Building Technologies

BOSCH

Access Management System (AMS) version 3.0.1 Release notes

2021-03

This document is intended to familiarize you with your new AMS Version as quickly as possible.

Document history.

Version	Description
1	2021-02 initial version
2	2021-03 Revisions
3	2021-03-31 Release

Table of Contents:

1 Installation Notes 3

1.1 Documentation 3

1.2 Supported operating systems 3

1.3 Cipher suite 3

1.4 Server 3

1.5 Client 4

1.6 Update of AMS 1.0 to AMS 3.0 4

1.7 Update of AMS 2.0 to 3.0.1, or AMS 3.0 to 3.0.1 4

2 New Features in AMS 3.0.1 5

2.1 Visitor Management 5

2.2 Mode override 5

2.3 Access certificate tool 6

2.4 PegaSys 6

3 Mandatory installation steps for Intrusion integration 7

3.1 Supported panels and panel extensions 7

3.2 ACE SDK 7

4 Optional post-installation steps 8

4.1 Security recommendations for user authorizations 8

4.2 Retention Time of System Events 8

4.3 Trace level of services used by Map View.... 8

5 Known limitations in AMS 3.0.1.... 11

5.1 Languages.... 11

5.2 Intrusion.... 11

5.3 Remarks and Limitations on MapView and Services.... 12

5.4 Dialog Manager limitations.... 12

5.5 SQL Server.... 12

5.6 Security issue in Milestone Xprotect.... 13

5.7 Microsoft SQL Express.... 13

6 Additional Notes.... 14

6.1 Tools in Start Menu (Server).... 14

6.2 Web Service.... 14

6.3 Forms Dialog.... 15

6.4 Intrusion integration.... 15

6.5 Reload button in Map View.... 16

7 Known Bugs and Workarounds for AMS 3.0.1.... 17

7.1 AMS Setup and Update.... 17

7.2 AMS General.... 18

7.3 Visitor Management.... 19

7.4 Milestone Plugin.... 20

7.5 BioEntry W2 Fingerprint Reader.... 20

7.6 SimonsVoss.... 20

Aachen
2021-03

1 Installation Notes

1.1 Documentation

Due to the possibility of late changes, the technical documentation for this product in the online catalogue may be more up-to-date than that within the product ZIP files, and should be given preference.

1.2 Supported operating systems

AMS runs on the following operating systems:

	AMS Server	AMS Client
Windows 10, Version 1809 LTSC Windows 10 Professional and Enterprise, Version 20H2	Yes	Yes
Windows Server 2016 (64bit) Standard or Datacenter	Yes	Yes
Latest drivers and OS updates are highly recommended.		

1.3 Cipher suite

This product uses the cipher suite: `TLS_RSA_WITH_AES_256_GCM_SHA384` for certificate-based communication. Ensure that this cipher suite is not disabled on participating computers.

1.4 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

1.5 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 application.

1.6 Update of AMS 1.0 to AMS 3.0

1. Upgrade from 1.0 to 2.0 as described in the AMS 2.0 installation guide.
2. Upgrade 2.0 to 3.0.1, as described below.

1.7 Update of AMS 2.0 to 3.0.1, or AMS 3.0 to 3.0.1

1. Create a backup of the AMS 2.0 or 3.0 installation.
2. Update directly to AMS 3.0.1, as described in its installation guide.

2 New Features in AMS 3.0.1

2.1 Visitor Management

AMS 3.0.1 is the first version to support the Visitor Management tool. The Visitor Management server setup must be executed on the same computer as the AMS server. The AMS license to use the Visitor Management must be activated.

Data changed in Visitor Management are transferred directly to the access control system. Data changed on the access control system are synchronized every 5-10 minutes with the Visitor Management system.

The backup and restore of the AMS system includes the Visitor Management data.

2.2 Mode override

"Mode override" enables a Map View user to **temporarily override** those mode settings of doors and readers that are configured in the device editor. The temporary settings stay in effect until the Map View user sends the „Disable Permanent Open" or "Unblock door" command. At this point the mode settings made in the device editor, such as time models, are restored to the devices.

Any changes that an operator makes in the device editor while the mode override is in operation are buffered, and come into effect when the „Disable Permanent Open" or "Unblock door" command arrives.

