Aachen
2020-10

Release notes for Access Management System (AMS) Version 3.0

These release notes are intended to acquaint you with your new software version as quickly as possible.

Revision History	
Original version	2020-06
Added 1.6 Advice for security of personal data	2020-10

Table of Contents:

1 Installation Notes

1.1 Supported operating systems

AMS runs on the following operating systems:

	AMS Server	AMS Client
Windows 10 Enterprise 2019 LTSC (Windows 10, Version 1809)	Yes	Yes
Windows 10 Professional (Version 1909)	Yes	Yes
Windows Server 2016 (64bit) Standard or Datacenter	Yes	Yes
Latest drivers and OS updates are highly recommended.		

1.2 Server

The following are the hardware and software requirements for an AMS server

Minimum hardware requirements	• Intel i5 processor with at least 4 physical cores
	• 8 GB RAM (32 GB recommended)
	• 200 GB of free hard disk space (SSD recommended)
	• Graphics adapter with
	  ○ 256 MB RAM,
	  ○ a resolution of 1280x1024
	  ○ at least 32 k colors
	• 1 Gbit/s Ethernet card
	• A free USB port or network share for installation files

1.3 Client

The following are the hardware and software requirements for a AMS client

Minimum hardware requirements	• Intel i5 processor (4 Core) or greater • 8GB RAM (16 GB recommended) • 20GB free hard disk space • Graphics adapter with 1920 x1080 resolution, 32k colors, 256MB dedicated memory with DirectX 11 or later • 1 Gbit/s Ethernet card • Free USB port for Dialog Reader or camera • Recommended: Wide-screen monitor for Map View.

1.4 Update of AMS 1.0 to AMS 3.0

Upgrade from 1.0 to 2.0 as described in AMS 2.0.

Then upgrade to 3.0 as described below.

1.5 Update of AMS 2.0 to AMS 3.0

Recommended way:

1. Create backup of AMS 2.0
2. Update AMS 2.0 to AMS 3.0 on same machine.

Update of multiple MACs:
If your installation uses multiple MACs, deinstall the MAC of AMS 2.0 package on each MAC server, and then run the MAC installer of the AMS 3.0 package on each MAC server.

1.6 Advice for security of personal data

In accordance with international and national data protection laws, companies are obliged to delete from their electronic media all personal data when it is no longer required.
You are hereby advised that access controllers and readers may contain such personal information, and that you are consequently obliged to use and dispose of them as electronic media in the sense of these data protection laws.

2 New features in AMS 3.0

2.1 AMS/BVMS Integration

AMS now integrates with BVMS as a Video Management System (VMS). Operators can monitor alarms, events and device states from the AMS on BVMS, and send commands to AMS devices via the BVMS Operator Client.

Use cases for AMS/BVMS integration:

- Browsing of configured doors and readers,
- Video Verification of the IDs of persons entering the building, and the ability to grant or deny access from BVMS.
- Door commands: (disable, set normal or office modes of operation).
- Handling reader events: (access denied, access granted, access requested, cardholder did not enter after access granted, access granted but randomly selected for extra checks, “random screening”).
- Handling door events/states: door forced, door jammed open, door contact states: [Door opened, Door closed], door lock states [unlocked, locked, secured]
- Handling duress signals.
- DIP/DOP (generic binary open/close events and commands.
- Handling Devices online/offline events

2.2 Intrusion panel Integration

AMS now integrates Bosch Intrusion panels, allowing an operator to monitor, arm and disarm intrusion areas.

Use cases for Intrusion panel integration:

- Alarm viewer
  - Incoming intrusion alarms are listed
    The time recorded in the alarm list is the time when alarm was received in AMS (for intrusion events)
  - Hint: Configure intrusion alarms as Critical in the alarm list of the Map View application.
- Map
  - Listing and filtering Intrusion areas in the Intrusion areas table
  - Adding areas, points (detectors) and panels graphically via the edit function. Intrusion panels and points appear on the map as icons
  - Displaying the states of Intrusion areas in the area list
  - Filtering of layers for access and intrusion devices / areas(Intrusion)
  - Single selection of multiple intrusion areas for sending commands

NOTE: The receiving of events and alarms depends on the network and system availability. AMS does not buffer intrusion alarms that occur while the network or the system itself is down.

