S

EN

Installation and Configuration

AEOS Milestone plug-in

Version 9 | 13-11-2018

security management

www.nedapsecurity.com

Date	Version	Changes
13-11-2018	9	Added remark on use of host names for TLS connections
13-06-2018	8	Minor improvements
07-05-2018	7	Added list of supported AEOS events
29-03-2018	6	Update on security certificates, SSL use and debug info, personalisation
19-06-2017	5	Update on security certificates
16-05-2017	4	Update on security certificates
22-03-2017	3	Additional requirement added. Event Server has to be stopped before plug-in installation. Lay-out.
24-01-2017	2	General update of the document. Extra information for AEOS Classic users. Information regarding system properties added.
04-11-2016	1	New document

Contents

1. Introduction

Integrating AEOS in Milestone enables you to enrich the visual evidence provided by Milestone with access control information from AEOS in a single client user interface. The standard display of identifier information, such as name, department or pictures as well as controls like door lock and unlock will help to optimize work processes, improve control over premises and increase the security level.

This manual presents step-by-step instructions for the setup of the AEOS Milestone plug-in with AEOS. This document is intended for system installers and system administrators.

2. Requirements

The following requirements have to be met:

- AEOS version 3.2.2 or a newer version is installed. Note that AEOS version 3.4 will support an encrypted SSL connection between AEOS and Milestone XProtect.
- Milestone XProtect Express, Professional, Enterprise, Expert, or Husky M20, M30, M50, M500A, or M550A Corporate (2014 and 2016) must be fully installed to be compatible with AEOS.
- Milestone only supports MS SQL databases. The database must be case insensitive.
- Microsoft .NET framework 4.6.1 or higher needs to be installed at the server on which the Milestone XProtect environment is running. Otherwise the plug-in cannot be used properly.

3. Preparation

- Milestone and AEOS use the same port number. Therefore, either install AEOS and Milestone XProtect on different servers, or update the AEOS database by running the setup of AEOS again, and changing the port number for the AEOS server during the setup.
- AEOS Classic users have to purchase a license for the SOAP WebService (8019223).
- Check with the customer which carrier types (for example, employees, visitors, contractors) are required to be visible in the Milestone XProtect environment. If also the carrier information of contractors has to be visible in the Milestone XProtect environment, AEOS Blue users have to activate system property 44.04 'Contractor management'. AEOS Classic users have to purchase license 9809090, if contractor details have to be visible in the Milestone XProtect environment.
- Note the port number that the customer is using for the Socket Interface. The default port number is 8035.
- Note the port number that the customer is using for the Soap WebService. The default port number is 8443.
- The Milestone system checks the local computer's root certificates. This means the AEOS security certificate must be available in the local computer's certificate store (see the instructions section, steps 10 and 11)
- The AEOS Milestone plug-in is available at our partner portal: https://nedapsecurity.com.

4. Instructions

Step 01 Activate the SOAP WebService option

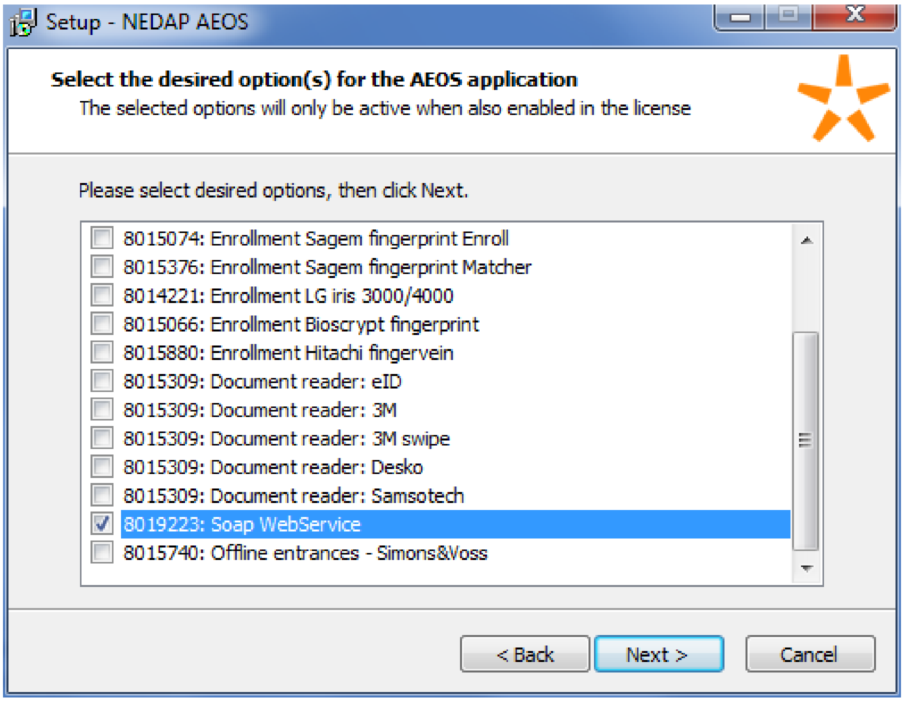
There is one key point to consider when installing AEOS: To use the AEOS Milestone plug-in, AEOS option **8019223: Soap WebService** needs to be enabled.

When AEOS has already been installed without this option, you need to run the AEOS setup again.

In the setup wizard:

1. Select **change current settings**.
2. Select **upgrade the existing database**.
3. Enable AEOS option **8019223: Soap WebService**.

Please refer to the *AEOS Software Installation Guide* for general instructions on the installation of AEOS.



Setup - NEDAP AEOS

Select the desired option(s) for the AEOS application

The selected options will only be active when also enabled in the license

Please select desired options, then click Next.

- □ 8015074: Enrollment Sagem fingerprint Enroll
- □ 8015376: Enrollment Sagem fingerprint Matcher
- □ 8014221: Enrollment LG iris 3000/4000
- □ 8015066: Enrollment Bioscrypt fingerprint
- □ 8015880: Enrollment Hitachi fingervein
- □ 8015309: Document reader: eID
- □ 8015309: Document reader: 3M
- □ 8015309: Document reader: 3M swipe
- □ 8015309: Document reader: Desko
- □ 8015309: Document reader: Samsotech
- ☑ 8019223: Soap WebService
- □ 8015740: Offline entrances - Simons&Voss

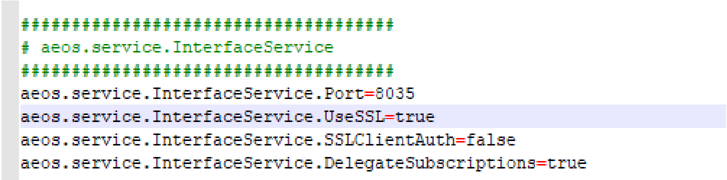
Step 02

For AEOS version 3.4 and newer versions: Enable SSL in the aeos.properties file

!

Enabling SSL in the aeos.properties file has impact on other applications using the AEOS InterfaceService. Those applications must also start using SSL certificates.

