, Area is armed
1319	2.2	ArmStateEvent, Area is not armed
1320	2.2	PresenceTimeExceededEvent Maximum Presence time exceeded Note that the event is generated by the application server
1321	2.2	MaxMovementsExceededEvent Maximum movements exceeded Note that the event is generated by the application server
1322	2.2	VisitReleaseTimeExceededEvent Visit Release time exceeded This event is only generated in case the option ‘Extended visitor management’ is active. After release of a visitor the badge has to be withdrawn within a certain time. When this time is exceeded, the event will be generated.
1323	2.2	BadgeNoAccessEvent, Airlock occupied Unauthorized badge caused by Airlock occupied
1324	2.2	BadgeNoAccessEvent, Airock timeout alarm Unauthorized badge caused by Airlock timeout alarm
1325	2.2	LockOccupationTimeoutAlarmEvent, Start of alarm Airlock occupation time-out alarm occurs
1326	2.2	LockOcupationTimeoutAlarmEvent, End of alarm Airlock occupation time-out alarm ended
1327	2.2	Input contact inhibit state changed, false Input inhibit state is been changed to non-inhibit
1328	2.2	Input contact inhibit state changed, true Input inhibit state is been changed to inhibit
1329	2.2	BadgeNoAccessEvent, Security-level block Unauthorized badge caused by Security-level block
1330	2.2	ZoneAlarmStateChangedEvent, BURGLARY_ZONE, State is active
1331	2.2	ZoneAlarmStateChangedEvent, BURGLARY_ZONE, State is passive
1332	2.2	ZoneAlarmStateChangedEvent, BURGLARY_ZONE, State is unknown
1333	2.2	ZoneAlarmStateChangedEvent, WALK_IN_OUT_ZONE, State is active
1334	2.2	ZoneAlarmStateChangedEvent, WALK_IN_OUT_ZONE, State is passive
1335	2.2	ZoneAlarmStateChangedEvent, WALK_IN_OUT_ZONE, State is unknown
1336	2.2	ZoneAlarmStateChangedEvent, FIRE_ZONE, State is active
1337	2.2	ZoneAlarmStateChangedEvent, FIRE_ZONE, State is passive
1338	2.2	ZoneAlarmStateChangedEvent, FIRE_ZONE, State is unknown
1339	2.2	ZoneAlarmStateChangedEvent, TECHNICAL_ZONE, State is active
1340	2.2	ZoneAlarmStateChangedEvent, TECHNICAL_ZONE, State is passive
1341	2.2	ZoneAlarmStateChangedEvent, TECHNICAL_ZONE, State is unknown

Event type number	Version	Event description
1342	2.2	ZoneAlarmStateChangedEvent, SYSTEM_SWITCH_ZONE, State is active
1343	2.2	ZoneAlarmStateChangedEvent, SYSTEM_SWITCH_ZONE, State is passive
1344	2.2	ZoneAlarmStateChangedEvent, SYSTEM_SWITCH_ZONE, State is unknown
1345	2.2	ZoneAlarmStateChangedEvent, RESET_ALARM_ZONE, State is active
1346	2.2	ZoneAlarmStateChangedEvent, RESET_ALARM_ZONE, State is passive
1347	2.2	ZoneAlarmStateChangedEvent, RESET_ALARM_ZONE, State is unknown
1348	2.2	ZoneAlarmStateChangedEvent, SABOTAGE_ZONE, State is active
1349	2.2	ZoneAlarmStateChangedEvent, SABOTAGE_ZONE, State is passive
1350	2.2	ZoneAlarmStateChangedEvent, SABOTAGE_ZONE, State is unknown
1351	2.2	ZoneAlarmStateChangedEvent, FAULT_ZONE, State is active
1352	2.2	ZoneAlarmStateChangedEvent, FAULT_ZONE, State is passive
1353	2.2	ZoneAlarmStateChangedEvent, FAULT_ZONE, State is unknown
1354	2.2	ZoneAlarmStateChangedEvent, NOT_USED_ZONE, State is active
1355	2.2	ZoneAlarmStateChangedEvent, NOT_USED_ZONE, State is passive
1356	2.2	ZoneAlarmStateChangedEvent, NOT_USED_ZONE, State is unknown
1357	2.2	ZoneAlarmStateChangedEvent, PANIC_ZONE, State is active
1358	2.2	ZoneAlarmStateChangedEvent, PANIC_ZONE, State is passive
1359	2.2	ZoneAlarmStateChangedEvent, PANIC_ZONE, State is unknown
1360	2.2	ZoneIsolateEvent, PANIC_ZONE, is isolated
1361	2.2	ZoneIsolateEvent, PANIC_ZONE, is not isolated
1362	2.2	DoorOpenedEvent, activated Door contact input deactivated at Access Point
1363	2.2	DoorOpenedEvent, deactivated Door contact input deactivated at Access Point
1364	2.2	UnlockedEvent, activated Unlock relay is activated from Access Point
1365	2.2	UnlockedEvent, deactivated Unlock relay is deactivated from Access Point
1366	2.2	ZoneIsolatedEvent, BURGLARY_ZONE, is isolated
1367	2.2	ZoneIsolatedEvent, BURGLARY_ZONE, is not isolated
1368	2.2	ZoneIsolatedEvent, WALK_IN_OUT_ZONE, is isolated
1369	2.2	ZoneIsolatedEvent, WALK_IN_OUT_ZONE, is not isolated
1370	2.2	ZoneIsolatedEvent, FIRE_ZONE, is isolated
1371	2.2	ZoneIsolatedEvent, FIRE_ZONE, is not isolated
1372	2.2	ZoneIsolatedEvent, TECHNICAL_ZONE, is isolated
1373	2.2	ZoneIsolatedEvent, TECHNICAL_ZONE, is not isolated
1374	2.2	ZoneIsolatedEvent, SYSTEM_SWITCH_ZONE, is isolated