2.2.1 Cardholder synchronization with B/G panels

AMS 3.0 supports the synchronization of cardholder data between AMS and B/G panels via the RPS (Remote Programming Software) tool.
The items synchronized include:

- name
- user group
- passcode
- access card
- key fob
- remote access authorization
- language
- authorization profile
- authorization level
- reports

Limitations:

- Multiple intrusion panels can belong to one AMS Intrusion authorization profile, but only one AMS Intrusion authorization profile can be assigned to one person.
- If 37 bit cards, e.g iClass HID 37 bit cards are used both for arming intrusion panels and for access control in AMS, then the facility code must not be larger than 32767.
  If these cards are used only for access control functionality in AMS then the limitation does not apply.
- Temporary cards cannot be used for intrusion panels, because intrusion authorisations cannot currently be transferred to temporary cards.

2.3 Support TLS 1.2 for ODBC connections

We have updated our ODBC connections to support TLS 1.2.
For high-security sites, configure your Windows system to disallow TLS 1.0 and 1.1 connections.

2.4 Device editor allows the copy/paste of AMC device trees

The device editor allows you to copy and paste the configurations of AMCs with all subdevices.

2.5 Enhanced door model 14

Door model 14 has been enhanced to allows the disarming of alarms and access in one step, if so configured.

2.6 Handling of the "Outside" area by the MAC

The default timeout for the location of persons within the site is 24 hours. After this time, the location of these persons will be set automatically to **Outside**. This timeout is now configurable for each MAC in the device editor. The timeout can be disabled by setting a value of 0.

2.7 Faster communication down the device hierarchy

Improved the communication speed from DMS to MAC to AMC: Cold and warm starts are performed multiple times faster than before, depending on the number of cardholders) Excellent performance is possible using AMCs with 2GB CF cards, as tested with more than 400.000 cardholders.

2.8 SDK: 1 factor authentication

3rdParty systems can use the AMS API to present an access card virtually at an existing and configured access reader. The AMC validates the permission of the transmitted card data, and makes the access decision as usual. For details, see the API documentation.
The access card reader remains fully functional and can continue to be used in the normal way.

2.9 Map View: enhancement to device labels

If a device or an intrusion area is dragged onto the map, it is possible to specify a label for that map element. By default, the name of the device or area is being used.

In AMS V2.0, *subsequent* changes of the device/area name were not propagated to the corresponding map element. The operator had to change the label of the map element manually.

In AMS V3.0, renames in the device editor are automatically propagated to the corresponding map element unless the operator has overwritten the label manually (manually given labels take precedence).

3 Mandatory-installation steps for Intrusion integration

AMS/Intrusion integration requires the installation of RPS API package version V2.1.25454 or later.
The RPS API must be installed on a separate computer from the AMS server. For example it can be installed where the RPS tool itself is installed. The RPS tool is needed to configure and manage the B/G panels.
Communication between AMS and the RPS tool to the panels is performed via the RPS-API. Both tools (RPS tool and RPS API) need to be installed on a computer other than the AMS server.
SDK communication to the B/G panels is inlcuded in AMS. No separate installation is required, but `Mode2`and a `AutomationPasscode` must be enabled in the panel.

3.1 Supported Panels

These B/G intrusion panels are supported by AMS 3.0:

- B3512
- B4512
- B5512
- B8512G
- B9512G
- B6512

3.2 ACE programming interface (SDK, API)

Applications using the SDK from AMS V3.0 are largely compatible with BISACE 4.6-4.8 and AMS V2.0.
Changes to the API are documented in detail in the files, `ACE API.pdf` and `ACE API Database- xxx.pdf`.