1. Stop the **AEOS Application Server**.
   a. In Windows, press the ⊞ **Win + R** key and enter **services.msc**. Click **OK**.
   b. In the **Services** window, right-click on **AEOS Application Server SSK** and select **Stop.**
2. Go to the **...\AEOS\AEserver\jboss\standalone\configuration** folder.
3. Open the **aeos.properties file** (for example with Notepad++).
4. Set **aeos.service.InterfaceService.UseSSL** to `true`.



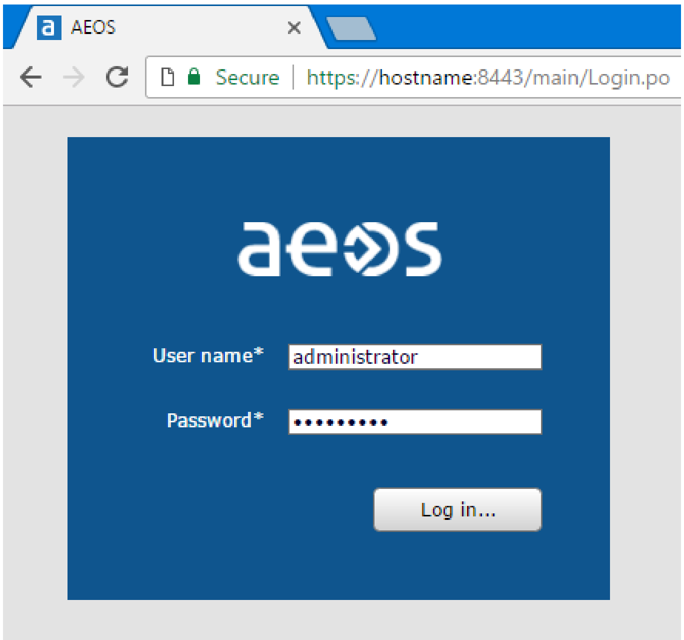
```
#####################################
# aeos.service.InterfaceService
#####################################
aeos.service.InterfaceService.Port=8035
aeos.service.InterfaceService.UseSSL=true
aeos.service.InterfaceService.SSLClientAuth=false
aeos.service.InterfaceService.DelegateSubscriptions=true
```

5. Save and close the the **aeos.properties** file.
6. Restart the **AEOS application server**.

Step 03 Log in as administrator to AEOS Maintenance and Configuration

Several configurations have to be made within the AEOS application. Therefore, it is necessary to log in as administrator to AEOS Maintenance and Configuration.

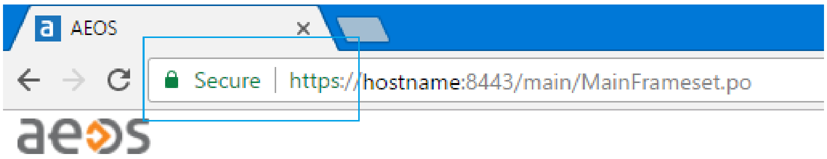
1. Click the internet browser address bar and enter `https://` followed by the hostname of the AEOS server and a colon. Add the AEOS server port number behind the colon `https://servername:port number`.
2. Enter the administrator's user name and password.
3. Click **Log in** to continue.



User name* administrator

Password* •••••••••

4. Make sure there's a secure connection with the AEOS server.
   For instructions, see the *AEOS SSL installation manual*.



Step 04 Activate system property 44.15: SOAP WebService

! This step only applies to AEOS Blue systems. With AEOS Classic, you need an additional AEOS licence option for SOAP WebService.

After activating the SOAP WebService during the AEOS setup, the SOAP WebService also has to be activated in the system properties (with AEOS Blue systems). Only if the system property is activated, AEOS and Milestone will eventually communicate with each other and exchange identifier information.

1. Go to **Administration** > **Maintenance** > **Settings** > **System properties**.
2. Enable system property **44.15: SOAP WebService.**
3. Click **OK** to save the settings.
4. Log off and log in again to activate the changes.

Step 05 Create a new AEOS user role

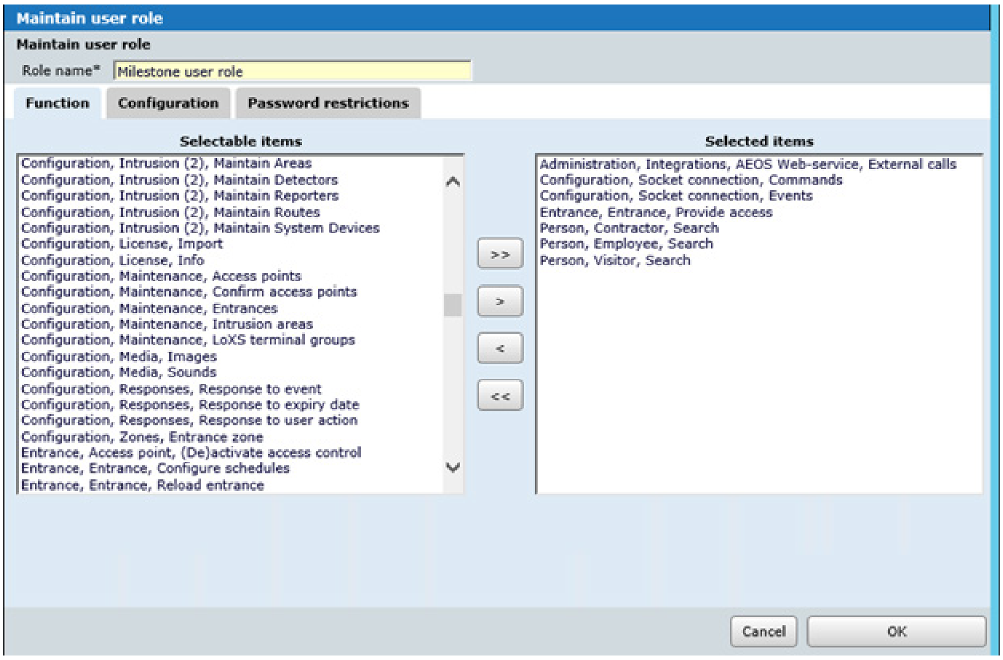
The SOAP Webservices are used for exchanging identifier information. The Socket Interface is used to send events and retrieve commands. To be able to exchange identifier information, and to send and retrieve information, a new user role needs to be created. Before creating this user role, it is necessary to know, which carrier types (employees, visitors, contractors) need to be visible in Milestone XProtect. In the example below, employees, visitors and contractors are included.

1. Log in to AEOS Maintenance & Configuration.
2. Go to **Management** > **Maintain user role.**
3. Click **New**.
4. Enter a new and meaningful name. at the blank space behind **Role name.**
5. Scroll down the list of selectable items in the function tab within the main window. Select the following items by clicking on the item, and subsequently on the **>** button at the panel in the middle of the screen:
   - **Administration, Integrations, AEOS Web-service, External calls**
     This item has to be selected to be able to use the SOAP WebService.
   - **Configuration, Socket connection, Commands**
     This item has to be selected so that Milestone can send the correct commands to AEOS.
   - **Configuration, Socket connection, Events**
     This item has to be selected so that Milestone can receive events from AEOS.
   - **Entrance, Entrance, Provide access**
     This item has to be selected to provide access to persons within the Milestone XProtect environment.
   - **Person, Contractor, Search**
     This item can be selected, if contractors need access to buildings and their identifier

information has to be visible within the Milestone XProtect environment. For AEOS Blue users this item is only available if the system property **44.04 Contractor management** has been activated beforehand. For AEOS Classic users this item is only available if license option 9809090 has been purchased.