Event type number	Version	Event description
1375	2.2	ZoneIsolatedEvent, SYSTEM_SWITCH_ZONE, is not isolated
1376	2.2	ZoneIsolatedEvent, RESET_ALARM_ZONE, is isolated
1377	2.2	ZoneIsolatedEvent, RESET_ALARM_ZONE, is not isolated
1378	2.2	ZoneIsolatedEvent, SABOTAGE_ZONE, is isolated
1379	2.2	ZoneIsolatedEvent, SABOTAGE_ZONE, is not isolated
1380	2.2	ZoneIsolatedEvent, FAULT_ZONE, is isolated
1381	2.2	ZoneIsolatedEvent, FAULT_ZONE, is not isolated
1382	2.2	ZoneIsolatedEvent, NOT_USED_ZONE, is isolated
1383	2.2	ZoneIsolatedEvent, NOT_USED_ZONE, is not isolated
1384	2.2	SpeedMeasuredEvent Time (s) and speed (km/h) measured, triggered by Id or other source This event is generated by a SpeedMeasuring component.
1385	2.3	BadgeRejectedByDeviceEvent Badge rejected by a non-AEpack device with given reason
1386	2.3	GuardTourMissedDemarcationPointEvent Indicates that the guard has arrived at a demarcation point which differs from the expected demarcation point.
1387	2.3	GuardTourResumedEvent Indicates that a suspended guard tour is resumed
1388	2.3	GuardTourStartedEvent Indicates that a suspended guard tour is started
1389	2.3	GuardTourStoppedEvent Indicates that a guard tour is stopped.
1390	2.3	GuardTourSuspendedEvent Indicates that a guard tour is suspended.
1391	2.3	GuardTourTooFastEvent Indicates that a guard has arrived too early at a demarcation point.
1392	2.3	GuardTourTooSlowEvent Indicates that a guard has arrived too late at a demarcation point.
1393	2.3	GuardTourCompletedEvent Indicates that a guard tour is completed.
1394	2.3	TotalGuardTourTooFastEvent Indicates that a guard has performed the entire guard tour too fast.
1395	2.3	TotalGuardTourTooSlowEvent Indicates that a guard has taken too long to perform the entire guard tour.
1396	2.1.7	AEPackMessageEvent Message from an AEpack
1397	2.2.2	BadgeNoAccessEvent, identifier is blocked. Unauthorized badge, identifier is blocked.