3.3 AMS-XPAN-1V30 license is missing from Licenses folder

Special instructions for purchasers of the license: **AMS-XPAN-1V30**
(a single additional Intrusion panel)

In order to activate this license in AMS 3.0 perform the following prerequisite steps, directly after installing AMS 3.0:

1. From the online catalogue, download the ZIP file:
   `AMS 3.0 AMS-XPAN-1V30 License Patch.zip` to your computer.

2. From the ZIP file, extract the folder `AMS-XPAN-1V30` (directly below the `licensing` folder).
3. Copy this folder and its contents to the `Licenses` folder of your AMS 3.0 installation. The default path is:
   `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\AccessEngine\AC\Licensing\Licenses\`
4. Run AMS as Administrator, and navigate to **Main menu** > **Configuration** > **Licenses**

Click **Start license manager...** and verify that the license type **AMS-XPAN-1V30** appears in the **Expansion** list.

4 Optional post-installation steps

4.1 Retention Time of System Events

The retention time for system events is configurable. The default is 30 days, which means that events that are older than 30 days are deleted automatically.
To specify a different value, follow these steps:

1. Start Registry Editor (press [Windows]+[R], enter “regedit.exe”)
2. Navigate to path
   `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Micos\SPS\DEFAULT_\Loggifier\SysKeep`
3. Double click value “@value” (shown in the right pane) and enter a new value.

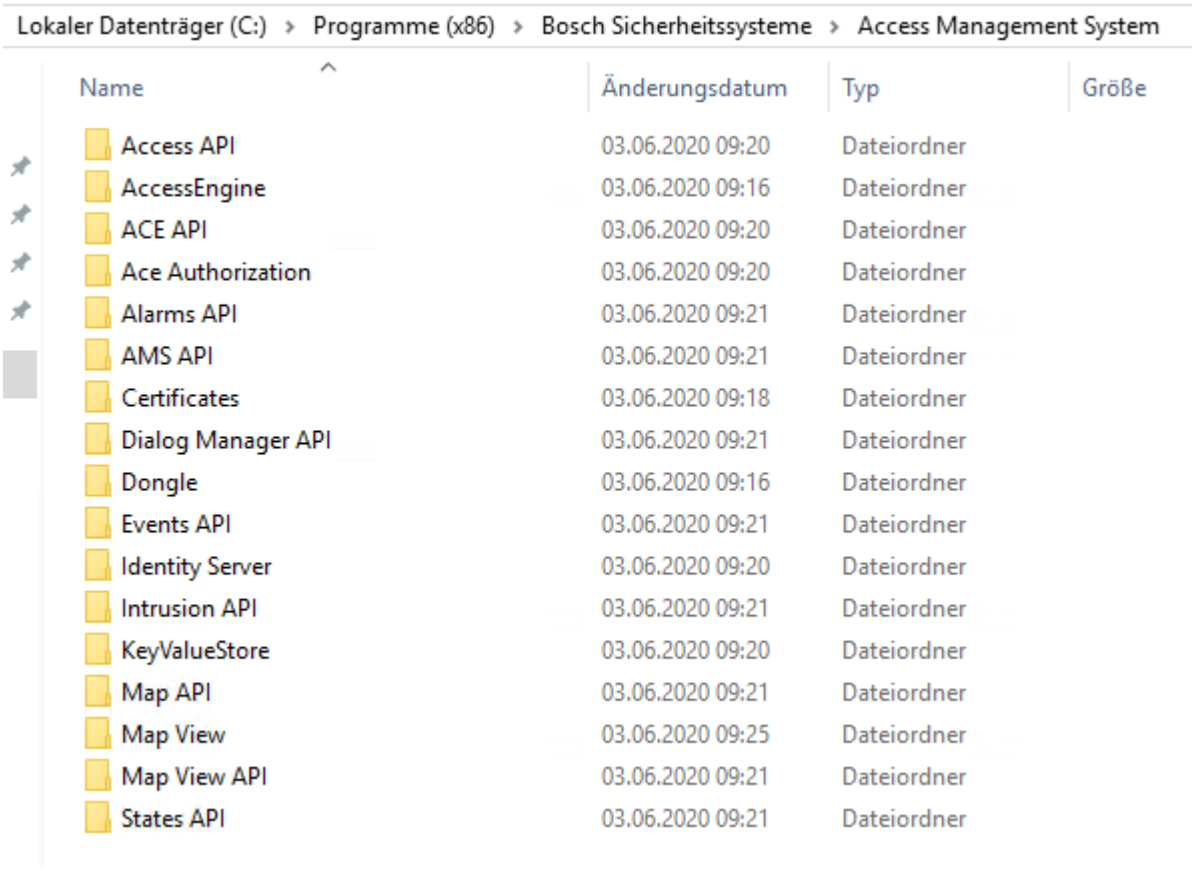
Note that the retention time has a major impact on the size of the backup files. To make the most of your storage space, choose the lowest value compatible with your contractual and legal requirements.