- **Person, Employee, Search**
  This item can be selected if employees need access to buildings and their identifier information has to be visible within the Milestone XProtect environment.
- **Person, Visitor, Search**
  This item can be selected if visitors need access to buildings and their identifier information has to be visible within the Milestone XProtect environment.

6. Click **OK** to save the settings.



Maintain user role

Maintain user role

Role name* Milestone user role

Selectable items

Configuration, Intrusion (2), Maintain Areas
Configuration, Intrusion (2), Maintain Detectors
Configuration, Intrusion (2), Maintain Reporters
Configuration, Intrusion (2), Maintain Routes
Configuration, Intrusion (2), Maintain System Devices
Configuration, License, Import
Configuration, License, Info
Configuration, Maintenance, Access points
Configuration, Maintenance, Confirm access points
Configuration, Maintenance, Entrances
Configuration, Maintenance, Intrusion areas
Configuration, Maintenance, LoXS terminal groups
Configuration, Media, Images
Configuration, Media, Sounds
Configuration, Responses, Response to event
Configuration, Responses, Response to expiry date
Configuration, Responses, Response to user action
Configuration, Zones, Entrance zone
Entrance, Access point, (De)activate access control
Entrance, Entrance, Configure schedules
Entrance, Entrance, Reload entrance

Selected items

Administration, Integrations, AEOS Web-service, External calls
Configuration, Socket connection, Commands
Configuration, Socket connection, Events
Entrance, Entrance, Provide access
Person, Contractor, Search
Person, Employee, Search
Person, Visitor, Search

Step 06 Create a new AEOS system user

After defining the new user role, register a user that works as AEOS system user for the AEOS Milestone plug-in.

To add a new user:

1. Go to **Management > System users > Maintain user**.
2. Click **New** to add a new user.
3. Fill in the details under the **User** tab: name, password, role have to be filled in. For the role, select the role name you created in step 5, that corresponds with the new system user.
4. Click **OK** to save the settings.

Step 07 Stop the Milestone XProtect Management Server

1. In Windows, press the ⊞ **Win + R** key and enter **services.msc**.
2. Click **OK.**
3. In the **Services** window, right-click on **Milestone XProtect Management Server** and select **Stop**

Step 08 Install the AEOS Milestone plug-in

Download and install the plug-in to establish the connection between AEOS and Milestone.

1. Go to https://nedapsecurity.com. Go to **Firmware, configurations & tooling > Additional programmes**.
2. Download the **AEOS Milestone Xprotect plug-in** setup file.
3. Run the setup.
4. Install the plug-in at the following location:
   C:\Program Files\VideoOS\MIPPlugins\Nedap

Step 09 Restart the Milestone XProtect Management Server

Opening and configuring the Milestone XProtect environment is only possible after the Milestone XProtect Management Server has been restarted.

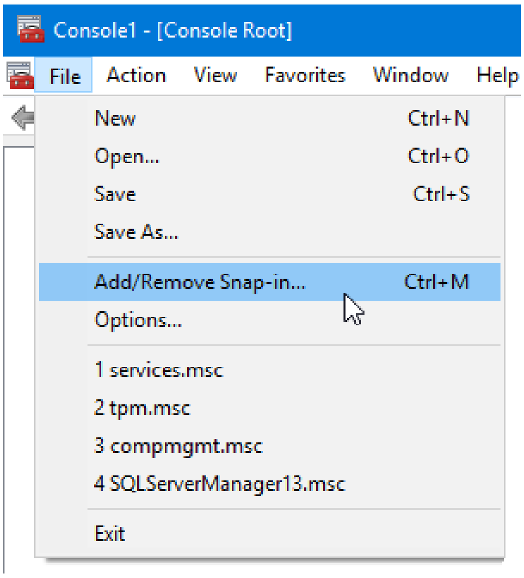
1. In Windows, press the ⊞ **Win + R** key and enter **services.msc**.
2. Click **OK.**
3. In the **Services** window, right-click on **Milestone XProtect Management Server** and select **Start.**

Step 10 Add the Certificate Manager to Microsoft Management Console

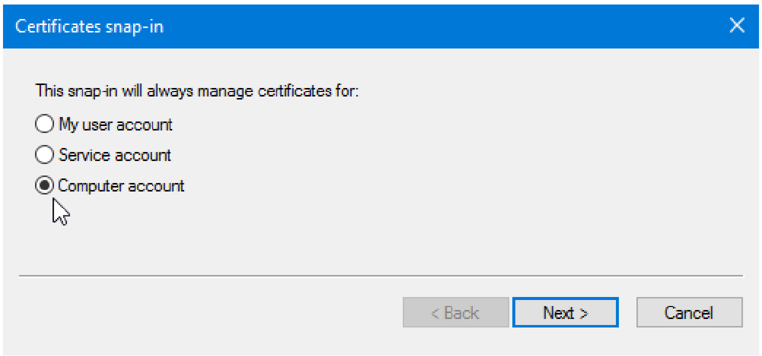
The Milestone server checks the local computer's root certificates. This means the AEOS certificate should be available in the local computer's certificate store. You can use the Microsoft Management Console (mmc.exe) to add the certificate to the local computer's certificate store.

First you need to add the Certificate Manager to Microsoft Management Console:

1. In Windows, press the ⊞ **Win + R** key and enter `mmc`.
2. Click **OK**.
3. In the **File** menu, click **Add/Remove Snap-in...**



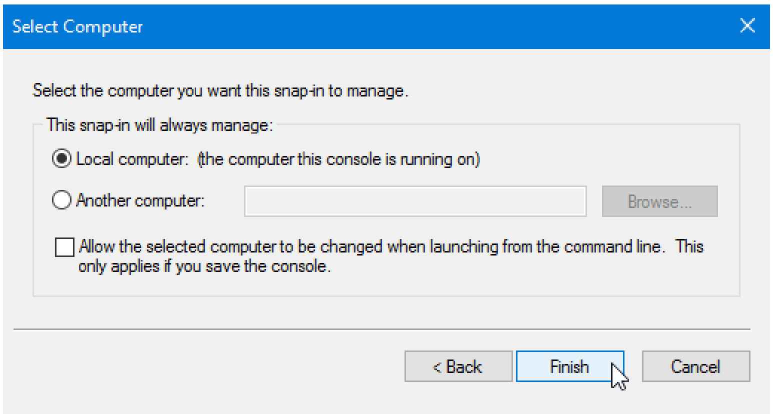
4. In the **Add/Remove Snap-in** box, click **Add**.
5. In the **Available Standalone Snap-ins** list, click **Certificates** and then click **Add**.
6. Click **Computer Account** and then click **Next**.