Note:
While mode override is in operation there is currently no visual indication of this in Map View or in the device editor. This will be rectified in the next version

Example:
A door is configured by time model to be unlocked workdays from 8.00 to 12.00.
On one workday a Map View operator sends a "set door permanently open" command to the door at 6:00.
Through "mode override" the door is unlocked immediately and remains unlocked until the operator sends a „Disable Permanent Open" or "Unblock door" command. Then the door reverts back to the device-editor configuration, where it was governed by time model. If the command arrives between 8.00 and 12.00 on a workday, the door remains unlocked as per the time model. Otherwise it is immediately locked. Prior to version 3.0.1 a command sent from Map View would replace the device-editor configuration completely.

2.3 Access certificate tool

`AccessCertificateTool.exe` is now part of AMS. It allows you to update and replace certificates. The Output folder should always be the Certificates folder below the installation folder, e.g. `Access Management System > Certificates`

2.4 PegaSys

PegaSys is now supported for the following card types:

- MIFARE DESFire
- LEGIC advant

3 Mandatory installation steps for Intrusion integration

The integration of B/G intrusion panels in AMS requires the installation of the intrusion RPS API version V2.1.25920 or later.
The RPS API must be installed on the same computer as the RPS tool. The RPS tool is needed to configure and manage the communication with the B/G panels.
The RPS API conveys communications from AMS to the RPS tool, which then communicates with the panels.
SDK communication to the B/G panels is integrated in AMS. No separate installation is required, but **Mode2** and a **AutomationPasscode** must be enabled on the panel.

For small installations it is possible to install AMS and RPS on the same computer, with the following prerequisites:

- AMS has never been installed on that computer
- SQL Server database has never been installed on that computer
- You install RPS before AMS

3.1 Supported panels and panel extensions

The following B/G intrusion detection panels are supported by AMS 3.0.1:

- B3512
- B4512
- B5512
- B8512G
- B9512G
- B6512
- B901 Access Control Module (door state only and cardholder management possible)

3.2 ACE SDK

Applications using API from AMS V3.0.1 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.`

4 Optional post-installation steps

4.1 Security recommendations for user authorizations

On the AMS server define only Windows users who are intended to change the AMS setup (files, certificates, registry and licenses), and give them Windows Administrator rights.
Explanation: The file structure containing the certificates and configuration files should only be accessible to Windows Administrator and System users.

4.2 Retention Time of System Events

The retention time for system events is configurable. The default is set to 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.

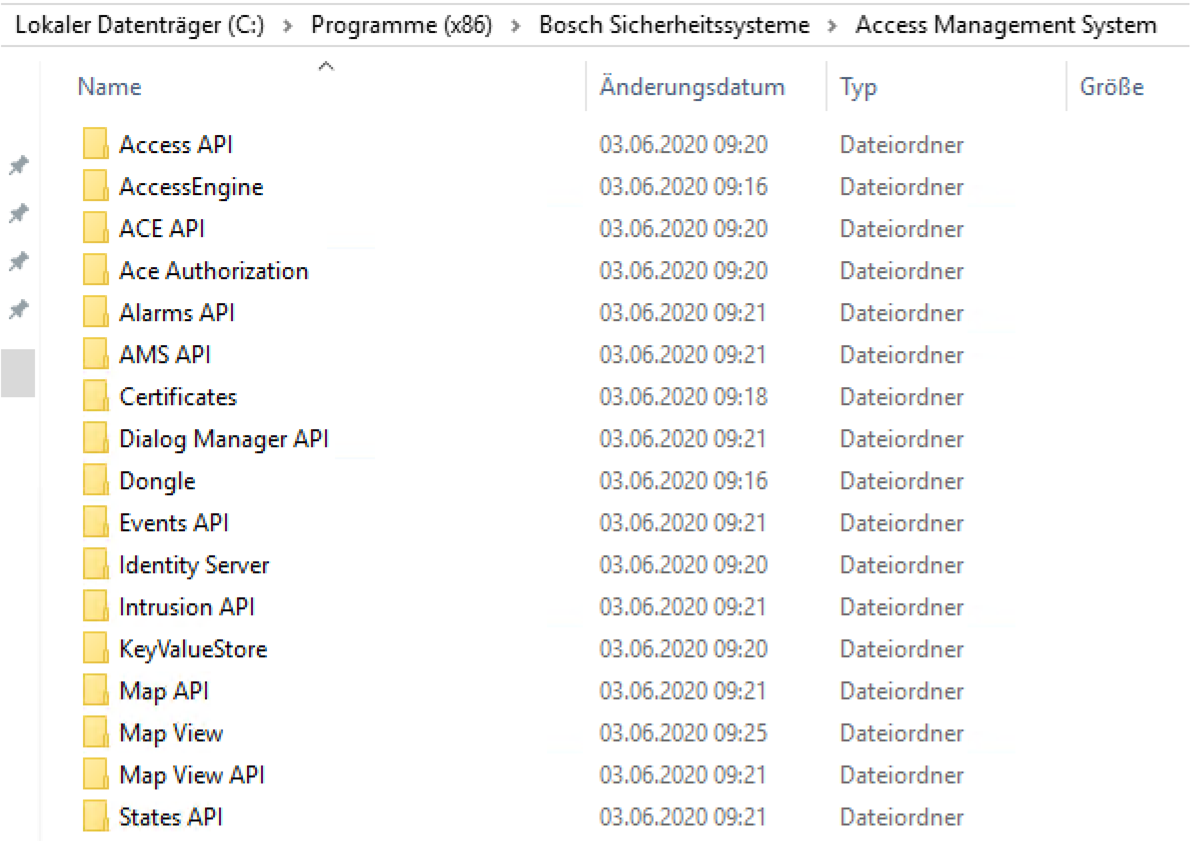
Note that the retention time has a major impact on the size of the backup files being created. So please choose a value that is as low as possible.