Events 1400-1499

Event type number	Version	Event description
1400	2.3.1	UserActionEvent, User login
1401	2.3.1	UserActionEvent, User logout
1402	2.3.1	UserActionEvent, Remote command execution
1403	2.3.1	FallBackModeEvent, Fallback mode activated
1404	2.3.1	FallBackModeEvent, Fallback mode deactivated
1405	2.3.1	ActionOnCarrierAlarm Alarm is generated when a Create, Update, Delete action on a carrier is performed + a generate alarm action on carrier is defined
1406	2.1.8	RmiLoginEvent, Rmi-login
1407	2.1.8	RmiLoginEvent, Rmi-logout
1408	2.1.8	RmiLoginEvent, Rmi-logout (by timeout)
1409	2.3.1	BadgeNoAccessEvent, Fake verifier Unauthorized badge, Fake verifier
1410	2.3.1	BadgeNoAccessEvent, Generic error from external device Unauthorized badge, Generic error from external device
1411	2.3.1	ActionOnTokenAssignmentAlarm Alarm is generated when a Create, Update, Delete action on a token assignment is performed + a generate alarm action on a token assignment is defined
1412	2.3.1	ActionOnVerificationExclusionAlarm Alarm is generated when a Create, Update, Delete action on a verification exclusion is performed + a generate alarm action on a verification exclusion is defined
1413	2.3.1	ActionOnApbExclusionAlarm Alarm is generated when a Create, Update, Delete action on an APB exclusion is performed + a generate alarm action on an APB exclusion is defined.
1414	2.3.1	CarrierDateFieldExpirationAlarm Alarm is generated when some date field when some date field related to a carrier is about to or has been expired. Date fields are defined through the field meta data so they can be static fields or free fields.
1415	2.3.1	MaxThresholdExceededEvent Event is generated when one of the thresholds is exceeded. This can occur in the Sagem Matcher for instance
1416	2.3.1	ActionOnProfileAlarm Alarm is generated when a Create, Update, Delete action on a profile is performed + a generate alarm action on a profile is defined.
1417	2.3.1	SilentAlarm Alarm is generated when event is discovered which complies to any response to event configuration.
1418	2.2	ACConfigurationChangedEvent Event indicates that a change in security scenario has occurred
1419	2.3.1	ActionOnTemplateAlarm Alarm is generated when a Create, Update, Delete action on an authorization template is performed + a generate alarm action on an authorization template is defined.

Event type number	Version	Event description
1420	2.3.1	ActionOnEntranceGroupAlarm Alarm is generated when a Create, Update, Delete action on an (offline) entrance group is performed + a generate alarm action on an (offline) entrance group is defined.
1421	2.3.2	FallBackModeACDataLoadEvent, started Download of fallback data started to AP6003
1422	2.3.2	FallBackModeACDataLoadEvent, completed Download of fallback data completed to AP6003
1423	2.3.2	FallBackModeACDataLoadEvent, canceled Download of fallback data canceled to AP6003
1424		IncompatibleAEpuVersionEvent Indicates that an AEpu is discovered that has a version number that differs from the server.
1425	2.4	LicenceExpiresEvent Event is generated when the AEOS license is about to expire
1426	2.3.8	IMSConnectionEvent, connection lost IMS (InterMediate Server) Connection seems to be lost
1427	2.3.8	IMSConnectionEvent, connection re-established IMS (InterMediate Server) Connection is re-established again
1428	2.4	LockerDoorStateEvent, Locker is open and unlocked Related to LoXS Terminal – AEOS connection
1429	2.4	LockerDoorStateEvent, Locker is open and locked Related to LoXS Terminal – AEOS connection
1430	2.4	LockerDoorStateEvent, Locker is closed and unlocked Related to LoXS Terminal – AEOS connection
1431	2.4	LockerDoorStateEvent, Locker is closed and locked Related to LoXS Terminal – AEOS connection
1432	2.4	LockerOccupiedEvent, Locker is occupied Related to LoXS Terminal – AEOS connection
1433	2.4	LockerOccupiedEvent, Locker is not occupied Related to LoXS Terminal – AEOS connection
1434	2.4	LockerPresenceEvent, Locker is present Related to LoXS Terminal – AEOS connection
1435	2.4	LockerPresenceEvent, Locker is not present Related to LoXS Terminal – AEOS connection
1436	2.4	LockerTerminalPresenceEvent, Terminal is present Related to LoXS Terminal – AEOS connection
1437	2.4	LockerTerminalPresenceEvent, Terminal is not present Related to LoXS Terminal – AEOS connection
1438	2.4	LockerSabotageAlarmEvent, Alarm state start Related to LoXS Terminal – AEOS connection
1439	2.4	LockerSabotageAlarmEvent, Alarm state end Related to LoXS Terminal – AEOS connection
1440	2.4	LockerOpenTooLongAlarmEvent, Alarm state start