Certificates snap-in

This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

7. Click **Local computer** (the computer this console is running on)' option, and then click **Finish**.


Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

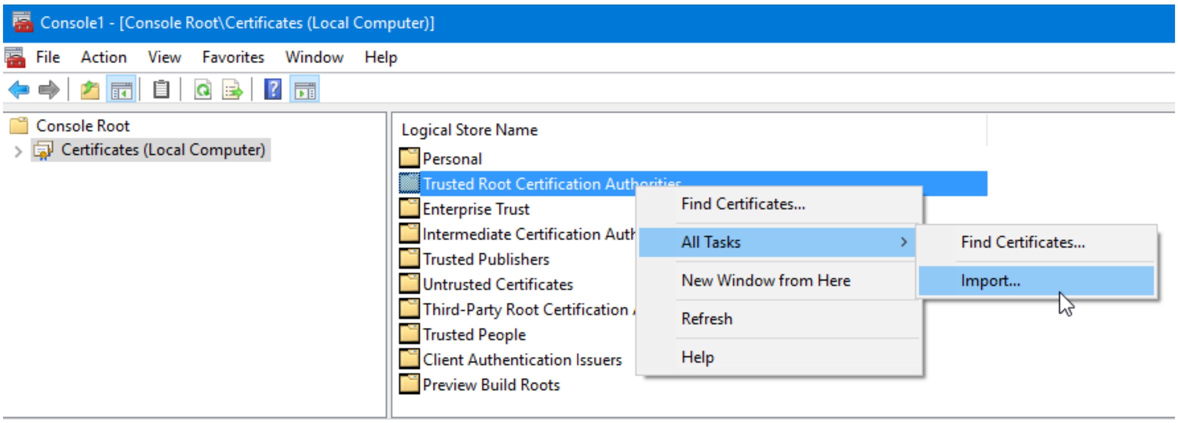
8. Click **Close**, and then click **OK**.

Step 11 Add the AEOS certificate to the certificate store

Now you can use the Microsoft Management Console to add the AEOS certificate to the local computer's certificate store:

In some situations, you first need to export the AEOS certificate. If so, please read the instructions in the *AEOS Software Installation Manual* or the *AEOS SSL Manual*. Steps may differ according to your browser.

9. Click **Certificates (Local Computer).**
10. Right mouse click T**rusted Root Certification Authorities**, select **All tasks** and click **Import**. The Certificate Import Wizard will start.



11. Import the AEOS certificate, using the Certificate Import Wizard.

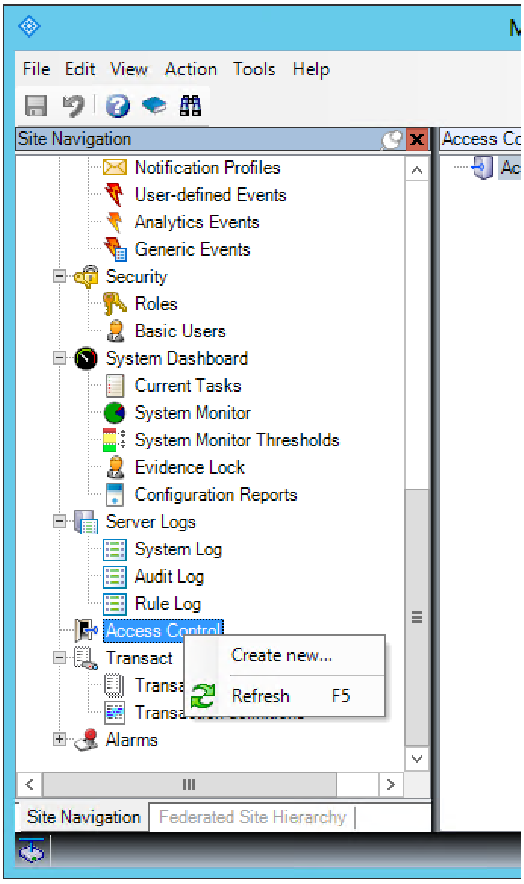
Step 12 Restart the Milestone Event Server

1. In Windows, press the ⊞ **Win + R** key and enter **services.msc**.
2. Click **OK.**
3. In the **Services** window, right-click on **Milestone Event Server** and select **Restart.**

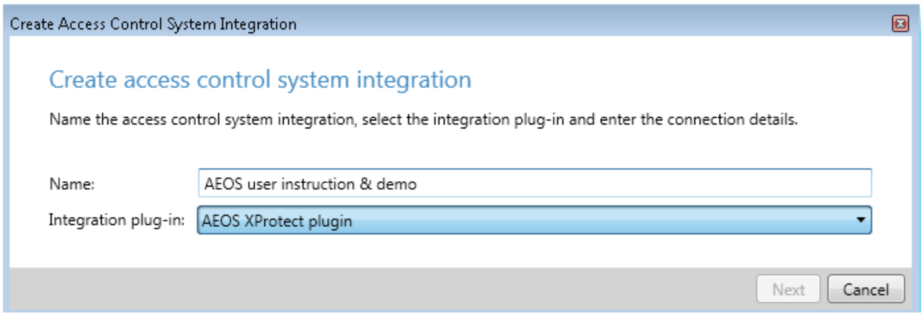
Step 13 Configure AEOS in Milestone

To connect the access points to the cameras, the configuration takes place in the Milestone XProtect Management client.

1. Open the Milestone XProtect Management Client.
2. Right mouse click **Access Control**.
3. Select **Create new**.



4. Enter a name.
5. Select **AEOS XProtect plug-in**.



Create Access Control System Integration

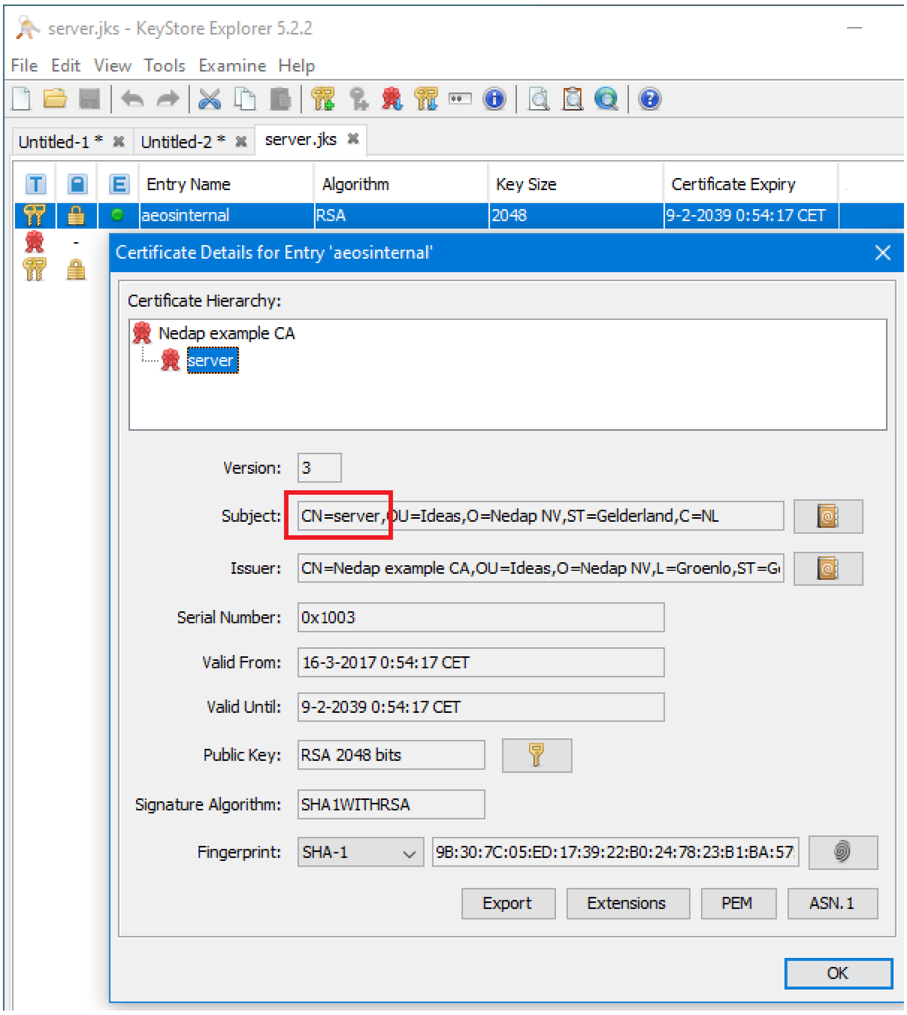
Create access control system integration