4.2 Trace Level of Services used by Map View

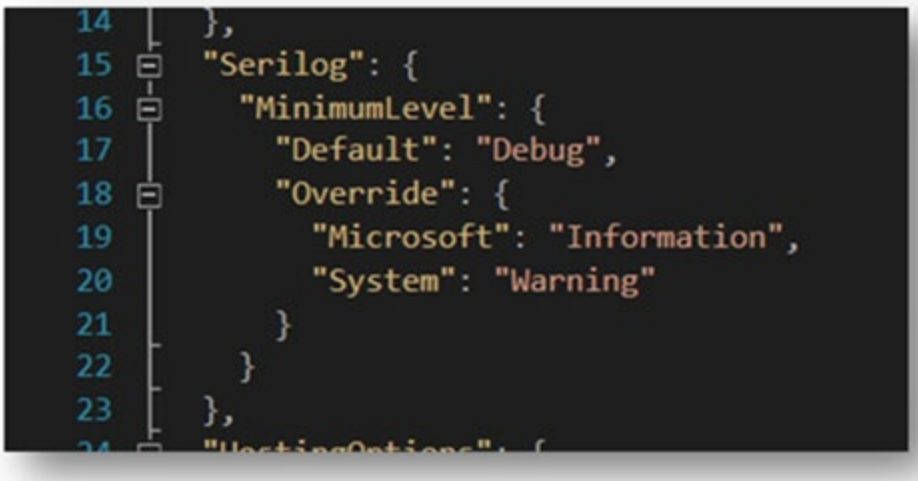
The services used by the Map View application use a logging interface that is independent of that of the other backend services. This section describes how this logging can be configured.

The logging configuration can be found on the server in the individual API folders in a file called `appsettings.json`. If installed in the default directory, this file can only be changed by users with Administrative rights.

- Bosch Access API
- Bosch ACE API
- Bosch ACE Authorization
- Bosch AMS API
- Bosch Dialogmanager API
- Bosch States API
- Bosch Alarms API
- Bosch KeyValueStore
- Bosch Intrusion API
- Bosch Events API
- Bosch Map API
- Bosch MapView API
- Bosch ACE Identity Server



The `appsettings.json` file can be opened with a text editor. The section for logging configuration section is as follows:



Default logging configuration:

```
"Serilog": {
    "MinimumLevel": {
```

```
        "Default": "Warning",
        "Override": {
            "Microsoft": "Warning",
            "System": "Warning"
        }
    }
}
```

Explanation: We are using Serilog for our logging, and it defines the levels: `Verbose`, `Debug`, `Information`, `Warning`, `Error` and `Fatal`.
The "MinimumLevel" settings (`Warning` in the screenshot) applies to all log sources (i.e. to the components that write to the log).

The "Override" section applies to specific log sources. For example in the screenshot, from components whose namespace starts with "Microsoft" only messages of level "Information" or higher will be logged. Similarly from .NET framework (i.e. namespace starting with "System"), only messages of level "Warning" or higher will be logged.

A minimal configuration would be:

```
"Serilog": {
    "MinimumLevel": {
        "Default": "Fatal"
    }
}
```

This minimal configuration will likely result in almost no log entries, except for the last error that crashed the runtime. There is no setting in the API to completely disable logging.

5 Known limitations in AMS 3.0

5.1 Languages

5.1.1 Settings required for Arabic installations

AMS requires the Windows System Locale to be set to Arabic. Otherwise AMS reports and some dialog controls will show invalid characters instead of Arabic characters.