Event type number	Version	Event description
		Related to LoXS Terminal – AEOS connection
1441	2.4	LockerOpenTooLongAlarmEvent, Alarm state end Related to LoXS Terminal – AEOS connection
1442	2.4	AreaArmStateEvent, is armed
1443	2.4	AreaArmStateEvent, is not armed
1444	2.4	AlarmStateEvent, alarm activated
1445	2.4	AlarmStateEvent, alarm deactivated
1446	2.4	BypassStateEvent, is bypassed
1447	2.4	BypassStateEvent, is not bypassed
1448	2.4	TamperStateEvent, tamper activated
1449	2.4	TamperStateEvent, tamper deactivated
1450	2.4	LockerBadgeEvent, Badge authorized Related to LoXS Terminal – AEOS connection
1451	2.4	LockerBadgeEvent, Badge unauthorized Related to LoXS Terminal – AEOS connection
1452	2.4	BadgeNoAccessEvent, external authorization check not possible Related to ExternalAuthorization AEbc
1453	2.4	BadgeNoAccessEvent, external system denies authorization Related to ExternalAuthorization AEbc
1454	2.4	BadgeNoAccessEvent, cabinet keys in possession Related to Key Cabinet systems
1455	2.4	BadgeNoAccessEvent, communication problem with external system Related to Key Cabinet systems
1456	2.4.1	KeyAccessEvent, Key is taken Related to Key Cabinet systems
1457	2.4.1	KeyAccessEvent, Key is returned Related to Key Cabinet systems
1458	2.4.1	ExternalCounterEvent, Counter values
1459	2.4.2	BadgeNoAccessEvent, Unauthorized badge because APB Blocking time is active
1460	2.4.2	BadgeNoAccessEvent, Badge is blocked on LoXS-locker Related to LoXS Terminal – AEOS connection
1461	2.4.2	BadgeNoAccessEvent , Dynamic LoXS-locker assignment is not allowed Related to LoXS Terminal – AEOS connection
1462	2.4.3	KNXDatapointGetValueCommandEvent KNX datapoint get value command
1463	2.4.3	BadgeQueueActionEvent Badge queue Action
1464	2.4.3	KNXDatapointSetValueCommandEvent KNX datapoint set value command

Event type number	Version	Event description
1465	2.3.17.2	LookupServerDiscoverEvent Lookup server is in unknown state
1466	2.3.17.2	LookupServerDiscoverEvent Lookup server is discovered
1467	2.3.17.2	LookupServerDiscoverEvent Lookup server is discarded
1468	2.4.5	OfflineBadgeAccessEvent Authorized badge on an offline door
1469	2.4.5	OfflineBadgeNoAccessEvent Unauthorized badge on an offline door
1470	2.4.5	OfflineBatteryLowLevelEvent Low Battery level on an offline door
1471	3.0.1	RFLockDoorLeftOpenAlarmEvent Alarm is started at RF lockId
1472	3.0.1	RFLockDoorLeftOpenAlarmEvent Alarm is ended at RF lockId
1473	3.0.1	RFLockIntrusionAlarmEvent Alarm is started at RF lockId
1474	3.0.1	RFLockIntrusionAlarmEvent Alarm is ended at RF lockId
1475	2.4.7	BadgeNoAccessEvent Unsupported verification type
1480	3.0.2	ArmDisarmLogbookEntry Area armed
1481	3.0.2	ArmDisarmLogbookEntry Area forced armed
1482	3.0.2	ArmDisarmLogbookEntry Area disarmed
1483	3.0.2	StartStopTestLogbookEntry Test started
1484	3.0.2	StartStopTestLogbookEntry Test stopped
1485	3.0.2	InhibitLogbookEntry Detector inhibited
1486	3.0.2	InhibitLogbookEntry Detector uninhibited
1487	3.0.2	IsolateLogbookEntry Detector isolated
1488	3.0.2	IsolateLogbookEntry Detector unisolated
1489	3.0.2	AlarmRestoreLogbookEntry Burglary alarm restored by user

Event type number	Version	Event description
1490	3.0.2	AlarmRestoreLogbookEntry Panic alarm restored by user
1491	3.0.2	AlarmRestoreLogbookEntry Hold-up alarm restored by user
1492	3.0.2	AlarmRestoreLogbookEntry 24-hour alarm restored by user
1493	3.0.2	AlarmRestoreLogbookEntry Technical alarm restored by user
1494	3.0.2	AlarmRestoreLogbookEntry Tamper alarm restored by user
1495	3.0.2	AlarmRestoreLogbookEntry Fault alarm restored by user
1496	3.0.2	AlarmRestoreLogbookEntry Masked alarm restored by user
1497	3.0.2	AlarmLogbookEntry Burglary alarm started
1498	3.0.2	AlarmLogbookEntry Burglary alarm restored
1499	3.0.2	AlarmLogbookEntry Panic alarm started

Events 1500-1599

Event type number	Version	Event description
1500	3.0.2	AlarmLogbookEntry Panic alarm restored
1501	3.0.2	AlarmLogbookEntry Hold-up alarm started
1502	3.0.2	AlarmLogbookEntry Hold-up alarm restored
1503	3.0.2	AlarmLogbookEntry 24-hour alarm started
1504	3.0.2	AlarmLogbookEntry 24-hour alarm restored
1505	3.0.2	AlarmLogbookEntry Technical alarm started
1506	3.0.2	AlarmLogbookEntry Technical alarm restored
1507	3.0.2	AlarmLogbookEntry Tamper alarm started, reason: Sabotaged, shortcut
1508	3.0.2	AlarmLogbookEntry