Name the access control system integration, select the integration plug-in and enter the connection details.

Name: AEOS user instruction & demo

Integration plug-in: AEOS XProtect plugin

6. Enter the correct settings.
7. For AEOS version 3.4 and newer versions:
   Enter the **Socket Certificate Subject CN**.
   Use KeyStore Explorer (or another application to navigate KeyStores) to find the correct settings. Browse to **...\AEOS\AEserver\jboss\standalone\certs\server.jks**. The default keystore password is **nedap123**. See the example below:



server.jks - KeyStore Explorer 5.2.2

T	E	Entry Name	Algorithm	Key Size	Certificate Expiry
		aeosinternal	RSA	2048	9-2-2039 0:54:17 CET

Certificate Details for Entry 'aeosinternal'

Certificate Hierarchy:
Nedap example CA
server

Version: 3

Subject: CN=server,OU=Ideas,O=Nedap NV,ST=Gelderland,C=NL

Issuer: CN=Nedap example CA,OU=Ideas,O=Nedap NV,L=Groenlo,ST=G

Serial Number: 0x1003

Valid From: 16-3-2017 0:54:17 CET

Valid Until: 9-2-2039 0:54:17 CET

Public Key: RSA 2048 bits

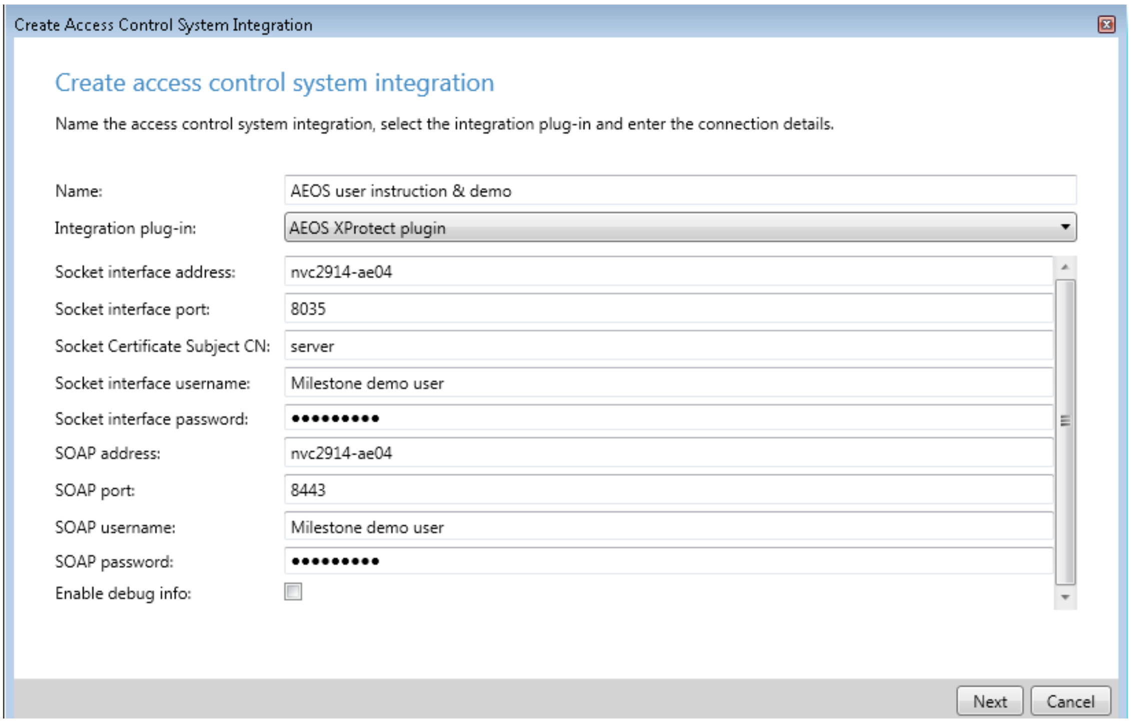
Signature Algorithm: SHA1WITHRSA

Fingerprint: SHA-1 9B:30:7C:05:ED:17:39:22:B0:24:78:23:B1:BA:57

8. Use the AEOS system username/password you created in step 6 for the socket interface username/password and the SOAP username/password.
9. Leave the **Enable debug info** box unchecked.
   It is possible to log debug information in the Milestone Xprotect Event Server log, located at **...\ProgramData\Milestone\XProtect Event Server\logs\MIPLogs**. Nedap recommends you not to use this function together with the AEOS Milestone plug-in unnecessarily, as the log files can grow very large.

The certificate uses hostnames. You cannot use IP addresses for TLS enabled connections to the AEOS server.