This is especially important if the operating system was not originally Arabic and the support for Arabic language was added by installing a language pack. Installing a language pack does not update the system locale, so it must be set manually:

- Regional Settings > Administration > Language for non-Unicode programs > Change system locale: select an Arabic language
- Verify that the SQL server collation is set to “Arabic_CI_AS”

Alternatively, run the 'Set-WinSystemLocale' cmdlet with Administrator permissions. For example, ' Set-WinSystemLocale "ar-SA"' sets the System Locale to 'Arabic (Saudi Arabia)'.

5.1.2 AMS languages and Operating Systems

The language of the AMS installation must be the same as that of the operating system (OS). **The only exception is Turkish, where the OS has to be in English**.
Make sure that Client and Server are installed in the same language, otherwise the texts in the clients will contain a mix of languages.

5.1.3 AMS Setup languages and Operating Systems

The language of the AMS Setup corresponds to the UI culture of the OS. For example, if the UI culture of the OS is Brazilian Portuguese (pt-BR), the AMS Setup UI will be also in Brazilian Portuguese. The current UI culture of the OS can be checked by the PowerShell command *Get-UICulture*. If the OS UI culture does not match the locale of the AMS Setup, the AMS Setup UI will be in English (en-US).

5.2 Remarks and Limitations on MapView and Services

5.2.1 Initial States

Please note that the states initially displayed by the system immediatlely after installation are not necessarily correct. The reason for this behavior is that the system stores the states of the devices during operation, and on startup displays the states last seen. However some device states might have changed between the last shutdown and the current installation of the AMS Software. An example of this behavior is where MAC and Twin MAC are initially both displayed

with a slave symbol (**#216448)**. Only after a MAC-switch are the correct master and slave symbols displayed.
To refresh all device states, coldstart the system (DMS, MAC, AMCs, Readers etc..) and so force a MAC-switch.

5.3 Dialog Manager limitations

5.3.1 Signature Pad

Make sure that the latest signature pad firmware is installed on the corresponding client machine. The latest driver can be downloaded from `https://en.signotec.com/service/downloads/drivers/` > TWAIN and WIA Driver (`signotec_TWAIN_8.0.0.exe` or later).

5.3.2 Guard tour and SimonsVoss readers

Readers from SimonsVoss are not supported for guard tours.

5.3.3 Access IPconfig Tool

The Access IP config tool can not scan multiple network segments for fingerprint readers.

5.4 SQL Server machine

Run SQL Server only on the same machine as the AMS server. Database server computers separate from the AMS server are not supported.

5.5 Security issue in Milestone Xprotect

A bug in older versions of Milestone XProtect causes certificate validation to fail, and communication becomes insecure.

This bug has been verified in:

- XProtect 2018 R3 Corporate
- XProtect 2019 R2 Professional+
- XProtect 2019 R2 Corporate+

This bug is not present in:

- XProtect 2018 R3 Professional and possibly older versions
- XProtect Corporate 2020 R1

We recommend using **XProtect Corporate 2020 R1**.

Limitation:

The AMS-Milestone plugin does not work correctly if either the MAP 5000 plugin or the G-Series Panel plugin is installed on the same Milestone system.

5.6 Microsoft SQL Express

Microsoft SQL Express limitation:
The SQL Express database, installed with AMS 3.0, supports up to 1 million events.
The default retention time is 90 days.
Old events are deleted if:

- the database is at 85 % of its maximum capacity (the maximum size of an SQL Express 2017 database is 10 GB),
  or
- the retention period has expired

If your projections for the number of access events exceed these limitations, then we recommend you use a full version of Microsoft SQL Server.

6 Additional Notes

6.1 Tools in Start Menu (Server)

The following tools are provided in the Access Manager menu:

6.1.1 Access IP Config

A tool to scan the network for IP-based access devices. The tool contains its own online help.

6.1.2 Configuration Collector

A tool which is installed as part of the AMS server. It guides you through the collection of configuration information, and stores it in a ZIP file. This ZIP file can then be sent to Bosch Technical Support for troubleshooting.
The Configuration Collector provides its own online help, which can be invoked from any of its tab pages.