Event type number	Version	Event description
		Tamper alarm started, reason: Sabotaged, open
1509	3.0.2	AlarmLogbookEntry Tamper alarm started, reason: Sabotaged, connection lost
1510	3.0.2	AlarmLogbookEntry Tamper alarm started, reason: Masked
1511	3.0.2	AlarmLogbookEntry Tamper alarm started, reason: Alarm equipment tampered
1512	3.0.2	AlarmLogbookEntry Tamper alarm restored, reason: Sabotaged, shortcut
1513	3.0.2	AlarmLogbookEntry Tamper alarm restored, reason: Sabotaged, open
1514	3.0.2	AlarmLogbookEntry Tamper alarm restored, reason: Sabotaged, connection lost
1515	3.0.2	AlarmLogbookEntry Tamper alarm restored, reason: Masked
1516	3.0.2	AlarmLogbookEntry Tamper alarm restored, reason: Alarm equipment tampered
1517	3.0.2	AlarmLogbookEntry Fault alarm started, reason: Dialer not polled
1518	3.0.2	AlarmLogbookEntry Fault alarm started, reason: Dialer has no Ethernet connection
1519	3.0.2	AlarmLogbookEntry Fault alarm started, reason: Dialer has no GSM registration
1520	3.0.2	AlarmLogbookEntry Fault alarm started, reason: No communication with dialer
1521	3.0.2	AlarmLogbookEntry Fault alarm started, reason: Dialer could not send event to ATS
1522	3.0.2	AlarmLogbookEntry Fault alarm started, reason: AC power trouble
1523	3.0.2	AlarmLogbookEntry Fault alarm started, reason: Power supply trouble
1524	3.0.2	AlarmLogbookEntry Fault alarm started, reason: Sensor power trouble
1525	3.0.2	AlarmLogbookEntry Fault alarm started, reason: Battery low voltage
1526	3.0.2	AlarmLogbookEntry Fault alarm started, reason: Battery failure
1527	3.0.2	AlarmLogbookEntry Fault alarm started, reason: Battery missing
1528	3.0.2	AlarmLogbookEntry Fault alarm started, reason: Device connection lost
1529	3.0.2	AlarmLogbookEntry Fault alarm started, reason: Masked

Event type number	Version	Event description
1530	3.0.2	AlarmLogbookEntry Fault alarm started, reason: Processing failure
1531	3.0.2	AlarmLogbookEntry Fault alarm started, reason: Detection
1532	3.0.2	AlarmLogbookEntry Fault alarm restored, reason: Dialer not polled
1533	3.0.2	AlarmLogbookEntry Fault alarm restored, reason: Dialer has no Ethernet connection
1534	3.0.2	AlarmLogbookEntry Fault alarm restored, reason: Dialer has no GSM registration
1535	3.0.2	AlarmLogbookEntry Fault alarm restored, reason: No communication with dialer
1536	3.0.2	AlarmLogbookEntry Fault alarm restored, reason: Dialer could not send event to ATS
1537	3.0.2	AlarmLogbookEntry Fault alarm restored, reason: AC power trouble
1538	3.0.2	AlarmLogbookEntry Fault alarm restored, reason: Power supply trouble
1539	3.0.2	AlarmLogbookEntry Fault alarm restored, reason: Sensor power trouble
1540	3.0.2	AlarmLogbookEntry Fault alarm restored, reason: Battery low voltage
1541	3.0.2	AlarmLogbookEntry Fault alarm restored, reason: Battery failure
1542	3.0.2	AlarmLogbookEntry Fault alarm restored, reason: Battery missing
1543	3.0.2	AlarmLogbookEntry Fault alarm restored, reason: Device connection lost
1544	3.0.2	AlarmLogbookEntry Fault alarm restored, reason: Masked
1545	3.0.2	AlarmLogbookEntry Fault alarm restored, reason: Processing failure
1546	3.0.2	AlarmLogbookEntry Fault alarm restored, reason: Detection
1547	3.0.2	AlarmLogbookEntry Masked alarm started
1548	3.0.2	AlarmLogbookEntry Masked alarm restored
1549	3.0.2	AutoInhibitLogbookEntry Detector automatically inhibited
1550	3.0.2	UILoginDisabledLogbookEntry Login disabled because of too many invalid attempts
1551	3.0.2	OverrideLogbookEntry