10. Click **Next** to continue.



Create Access Control System Integration

Create access control system integration

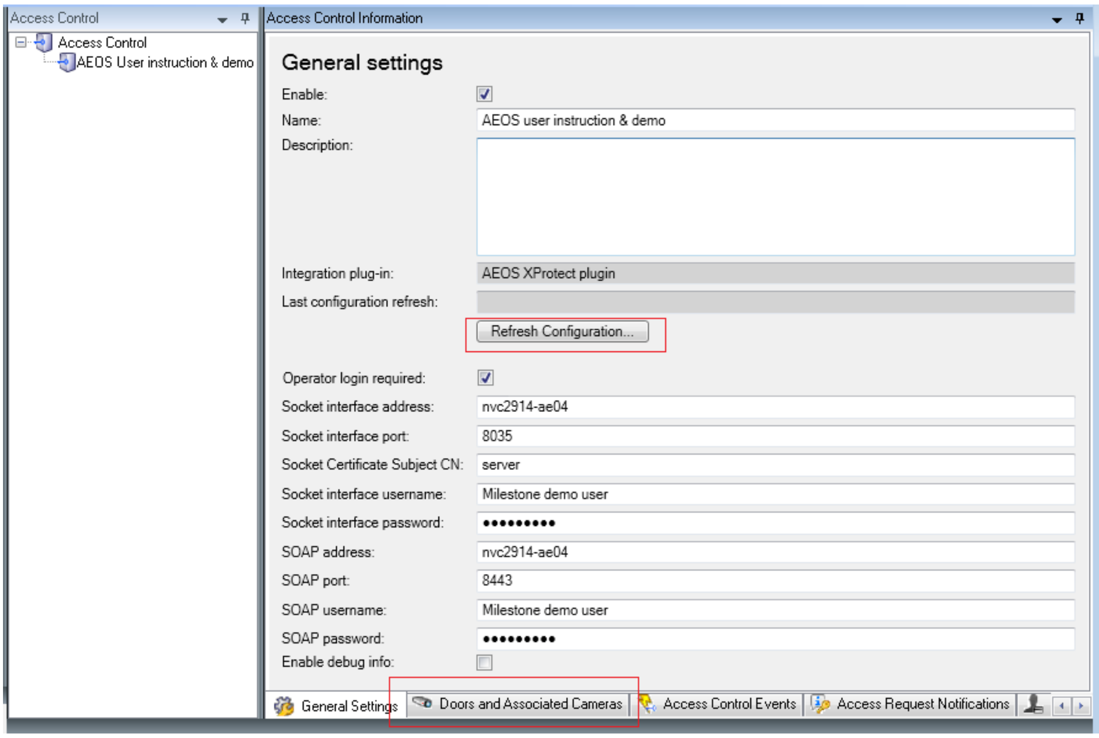
Name the access control system integration, select the integration plug-in and enter the connection details.

Name:	AEOS user instruction & demo
Integration plug-in:	AEOS XProtect plugin
Socket interface address:	nvc2914-ae04
Socket interface port:	8035
Socket Certificate Subject CN:	server
Socket interface username:	Milestone demo user
Socket interface password:	•••••••••
SOAP address:	nvc2914-ae04
SOAP port:	8443
SOAP username:	Milestone demo user
SOAP password:	•••••••••
Enable debug info:	□

11. Wait until all configuration data are collected. The window shows all doors, units, servers, events, commands and states that are detected by Milestone from AEOS. Click **Next** to continue.

The general settings of the new access control system appear in the main window. If these settings have to be adjusted, click the **Refresh Configuration...** button after the adjustments have been made.

12. For AEOS version 3.4 and newer versions:
    Enable the **Operator login required** checkbox if you want to personalise the access control commands. Enabling this function means that all operators must log in with their personal AEOS user credentials. AEOS will keep track of the commands that are sent by the individual operators. Also, specific filters can manage which entrances each individual operator is allowed to see, lock or unlock. only.



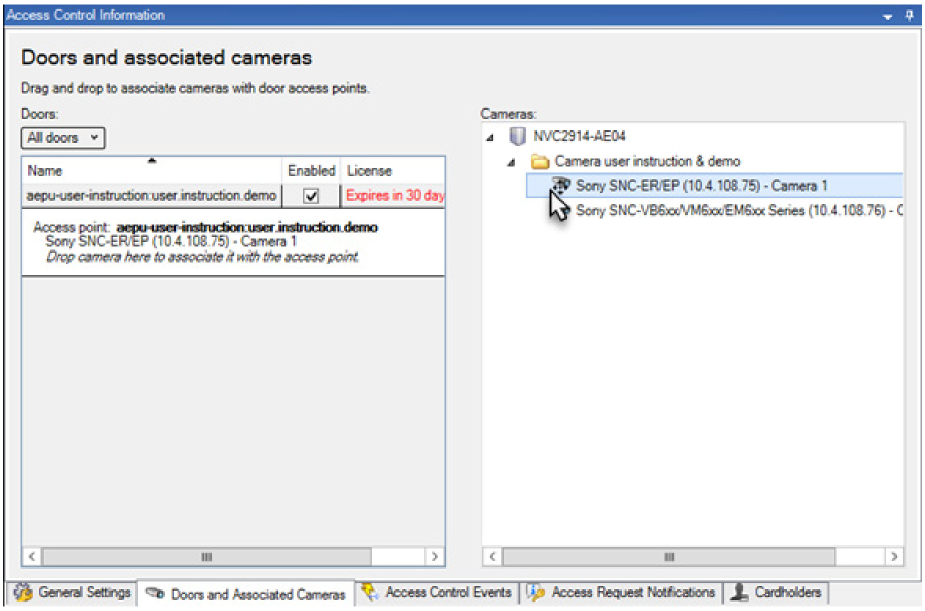
General settings

Enable: ☑
Name: AEOS user instruction & demo
Description:
Integration plug-in: AEOS XProtect plugin
Last configuration refresh:
Refresh Configuration...
Operator login required: ☑
Socket interface address: nvc2914-ae04
Socket interface port: 8035
Socket Certificate Subject CN: server
Socket interface username: Milestone demo user
Socket interface password: •••••••••
SOAP address: nvc2914-ae04
SOAP port: 8443
SOAP username: Milestone demo user
SOAP password: •••••••••
Enable debug info: □

13. Click the **Doors and Associated Cameras** tab at the bottom of the window.

A new window opens. On the left side of the window all access points (doors) are shown. On the right side of the window all cameras are shown. In this example only one entrance and one camera are available.

14. Select the camera that has to be connected to the access point (door). Drag and drop the camera to connect it to the correct access point (door).
15. Repeat this step for all cameras and associated access points (doors).
16. Check the **Enabled** checkbox to enable the connection between the camera and the access point.



Access Control Information

Doors and associated cameras

Drag and drop to associate cameras with door access points.

Doors: All doors

Name	Enabled	License
aepu-user-instruction:user.instruction.demo	☑	Expires in 30 day

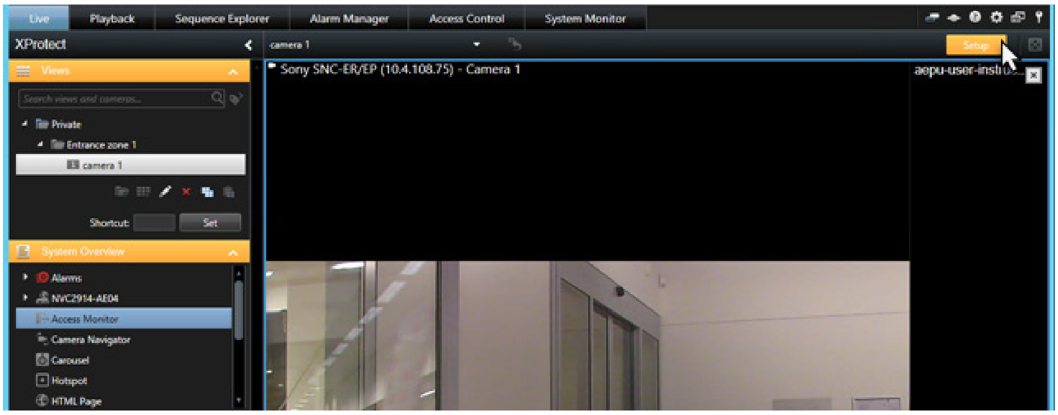
Access point: **aepu-user-instruction:user.instruction.demo**
Sony SNC-ER/EP (10.4.108.75) - Camera 1
Drop camera here to associate it with the access point.