4.3 Trace level of services used by Map View

The services used by the Map Viewer Application use a logging interface that is independent from the logging 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 a user with Administrator rights.

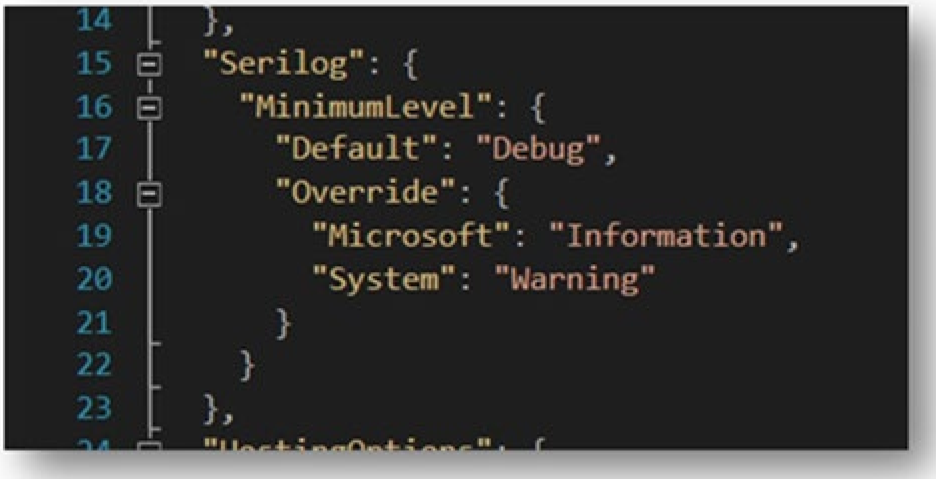
- Bosch Access API
- Bosch ACE API
- Bosch ACE Authorization
- Bosch AMS API
- Bosch Dialogmanager API
- Bosch States API
- Bosch Alarms API
- Bosch KeyValueStore
- Bosch Intrusion API
- Bosch Events API
- Bosch Map API
- Bosch MapView API
- Bosch ACE Identity Server



Lokaler Datenträger (C:) › Programme (x86) › Bosch Sicherheitssysteme › Access Management System

Name	Änderungsdatum	Typ	Größe
Access API	03.06.2020 09:20	Dateiordner	
AccessEngine	03.06.2020 09:16	Dateiordner	
ACE API	03.06.2020 09:20	Dateiordner	
Ace Authorization	03.06.2020 09:20	Dateiordner	
Alarms API	03.06.2020 09:21	Dateiordner	
AMS API	03.06.2020 09:21	Dateiordner	
Certificates	03.06.2020 09:18	Dateiordner	
Dialog Manager API	03.06.2020 09:21	Dateiordner	
Dongle	03.06.2020 09:16	Dateiordner	
Events API	03.06.2020 09:21	Dateiordner	
Identity Server	03.06.2020 09:20	Dateiordner	
Intrusion API	03.06.2020 09:21	Dateiordner	
KeyValueStore	03.06.2020 09:20	Dateiordner	
Map API	03.06.2020 09:21	Dateiordner	
Map View	03.06.2020 09:25	Dateiordner	
Map View API	03.06.2020 09:21	Dateiordner	
States API	03.06.2020 09:21	Dateiordner	

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



```
  },
  "Serilog": {
    "MinimumLevel": {
      "Default": "Debug",
      "Override": {
        "Microsoft": "Information",
        "System": "Warning"
      }
    }
  },
```

Default logging configuration:

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

Explanation: We are using Serilog for our logging. It defines the following levels: *Verbose, Debug, Information, Warning, Error and Fatal*.
The "MinimumLevel" settings ("Warning" in the screenshot) applies to all log sources (i.e. which component that is writing 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 will most likely result in almost no log entries, except for the last error that crashed the runtime. There is no function in the API to completely disable logging.