6.1.3 DB Password Change

A tool to change the password of the internal database account. System administrator “sa” privileges are required.

6.1.4 Backup

A tool to trigger database backups. It is described in detail in the operation manual.

6.1.5 Restore

A tool to start a database restore. It is described in detail in the operation manual.

6.2 Web Service

The Access Management System optionally provides a Web Service which can be used to retrieve specific data via HTTP.
Please note, that HTTP is not a secure protocol.
By default, the web service is disabled. To enable the service, follow these steps:

1. On the server, open the following file in a text editor: `\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\AccessEngine\AC\Cfg\PrcTable.tbl`

2. Locate the following section:

```
;set /executable=websrv-1.exe
;set /ready=0
;set /parameter=""
;set /restartlimit=3
;set /type=normal
;set /errorReset=100
;set /exitNumber=5000
;set /parameter=""
;add
```

3. Remove the semicolons at the beginning of each line
4. Save the file and restart the server.

After these steps, the web service is enabled. More details about using and configuring the service can be found in '`AddOns\ACE\AdditionalHTML-Docs`' on the AMS installation medium.

6.3 Integrating intrusion panels

Recommended practice:

While the RPS View dialog is open in the RPS Tool, then it is connected to the intrusion panel, and the AMS system cannot synchronize with the panels via the RPS API.

If panel users are configured in AMS then the changes are not propagated to the panels until the RPS View dialog is closed. This may take some time.
Recommendation: After configuring the intrusion panels in the RPS View dialog, close it. Do not leave the RPS View dialog open.

The AMS dialog **Panel administration** displays panels. These panels are displayed as soon as an RPS panel configuration is created in AMS. The panels displayed are read from RPS, and do not depend on the online status of those panels; that is, whether they are connected to an IP network or to a power supply, or even exist at all physically.

The panels displayed can be deleted in the following way:

1. Delete a panel configuration first in the RPS View dialog.
2. Close the RPS View dialog.
3. In the AMS dialog **Panel administration**, the panel state is shown as **deleted**
4. In the AMS dialog **Panel administration,** click **Delete selected panels** to delete those panels from AMS which are in state "**deleted**"

Do not integrate panels that contain their own users
To avoid data-synchronization conflicts, do not integrate panels that contain their own users. Create panel users only in AMS. Users created on the panel will be overwritten when AMS updates the RPS database. AMS / panel synchronization is only from AMS to panel, not panel to AMS.

Notes:

- Ensure that the Domain Name Service (DNS) is working properly for all participant Computers and devices.
- Synchronize Date/Time with NTP for AMS Server, the Clients and the RPS Computer
- Enable Mode 2 Protocol for API connections to all panels
- Set the **Automation Password** for all panels in RPS View dialog
- Synchronize Date/Time for all panels (the API cannot connect otherwise)

6.4 Use of the Reload button in Map View

The Map View application provides a **"Reload"** button in the toolbar.
Clicking this button reloads the *entire* data of the Map View application, which may take a long time, depending on the configuration.

We recommend clicking the reload button *only* after configuration changes, for example after adding new devices in the dialog manager, or new maps, because these are not automatically updated in the Map View.
Do not click the button to see device state changes, as these are automatically refreshed by the Map View application.

7 Known bugs and workarounds for AMS 3.0

#269523 MAC offline / down is not visualized in maps and device tree
The online/offline state of a MAC is not available until the MAC has been started.

#210697 Password dialog should be more detailed
The dialog rejects AMS client passwords that are too short, but does not specify the minimum length.
The minimum password length is 6 characters.

#184154 Fingerprint Reader: Wiegand green LED is OFF after red LED is triggered by AMC (for some card types)
After presenting an unauthorized card in Wiegand mode, for the card types MIFARE Classic CSN, iClass, EM, and Prox, the green LED does not illuminate, even if the door is set to office mode by the AMC.

#199503 Instability of the AMS dialog manager when trying to record a fingerprint when the reader has lost its network connection
Workaround: For fingerprint enrolment the enrolment reader must be online.