Cameras:

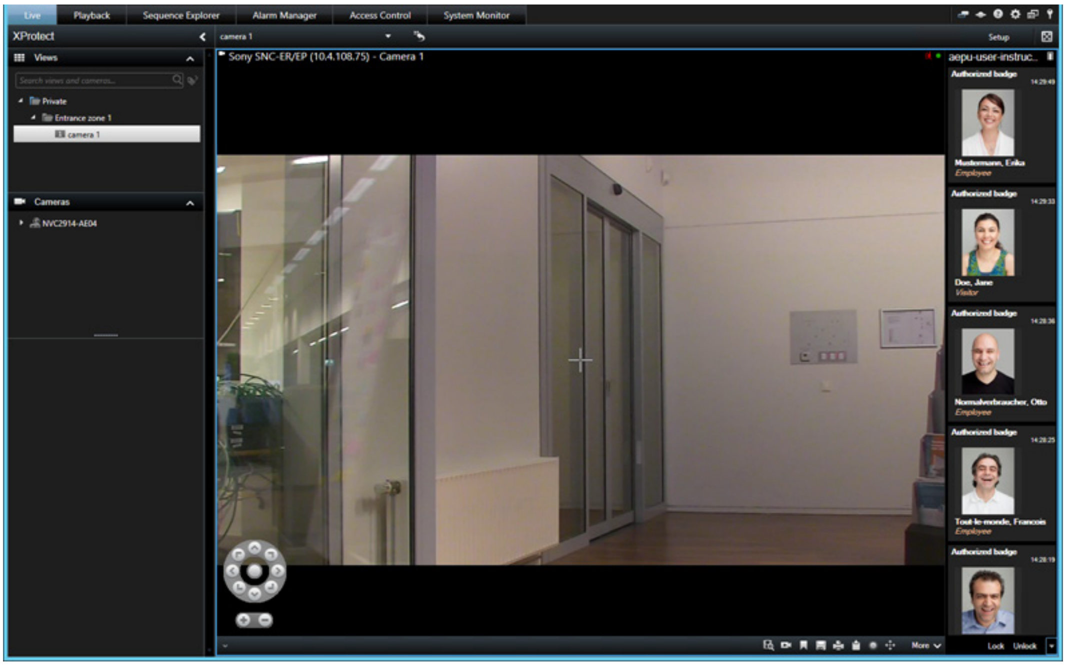
- NVC2914-AE04
  - Camera user instruction & demo
    - Sony SNC-ER/EP (10.4.108.75) - Camera 1
    - Sony SNC-VB6xx/VM6xx/EM6xx Series (10.4.108.76) - C

17. Save the settings by clicking the button in the upper left corner of the Milestone XProtect Management Client.

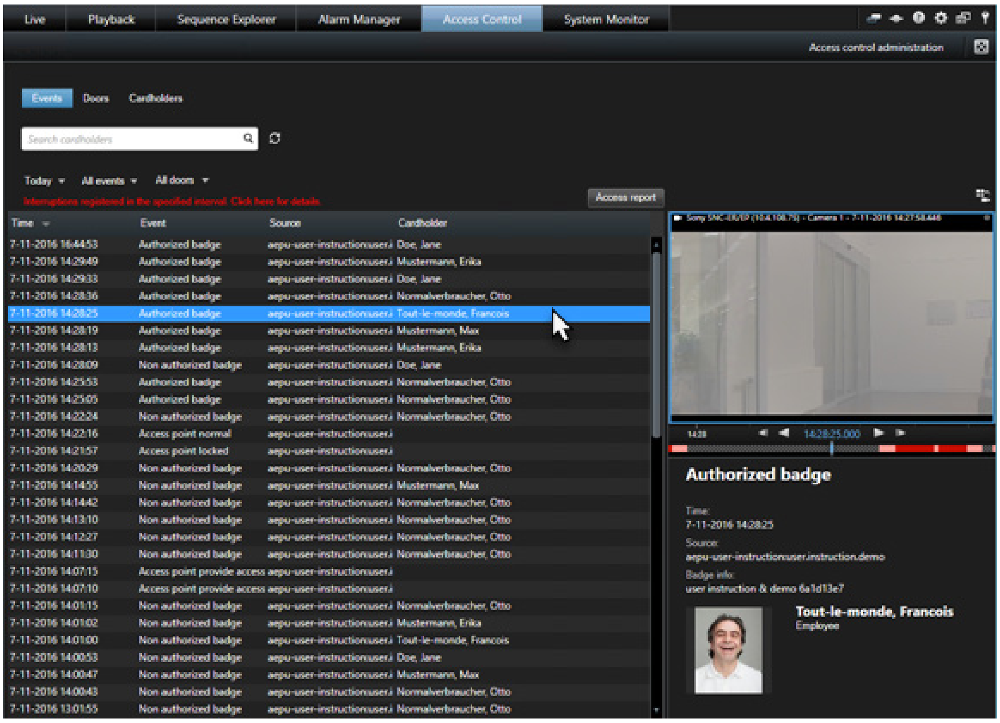
18. Open the **Live** mode in the Milestone XProtect Smart Client.
19. Click **Setup**.
20. Select **Access Monitor** in the left menu. Drag and drop **Access Monitor** into the right panel.
21. Click **Setup** again.



Now, all access point events for this door are visible in the right panel.



Detailed information about events is also visible in the **Access Control** mode.



Interruptions registered in the specified interval. Click here for details.