5 Known limitations in AMS 3.0.1

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

Language of AMS installation has to be the same as the one of the Operating System. The only exception is Turkish. There the OS has to be in English. Please note that also Client and Server Installations should have the same language as 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 current UI culture of the OS. For example. if the UI culture of the OS is Portuguese Brazil (pt-BR), the AMS Setup UI will be also in Portuguese Brazil. 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 Intrusion

5.2.1 Intrusion event limitation:

Receiving of events and alarms depends on the network and system availability.
Events and alarms are not repeated, if the AMS system has not received them.

5.2.2 Intrusion cardholder synchronization limitation:

In combination with intrusion, we only support default card definitions

- HID 37 BIT -> Intrusion 37 BIT with a Facility/Site code not larger than 32767.
- HID 26 BIT- > Intrusion 26 BIT
- EM 26 BIT- > Intrusion 26 BIT

5.3 Remarks and Limitations on MapView and Services

5.3.1 Initial States

Please note that the states initially displayed by the system immediately 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. Only after a MAC-switch are the correct master and slave symbols displayed.
One workaround, to refresh the states, is to coldstart the system (DMS, MAC, AMCs, Readers etc..) and so force a MAC-switch.

5.4 Dialog Manager limitations

5.4.1 Signature Pad

Make sure that the latest signature pad firmware is installed on the corresponding client machine. The firmware installation file is located within the delivered AddOns folder (Firmware File: signotec:TWAIN_8.0.0.exe). The latest driver can be downloaded from https://www.signotex.com/download/treiber/twain-wia-treiber/

5.4.2 Guard tour and SimonsVoss readers

Readers from SimonsVoss are not supported for guard tours.

5.4.3 Access IPconfig Tool

The fingerprint reader scan may not work when multiple network cards are used on the computer.

5.5 SQL Server

The SQL Server has to be run on the same machines as the AMS server. It is not possible to have an SQL Server on a machine other than the AMS Server.
.

5.6 Security issue in Milestone Xprotect

There is a bug in Milestone XProtect 2019 R2 Corporate edition which causes the certificate validation to fail, so leaving network communication unsecured.

The AMS – XProtect plugin communicates with AMS services using HTTPS. If the XProtect server and AMS server are on a separate computer, AMS certificate has to be imported on the XProtect server to establish trust with the AMS server for HTTPS communication. Due to a bug in XProtect, the trust validation is turned off, allowing HTTPS communication without installing the certificate. This bug has been confirmed in:

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

Other variants e.g. Expert 2019 R2, Professional 2019 R2, Express+ 2019 R2 and Express 2019 R2 might also be affected.
This bug is not present in:

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

We recommend XProtect Corporate 2020 R1.

5.7 Microsoft SQL Express

Microsoft SQL Express limitation:
Please note that the SQL Express DB installed with AMS 3.0.1 supports up to 1 million events.
The default retention time is 90 days.
Old events are deleted if:

- the DB usage 85 % of it max capacity (max file size 10 GB for SQL Express 2017), or
- the retention period has expired

In case more access events are expected then please consider using a Full Version of Microsoft SQL.

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

Tool to scan the network for IP based AC devices. The tool provides online help.

6.1.2 Configuration Collector

The *Configuration Collector* is a tool which is installed on the AMS server. It guides you through collecting configuration information which is being stored into a ZIP file. This ZIP file can then be sent to Bosch Technical Support for troubleshooting.
The Configuration Collector provides an online help which can be invoked from any of its tab pages.

6.1.3 DB Password Change

This tool can be used to change the password for the internal database account. SA privileges are required.

6.1.4 Backup

Used to trigger a database backup. Described in detail in the operation manual.