Event type number	Version	Event description
		Burglary alarm overridden
1552	3.0.2	OverrideLogbookEntry Panic alarm overridden
1553	3.0.2	OverrideLogbookEntry Hold-up alarm overridden
1554	3.0.2	OverrideLogbookEntry 24-hour alarm overridden
1555	3.0.2	OverrideLogbookEntry Technical alarm overridden
1556	3.0.2	OverrideLogbookEntry Tamper alarm overridden
1557	3.0.2	OverrideLogbookEntry Fault alarm overridden
1558	3.0.2	OverrideLogbookEntry Masked alarm overridden
1559	3.0.2	OverrideLogbookEntry Detector overridden
1560	3.0.3	GalaxyGroupAlarmStateEvent Group in alarm
1561	3.0.3	GalaxyGroupAlarmStateEvent Group idle
1562	3.0.3	GalaxyGroupAlarmStateEvent Group needs reset
1563	3.0.3	GalaxyGroupStateEvent Group armed
1564	3.0.3	GalaxyGroupStateEvent Group partially armed
1565	3.0.3	GalaxyGroupStateEvent Group disarmed
1566	3.0.3	GalaxyZoneAlarmStateEvent Zone alarm
1567	3.0.3	GalaxyZoneAlarmStateEvent Zone idle
1568	3.0.3	GalaxyZoneAlarmEvent Zone closed
1569	3.0.3	GalaxyZoneAlarmEvent Zone open
1570	3.0.3	FireSystemPanelEvent Event string includes panel number and state information
1571	3.0.3	FireSystemSensorEvent Event string includes sensor number and state information
1572	3.0.3	FireSystemZoneEvent Event string includes zone number and state information

Event type number	Version	Event description
1573	3.0.3	FireSystemModuleEvent Event string includes module number and state information
1574	3.1	SoaaCardUpdateSuccessfullEvent OSS-SO card successfully updated
1575	3.1	SoaaCardUpdateFailedEvent OSS-SO card update failed, card was removed.
1576	3.1	SoaaCardUpdateFailedEvent OSS-SO card update failed, no OSS-SO authorizations present.
1577	3.1	SoaaCardUpdateFailedEvent OSS-SO card update failed, unassigned card.
1578	3.1	SoaaLockBatteryLowEvent Low Battery on an OSS-SO door.
1579	3.1	SoaaLockJammedEvent OSS-SO door jammed
1580	3.1	SoaaCardUpdateFailedEvent OSS-SO card update failed, unsupported version.
1581	3.1	SoaaCardUpdateFailedEvent OSS-SO card update failed, card read error.
1582	3.1	SoaaCardUpdateFailedEvent OSS-SO card update failed, card write error.
1583	3.1	SoaaLockBatteryReplacedEvent Battery in lock was replaced successfully.
1584	3.1	SoaaLockSystemEvent The lock electronics has restarted but is still operational. Restart could be due to battery replacement or some intentional software reset of the lock.
1585	3.1	SoaaLockSystemEvent Some configuration of the lock firmware has been performed, that is group, ID, keys have changed.
1586	3.1	SoaaLockInternalErrorEvent Lock has detected an internal error.
1587	3.1	SoaaLockFailedToUnlockEvent Lock has failed to unlock door at some point.
1588	3.1	SoaaLockTamperEvent Some security breach to lock detected.
1589	3.1	SoaaLockBlackListedCardDetectedEvent Lock has detected a blacklisted card.
1590	3.1	SoaaLockBlacklistFullEvent Not possible to add more entries to the lock.
1591	3.1	SoaaLockAccessGrantedEvent Access granted on an OSS-SO door; General granted code.
1592	3.1	SoaaLockAccessGrantedEvent Access granted on an OSS-SO door; Granted access with default access time.

Event type number	Version	Event description
1593	3.1	SoaaLockAccessGrantedEvent Access granted on an OSS-SO door; Granted access with extended access time.
1594	3.1	SoaaLockAccessGrantedEvent Access granted on an OSS-SO door; Granted access with toggle function unlocking.
1595	3.1	SoaaLockAccessGrantedEvent Access granted on an OSS-SO door; Granted access with toggle function locking.
1596	3.1	SoaaLockAccessDeniedEvent Access denied on an OSS-SO door; General denied code.
1597	3.1	SoaaLockAccessDeniedEvent Access denied on an OSS-SO door; Denied access due to blacklisted CardId.
1598	3.1	SoaaLockAccessDeniedEvent Access denied on an OSS-SO door; Denied access due to expired validity.
1599	3.1.1	RegistrationEvent In/Out Registration on a terminal (Education) .