Time	Event	Source	Cardholder
7-11-2016 16:44:53	Authorized badge	aepu-user-instructionuser.i	Doe, Jane
7-11-2016 14:29:49	Authorized badge	aepu-user-instructionuser.i	Mustermann, Erika
7-11-2016 14:29:33	Authorized badge	aepu-user-instructionuser.i	Doe, Jane
7-11-2016 14:28:36	Authorized badge	aepu-user-instructionuser.i	Normalverbraucher, Otto
7-11-2016 14:28:25	Authorized badge	aepu-user-instructionuser.i	Tout-le-monde, Francois
7-11-2016 14:28:19	Authorized badge	aepu-user-instructionuser.i	Mustermann, Max
7-11-2016 14:28:13	Authorized badge	aepu-user-instructionuser.i	Mustermann, Erika
7-11-2016 14:28:09	Non authorized badge	aepu-user-instructionuser.i	Doe, Jane
7-11-2016 14:25:53	Authorized badge	aepu-user-instructionuser.i	Normalverbraucher, Otto
7-11-2016 14:25:05	Authorized badge	aepu-user-instructionuser.i	Normalverbraucher, Otto
7-11-2016 14:22:24	Non authorized badge	aepu-user-instructionuser.i	Normalverbraucher, Otto
7-11-2016 14:22:16	Access point normal	aepu-user-instructionuser.i	
7-11-2016 14:21:57	Access point locked	aepu-user-instructionuser.i	
7-11-2016 14:20:29	Non authorized badge	aepu-user-instructionuser.i	Normalverbraucher, Otto
7-11-2016 14:14:55	Non authorized badge	aepu-user-instructionuser.i	Mustermann, Max
7-11-2016 14:14:42	Non authorized badge	aepu-user-instructionuser.i	Normalverbraucher, Otto
7-11-2016 14:13:10	Non authorized badge	aepu-user-instructionuser.i	Normalverbraucher, Otto
7-11-2016 14:12:27	Non authorized badge	aepu-user-instructionuser.i	Normalverbraucher, Otto
7-11-2016 14:11:30	Non authorized badge	aepu-user-instructionuser.i	Normalverbraucher, Otto
7-11-2016 14:07:15	Access point provide access	aepu-user-instructionuser.i	
7-11-2016 14:07:10	Access point provide access	aepu-user-instructionuser.i	
7-11-2016 14:01:15	Non authorized badge	aepu-user-instructionuser.i	Normalverbraucher, Otto
7-11-2016 14:01:02	Non authorized badge	aepu-user-instructionuser.i	Mustermann, Erika
7-11-2016 14:01:00	Non authorized badge	aepu-user-instructionuser.i	Tout-le-monde, Francois
7-11-2016 14:00:53	Non authorized badge	aepu-user-instructionuser.i	Doe, Jane
7-11-2016 14:00:47	Non authorized badge	aepu-user-instructionuser.i	Mustermann, Max
7-11-2016 14:00:43	Non authorized badge	aepu-user-instructionuser.i	Normalverbraucher, Otto
7-11-2016 13:01:55	Non authorized badge	aepu-user-instructionuser.i	Normalverbraucher, Otto

Authorized badge

Time:
7-11-2016 14:28:25

Source:
aepu-user-instructionuser.instruction.demo

Badge info:
user instruction & demo 6a1d13e7

Tout-le-monde, Francois
Employee

5. List of supported AEOS events

Event number	Event description	Plug-in version
Accesspoint (210)		
Authorized badge access		
1015	Authorized badge access	2.1
Unauthorized badge access		
1119	BadgeNoAccessEvent, verification has no result	2.1
1120	BadgeNoAccessEvent, verification alarm	2.1
1121	BadgeNoAccessEvent, authorisation has no result	2.1
1122	BadgeNoAccessEvent, verification invalid	2.1
1123	BadgeNoAccessEvent, verification aborted	2.1
1127	BadgeNoAccessEvent, unassigned badge	2.1
1128	BadgeNoAccessEvent, outside schedule	2.1
1129	BadgeNoAccessEvent, not valid yet/anymore	2.1
1130	BadgeNoAccessEvent, internal error // invalid (non-existent) schedule	2.1
1131	BadgeNoAccessEvent, no authorization for this entrance	2.1
1132	BadgeNoAccessEvent, APB invalid direction	2.1
1133	BadgeNoAccessEvent, APB request from unknown entrance	2.1
1134	BadgeNoAccessEvent, APB auth. req. already running	2.1
1135	BadgeNoAccessEvent, APB illegal presence	2.1
1136	BadgeNoAccessEvent, APB unavailable zone manager	2.1
1137	BadgeNoAccessEvent, APB incorrect configured AEpu	2.1
1199	BadgeNoAccessEvent, person is blocked (blacklisted)	2.1
1200	BadgeNoAccessEvent, verification device does not know carrier	2.1
1201	BadgeNoAccessEvent, no authorization for this entrance	2.1
1202	BadgeNoAccessEvent, person is blocked	2.1
1203	(Replaced by 1397)	2.1
1204	(Replaced by 1397)	2.1
1205	(Replaced by 1397)	2.1
1206	(Replaced by 1397)	2.1
1207	BadgeNoAccessEvent, authorization is not yet valid	2.1
1208	BadgeNoAccessEvent, authorization is expired	2.1

Event number	Event description	Plug-in version
Door status		
1001	Access point locked	2.1
1002	Access point normal	2.1
1003	Access point unlocked	2.1
1362	DoorOpenedEvent activated	2.1
1363	DoorOpenedEvent de-activated	2.1
1397	BadgeNoAccessEvent	2.2
1196	ProvideAccessEvent	2.1
1005	Direct door alarm start	2.1
1006	Direct door alarm end	2.1
1007	Door open too long start	2.1
1008	Door open too long end	2.1
1012	Door manual unlock start	2.1
1013	Door manual unlock end	2.1
1050	EmergencyUnlockedEvent begin	2.1
1051	EmergencyUnlockedEvent end	2.1
Intrusion - AlarmLogbookEntry (215)		
1497	Burglary alarm started	2.1
1498	Burglary alarm restored	2.1
1499	Panic alarm started	2.1
1500	Panic alarm restored	2.1
1501	Hold-up alarm started	2.1
1502	Hold-up alarm restored	2.1
1503	24-hour alarm started	2.1
1504	24-hour alarm restored	2.1
1505	Technical alarm started	2.1
1506	Technical alarm restored	2.1
1507	Tamper alarm started, reason: Sabotaged, shortcut	2.1
1508	Tamper alarm started, reason: Sabotaged, open	2.1
1509	Tamper alarm started, reason: Sabotaged, connection lost	2.1
1510	Tamper alarm started, reason: Masked	2.1
1511	Tamper alarm started, reason: Alarm equipment tampered	2.1
1512	Tamper alarm restored, reason: Sabotaged, shortcut	2.1

Event number	Event description	Plug-in version
1513	Tamper alarm restored, reason: Sabotaged, open	2.1
1514	Tamper alarm restored, reason: Sabotaged, connection lost	2.1
1515	Tamper alarm restored, reason: Masked	2.1
1516	Tamper alarm restored, reason: Alarm equipment tampered	2.1
1547	Masked alarm started	2.1
1548	Masked alarm restored	2.1
Secured input (211)		
1034	Input contact changed, passive	2.2
1035	Input contact changed, active	2.2
1036	Input contact changed, sabotage open	2.2
1037	Input contact changed, sabotage shortcut	2.2
Toggle (216)		
1086	BooleanStateChangedEvent True	2.2
1087	BooleanStateChangedEvent False	2.2

Copyright

Disclaimer

Nedap has made every effort to ensure the accuracy of the information contained in this document. However, Nedap makes no representations or warranties whatsoever whether express or implied as to the accuracy, correctness, currency, completeness or fitness or suitability for any purpose of such information and therefore disclaims to the maximum extent permitted by applicable law any and all liability for any error, damage, loss, injury or other consequence which may arise from use in any manner of any information contained in this document. Nedap makes no commitment to update or keep current the information in this document and reserves the right to make improvements to this document and/or the products described therein at any time without notice.

Nedap Security Management
P.O. Box 103
NL - 7140 AC Groenlo
+31 (0)544 471 111
info@nedapsecurity.com
www.nedapsecurity.com

nedap | security management