6.1.5 Restore

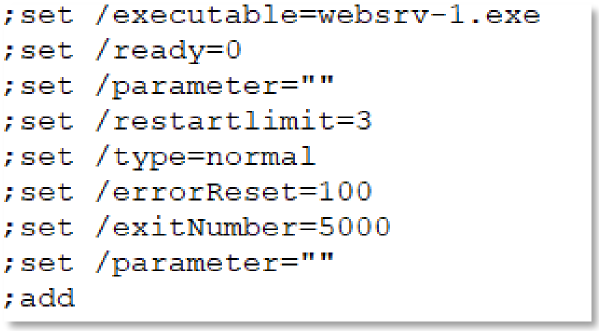
Used to start a database restore. Described in detail in the operation manual.

6.2 Web Service

The Access Management System optionally provides a Web Service which can be used to retrieve specific data over http.
Please note, that HTTP is a non-secure interface.
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 you have done the changes, 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 Forms Dialog

The AMS Client provides a dialog to edit templates for printable forms e.g. an acknowledgement form.
The dialog can be found in the menu **Configuration > Settings,** dialog item **Forms**.
This dialog can be used to import and export custom HTML forms. The AMS has two forms pre-installed which can be exported and customized.

6.4 Intrusion integration

Best practice:
While the RPS Tool is actively communicating with an Intrusion panel, the AMS system cannot propagate data down to that panel via the RPS API. The changes will be propagated after the communication channel has become clear.

Recommendation: After synchronization between RPS Tool and intrusion panel, they should be disconnected; do not leave the connection open.

AMS Dialog “Panel administration” displays panels. These panels are displayed as soon as an RPS panel configuration is created. This is irrespective of whether the panels are online or not.

To delete a panel from AMS do the following:

1. Delete the panel configuration with RPS Tool
   AMS dialog “Panel administration”, the panel state now shows “deleted”
2. AMS dialog “Panel administration”, any panel that is in state “deleted” can now be deleted from AMS by selecting “Delete selected panels”

Disarming an intrusion area on keypad via card is not possible for areas that are in the background.
In case “Arm” and “Disarm” via card should be presented on keypad, ensure that the area, which to be Armed and Disarmed is configured in the RPS Tool: **KEYPADS** > **Keypad Assignments** > **Area Assignment**

Recommendation: Present Arming and Disarming only by using a card from an intrusion user who is assigned to Area 1 (the default area, which is per default in foreground)

Do not create users by using the RPS Tool, only in AMS.
Explanation: If a user is already configured in the B/G panel with the same passcode as a new user created by AMS, a synchronization conflict will occur. The user that was created on the panel then cannot be deleted.

Note: for the command & control of intrusion devices in AMS Map View, the clocks of the intrusion panel and the AMS computer must be within 100 days of each other.

6.5 Reload button in Map View

The Map View application provides a “Reload” button in the toolbar.
After clicking that button the *entire* data of the Map View application will be reloaded.
Depending on the configuration, this will take several seconds or up to minutes.

Recommendation: Use this button only after making configuration changes (e.g. adding new devices or maps) as these are not automatically updated in the Map View.
Do not use it to view the latest state changes, as these are automatically processed by the Map View application.

7 Known Bugs and Workarounds for AMS 3.0.1

7.1 AMS Setup and Update

#329012 AMS setup does not work if 8.3 filenames are disabled

Despite an apparently successful setup, AMS 3.0.1 Map View does not operate correctly if filename format 8.3 is disabled in Windows.

Workaround:

Before installing AMS 3.0.1 ensure that 8.3-format filenames are enabled. Start the command shell as Administrator, and run the command:

```
fsutil 8dot3name query
```

The result should be: 0

If not, execute the command

```
fsutil behavior set disable8dot3 0
```

#240114 License manager application English only, requires Administrator rights

Application is available in English language only. The Dialog Manager must be started as Administrator to be able to use the license manager.

#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 language used (like Arabic or Russian) is not recognized, and the setup dialogs are shown in English. The setup dialogs are correct if the initial language of the operating system matches the selected setup language.

#287009 AMS 3.0 restriction on server names

If the AMS is installed on a computer whose name contains the string “APP”, the login will fail after installation.

Workaround: Do not use the string “APP” within the names of AMS servers.

#246461 Card Types are not correctly activated after update

In some configurations where multiple card types are used and the access system is updated, then the configuration is corrupted, and in the worst case no one can enter anymore.

Workaround: After the access system update, make a note of all existing card type definitions. Remove all the card type definitions, and save the changes. Assign the same card types again and save your selection.

#324081 BadgeDesigner – Only common division available

After an upgrade from an AMS where multiple divisions had been assigned to an operator: If you start the BadgeDesigner before the access dialog manager then sometimes only the “common” division is available to the BadgeDesigner menus.