#202508 While deleting a cardholder assigned to a SimonsVoss lock, the error message has limited information
While deleting a SimonsVoss lock, the error message says only that it is assigned to a SmartIntego whitelist authorization, but not which cardholders are affected.

#195988 Fingerprint reader BioEntryW2: Disable reader beep does not mute the sounder completely
Even if the beep for the reader is disabled in the configuration, the sound generated by the fingerprint reader is still audible when the fingerprint is read successfully.
Remark: The beep cannot be disabled for all reader types, including the BioEntryW2.

#219598 Set/reset command changes the displayed status of a relay, even if the IO extension board hosting it is offline.
Relay status representation in Map View changes even though the extension board is disconnected. The status is corrected as soon as the extension board comes back online.

#224650 Parallel working in device configuration and command operator
Simultaneous attempts to change devices in Map View and the AMS dialog manager can result in a deadlock or error messages.
Workaround: Coordinate device editing work between operators of the two applications.

#240114 Licence manager application
The license manager application is available in English language only. The AMS dialog manager must be run as Administrator in order to use the licence manager.

#268340 AMS30 – Time sync with panel
The time difference between panel and RPS machine must be not too big, otherwise the time cannot be set.
Workaround: set the time on each manually, and activate a time server for RPS server and AMS server.

#265906 AMS30 Setup UI – The Windows OS UI culture info does not always match the current windows display language
On some Windows operating systems the installed language (such as Arabic or Russian) is not idenitified, and the setup dialogs are shown in English.
The setup dialogs are correct if the original language of the operating system was the language selected for the AMS installation.

#266957 AMS30 MapViewer: Removing permission for the alarm event log creates an exception in alarms audit trail
If you remove a permission from an operator who is already logged on to the MAP View, then the operator will not be notified, and they will receive errors if they try to use that permission.
Workaround: If you remove permissions from an operator, ensure that the operator logs in again.

#265836 AMS 3.0 Restoring the backup taken from AMS 2.0 on AMS 3.0 failed
If backups are restored from older versions, the restore can fail because some services are still running.
Workaround:
1. Stop all AMS services manually before restoring, and ensure that no one is connected to the databases.
2. Start the AMS 3.0 setup in repair mode.
3. Restart the AMS server machine.

Note: If the new Bosch Access Importer/Exporter tool is installed, then the restore of backups older than AM3.0 will also fail.
Workaround: Install AMS 3.0 and restore the database before installing the Bosch Access Importer/Exporter tool.

BioEntry W2 Fingerprint Reader in “template on device” configuration
On very rare occasions after prolonged use, the card-reading (not the fingerprint-reading) interface of BioEntry W2 fingerprint readers has been observed to fail in “Finger or Card” mode. The exact causes are still under investigation, but the bug affects only fingerprint readers that are very rarely used as card readers (less than once per week).
Workaround: Power-cycle the reader

Intrusion panels fail to connect after computer restart
Under some rare conditions, after restarting the AMS server, intrusion panels may fail to connect to the AMS system. Their status may be wrong in Map View, and commands cannot be executed.
Workaround:
Restart the Intrusion API service manually.

Avoid unconfigured AMCs on the network
Do not leave AMCs unconfigured in your network, because they can cause communication problems, such as HSC channel messages and unexpected online/offline messages from the configured AMCs.

SimonsVoss

#206393 Sequence monitoring mode 1 does not function correctly when a SimonsVoss lock goes offline
In Access Sequence Monitoring mode 1, monitoring should be deactivated when a lock goes offline. This deactivation is currently not functioning for SimonsVoss Smartintego devices.

#206241 SimonsVoss deletion of a whitelist generates no confirmation
If a whitelist is deleted from a SimonsVoss device, the user receives no confirmation that the command has executed successfully.

#206988 SimonsVoss delete construction WhiteList
If the construction whitelist was used before being integrated into AMS then the MAC is not always able to delete the construction whitelist.
Workaround: Delete the construction whitelist manually.

#235565 SimonsVoss commands are not grayed out depending on specific of SimonsVoss device states
All SimonsVoss commands are available for readers of type SimonsVoss, regardless of whether the command is applicable to the current state of the reader device.