Events 1600-1699

Event type number	Version	Event description
1600	3.1.1	AutoStopTestLogbookEntry Automatically stop the Test mode on an area (by timer).
1601	3.1.1	SetSequenceAbortedLogBookEntry Set sequence was aborted.
1602	3.1.1	InstallerModeStartStopLogbookEntry Installer mode is started/stopped
1603	3.1.1	PACandLogInputChangeLogbookEntry Input value changed of a detector with type "PAC and Log".
1604	3.1.1	BadgeNoAccessEvent Intrusion terminal, no authorization.
1605	3.1.1	BadgeNoAccessEvent Intrusion terminal, Area functions are not valid at this time.
1606	3.1.2	ContainerModificationEvent A change of the configuration of the AEpu using AEmon.
1607	3.1.2	PasswordChangedEvent Password change by person on the AEpu.
1608	3.1.2	SoaaCardUpdateFailedEvent OSS-SO card update failed, authorization data size error.
1609	3.1.2	SoaaCardUpdateFailedEvent OSS-SO card update failed, blacklist data size error.
1610	3.1.3	SoaaCardUpdateFailedEvent

Event type number	Version	Event description
		OSS-SO card update failed, identifier could not be created from the received badge data.
1611	3.1.3	SoaaCardUpdateFailedEvent OSS-SO card update failed, OSS-SO authorization data is invalid.
1612	3.1.3	SoaaCardUpdateFailedEvent OSS-SO card update failed, presented card is not an OSS-SO card.
1613	3.1.4	IntercomCallEvent A call is received from an intercom device.
1614	3.1.4	IntercomAcceptCallEvent An intercom call is accepted.
1615	3.1.4	IntercomCloseCallEvent An intercom call is closed.
1616	3.1.4	LockerFreedEvent Locker is free (not occupied anymore).
1617	3.1.4	LockerExipredEvent Locker occupation is expired, locker is released.
1618	3.1.4	LockerExipredEvent Locker occupation is expired, locker is blocked.
1619	3.1.4	SignallerOutputStateEvent Toggle output has been set to True.
1620	3.1.4	SignallerOutputStateEvent Toggle output has been set to False.
1621	3.1.5	BadgeNoAccessEvent, Verifier inhibit Unauthorized badge, Verifier inhibit.
1622	3.1.5	ActionOnVerificationAlarm Alarm is generated when a CRUD action on a verification is performed + a generate alarm action on verification is defined.
1623	3.1.5	SoaaCardInitializeSuccessfulEvent OSS-SO card successfully initialized.
1624	3.1.5	SoaaCardInitializationFailedEvent OSS-SO card initialization failed, card was removed.
1625	3.1.5	SoaaCardInitializationFailedEvent OSS-SO card initialization failed, no OSS-SO authorizations present.
1626	3.1.5	SoaaCardInitializationFailedEvent OSS-SO card initialization failed, unassigned card.
1627	3.1.5	SoaaCardInitializationFailedEvent OSS-SO card initialization failed, unsupported version.
1628	3.1.5	SoaaCardInitializationFailedEvent OSS-SO card initialization failed, card read error.
1629	3.1.5	SoaaCardInitializationFailedEvent OSS-SO card initialization failed, card write error.
1630	3.1.5	SoaaCardInitializationFailedEvent OSS-SO card initialization failed, authorization data size error.
1631	3.1.5	SoaaCardInitializationFailedEvent

Event type number	Version	Event description
		OSS-SO card initialization failed, blacklist data size error.
1632	3.1.5	SoaaCardInitializationFailedEvent OSS-SO card initialization failed, identifier could not be created from the received badge data.
1633	3.1.5	SoaaCardInitializationFailedEvent OSS-SO card initialization failed, OSS-SO authorization data is invalid.
1634	3.1.5	SoaaCardInitializationFailedEvent OSS-SO card initialization failed, presented card is not an OSS-SO card.
1635	3.1.5	SoaaCardInitializationFailedEvent OSS-SO card initialization failed, no badgeID received.
1636	3.2.1	ValidVerifierEvent Valid verifier E: {name} direction:{1}
1637	3.2.1	BadgeNoAccessEvent E2E, No key found.
1638	3.2.1	BadgeNoAccessEvent E2E, Authentication failed.
1639	3.2.1	SoaaLockCRCErrorEvent CRC Error in Info file.
1640	3.2.1	SoaaLockCRCErrorEvent CRC Error in Data file.
1641	3.2.1	SoaaLockCRCErrorEvent CRC Error in Event file.
1642	3.2.1	SoaaLockCRCErrorEvent CRC Error in Blacklist file.
1643	3.2.1	ValidVerifierEvent Valid verifier.
1644	3.2.1	VerificationSuspendTimeStartedEvent The Suspend start time is set by the server.
1645	3.2.1	GalaxyGroupStateEvent Group ready to set.
1646	3.2.1	GalaxyGroupStateEvent Group time locked.
1647	3.2.1	BadgeNoAccessEvent, PIN in reset state Unauthorized badge; Verification/PIN in reset state (the person's PIN must be updated).
1648	3.2.1	BadgeNoAccessEvent, verification is suspended Unauthorized badge; Verification/PIN is suspended.
1649	3.2.1	SamDiscoveryEvent SAM discovery.
1650	3.2.1	SamAuthenticationFailureEvent SAM authentication fails.
1651	3.2.1	SamRemovalEvent SAM removal.