Workaround: Restart the dialog manager and log in before running the BadgeDesigner.

#326143 Certificate setup failed due to repair setup
The certificate part of the repair setup does not work as intended if the certificate tool was run beforehand.
Workaround: Start `certlm.msc` and delete the following certificate **before** running or repeating the repair setup:
Personal certificates > friendly name **Access Management System RabbitMQ Server**.

7.2 AMS General

#280440 AMC4W cannot detect the state open on an input
Sometimes the configuration of an input contact in the device editor is not propagated to an AMC 4W controller.
Workaround: Reset the controller.

#269523 MAC offline / down status is not visualized in maps and device tree
Workaround: Restart the MAC service.

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

#268340 AMS30 – Time sync with panel seems not to be working
A large time difference between a panel and the RPS machine prevents the time from being set.
Workaround: Start by setting the correct time manually, and activate a time server for RPS server and AMS server.

#266957 AMS30 Map View: Permission off for alarm event log creates exception in alarms audit trail
If you remove permissions from an operator the back end system reacts faster than the UI. For example, if Operator 1 is already using the Map View, and Operator 2 removes his permissions in the dialog manager, then Operator 1 may start getting error messages in Map View, because the back end checks the permission for *every* command.
Workaround: If you want to remove permissions from an operator, make sure that he logs off first.

# 270449 AMS3.0 Temporary cards will not be assigned to intrusion panel
Temporary cards are not automatically sent to the intrusion panels. The old card is deleted from the panel.

Workaround: Assign the temporary card manually to the intrusion user in AMS tab **Intrusion**

#268298 AMS 3.0 – Up and down buttons poled incorrectly

In the dialog "**Administration of alarm panels**" the up and down buttons for the port numbers work in the wrong directions.
Workaround: Enter the port number from your keyboard.

#281358 CFS – AMS threat level text incorrect

On deactivation of a threat level the MapView application shows a message without a threat level name. In all threat level activation messages the threat level name is shown.

#272849 AMS 3.0 Map View area counter for parking places

The MapView application for the overall parking area always shows 0 (zero). In the sub parking areas the real count of cars is shown.
Workaround: This is as designed, the value 0 can be ignored.

#268652 AMS 3.0: System asks you to remove division from pushbutton

If in the device configuration dialog a non- "common" division is assigned to an entrance, this misleading message box will be shown upon saving.
Workaround: Ignore the message, change all sub devices of the entrance to the same division and save.

#248582 CFS – Random screening abnormal

The random screening timeout below 10 minutes is configurable but does not work.
Workaround: Use only realistic values of 10 minutes and above.

7.3 Visitor Management

#327038 Visitor Management – Same visitor not editable in AMS

If visitors are created with same last name, first name and birthday, then the **Visitor** dialog in AMS will show the error message that the visitor already exists.
Workaround: Disable the unique key check in the registry key

```
\HKLM\SOFTWARE\WOW6432Node\Micos\SPS\DEFAULT\PersData\PkUnique
```

Set @value to 00

#282466 Visitor Management – Card reader not working if used by AMS and VM

If a LECTUS enroll 5000 MD reader is in use by the AMS Dialog Manager it cannot be used by Visitor Management simultaneously.
Workaround: Stop the Dialog Manager before using enrolment in Visitor Management, or use a different type of enrollment reader in the Dialog Manager.

7.4 Milestone Plugin

#316324 & 281130 CFS – Milestone plugin problem
If the XProtect plugin of AMS is used in parallel with plugins of other distributors, the initialization of the AMS plugin can fail.
If AMS DIP DOPs are used in Milestone the debug log file of Milestone grows dramatically, and this will decrease the overall system performance.

7.5 BioEntry W2 Fingerprint Reader

#199503 Instability of the AMS dialog manager when trying to record a fingerprint when the reader has lost its network connection
For fingerprint enrolment the enrolment reader must be online.
#184154 Fingerprint Reader: Wiegand green LED is OFF after red LED is triggered by AMC (for some card types)
In Wiegand mode for the card types MIFARE Classic CSN, iClass, EM, Prox: If an unauthorized card is used, the green LED is not shown, even if set permanent open by the controller.

#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.

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.
Workaround: Power-cycle the reader

7.6 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 in the case of SimonsVoss Smartintego devices.

#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.

#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 may not be not able to delete the construction whitelist.
Workaround: Delete the construction whitelist manually.

#235565 SimonsVoss commands are not grayed out, depending on specific SimonsVoss device states
All SimonsVoss commands are available if it is an SimonsVoss reader type.