Event type number	Version	Event description
1652	3.2.1	SamUpdateEvent SAM update.
1653	3.2.1	SamUpdateFailureEvent SAM update failure.
1654	3.2.1	RFLockBatteryStateEvent Battery state of RF lock-Id.
1655	3.2.1	RFLockDeviceConnectionStateEvent RF lock-Id is online.
1656	3.2.1	RFLockDeviceConnectionStateEvent RF lock-Id is offline.
1657	3.2.1	RFLockDeviceNoResponseEvent Device RF lock-Id doesn't respond on command .
1658	3.2.2	KeyAbsentTooLongEvent Key is absent too long.
1659	3.2.2	AreaNotArmedOnKeyReturnEvent Related area is not armed when key is returned.
1660	3.2.2	SelfTestStartedLogbookEntry Intrusion area self-test started.
1661	3.2.2	SelfTestStoppedLogbookEntry Intrusion area self-test has been completed.
1662	3.2.2	SelfTestStoppedLogbookEntry Intrusion area self-test has been canceled.
1663	3.2.2	SelfTestSuccessfulLogbookEntry Intrusion detector self-test successful.
1664	3.2.2	SelfTestFailedLogbookEntry Intrusion detector self-test failed.
1665	3.3	DuressAlarmEvent A carrier is forced to present their identifier.
1666	3.3	BadgeNoAccessEvent The carrier is not authorized for the requested function.
1667	3.3	BadgeNoAccessEvent Supplied AccessControlAction is unknown to the authorizer.
1668	3.3	BadgeNoAccessEvent Authorization from external source is not possible because the user id is unknown in the external system.
1669	3.3.1	BadgeNoAccessEvent Guidance, Invalid direction.
1670	3.3.1	BadgeNoAccessEvent Guidance, Unknown entrance.
1671	3.3.1	BadgeNoAccessEvent Guidance, authorization request is already running.
1672	3.3.1	BadgeNoAccessEvent Guidance, Illegal presence.

Event type number	Version	Event description
1673	3.3.1	BadgeNoAccessEvent Guidance, Unavailable zone manager.
1674	3.3.1	BadgeNoAccessEvent Guidance, Incorrect configured AEpu.
1675	3.3.1	BadgeNoAccessEvent Guidance, Guidance blocking time active.
1676	3.3.1	BadgeNoAccessEvent Guidance, Insufficient number of guides.
1677	3.3.1	BadgeNoAccessEvent Guidance, Entrance delay exceeded.
1678	3.3.2	CountAuthorizerEvent Carrier booking event.
1679	3.4	BadgeNoAccessEvent Certificate needed for decoding the badge could not be found.
1680	3.4	BadgeNoAccessEvent Certificate needed for decoding the badge is not yet valid.
1681	3.4	BadgeNoAccessEvent Certificate needed for decoding the badge has been expired.
1682	3.4	BadgeNoAccessEvent Badge is on the revoke list.
1683	3.4	BadgeNoAccessEvent Badge CRC failure.
1684	3.4	BadgeNoAccessEvent Badge validity has expired.
1685	3.4	BadgeNoAccessEvent Badge CSN (Card Serial Number) failure.
1686	3.4	BadgeNoAccessEvent Missing badge data.
1687	3.4	BadgeNoAccessEvent Badge has possibly been compromised.
1688	3.4	IdentifyUnsuccessfulEvent Carrier could not be identified.
1689	3.4	OSSCardInterventionMediaEvent Event indicating intervention media card was presented.
1690	3.4	BadgeAccessElevatorEvent Authorized badge on an elevator.
1691	3.4	ElevatorStatusEvent Device is connected.
1692	3.4	ElevatorStatusEvent Device is not connected.
1693	3.4	BadgeNoAccessElevatorEvent No location authorizations.
1694	3.4	BadgeNoAccessElevatorEvent

Event type number	Version	Event description
		No access authorizations.
1696	3.4	BadgeNoBookingElevatorEvent No booking, selection timeout.
1697	3.4	CameraEvent Unable to record.