Access Management System (AMS) version 5.0.1 Release Notes

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

Document history.

Version	Description
1	2023-02 Release of Access Management System 5.0.1

Table of Contents

1 Installation Notes

1.1 Documentation

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

1.2 Server requirements

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

Supported operating systems (standalone orclient/server mode). Installations of AMS on other operating systems may succeed, but are entirely withoutwarranty.	– Windows Server 2016, Windows Server2019 (64 bit, Standard, Datacenter) – Windows 10 Version 1809 LTSC, Windows 10 Professional and Enterprise, Version 21H1 (Note: in a domain environment, the server operating system is recomended) – Ensure that the latest software updates are installed. – Note: The default database delivered with this system is SQL Server 2019 Express edition with advanced services

Minimum hardware requirements	– Intel i7 processor generation 8
	– 16 GB RAM (32 GB recommended)
	– 250 GB of free hard disk space
	– 300 MB/s hard disk transfer rate
	– 10 ms or less average hard disk response time
	– 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

MAC server	
Supported operating systems. Installations on other operating systems may succeed, but are entirely without warranty.	– Windows Server 2016, Windows Server 2019 (64 bit, Standard, Datacenter) – Windows 10 Version 1809 LTSC, Windows 10 Professional and Enterprise, Version 21H1 – Ensure that the latest software updates are installed.

1.3 Client requirements

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

Supported operating systems (standalone or client/server mode). Installations of BIS on other operating systems may succeed, but are entirely withoutwarranty.	– Windows 10 Version 1809 LTSC, Windows 10 Professional and Enterprise, Version 21H1 – Ensure that the latest software updates are installed. **Note:** with a Pro edition, updates must be deferred until 8 months afterthe release of the AMS version. For further information see the Microsofttechnet page at https://technet.microsoft.com/en-us/itpro/windows/manage/introduction-to-windows-10-servicing
Other Software	– ASP.NET – .NET: On Windows 10, Windows Server 2016 and Windows Server 2019: .NET 3.51, .NET 4.8, .NET 5.0 and Core 3.1.7
Minimum hardware requirements	– Intel i5 (Gen 6 / Skylake or newer) or higher, multiple cores – 8 GB RAM (16 GB recommended) – 25 GB free hard disk space – Graphics adapter with – 256 MB RAM – a resolution of 1280x10240 – at least 32 k colors – OpenGL® 2.1 and DirectX® 11 – WebGL2-compatible (for example, Intel UHD Graphics 600 class or comparable), non-virtualized – 1 Gbit/s Ethernet card – Free USB port for Dialog Reader or camera – Recommended: Wide-screen monitor for Map application.

Web Browser	Version
Google Chrome	90 or higher
Microsoft Edge	90 or higher
Mozilla Firefox	88 or higher

1.4 Databases: support for MSQL 2019

For new installations of AMS 5.0 SQL Server 2019 Express edition will be installed if you are not using your own purchased version.
On update from AMS 3.0.1 the SQL Server 2017 is updated to SQL Server 2019.

Database backups are then found in `..\MSSQL14.ACE` instead of `..\MSSQL15.ACE`

1.5 Update of AMS 1.0 to AMS 5.0.1

1. Upgrade from 1.0 to 2.0 as described in the AMS 2.0 installation guide.
2. Upgrade 2.0 to 5.0.1 as described below.

1.6 Update of AMS 2.0/3.0/3.0.1/4.0/4.0.1/5.0 to AMS 5.0.1

1. Create a backup of the old AMS installation.
2. Update directly to AMS 5.0.1, as described in its installation guide.

Before putting AMCs online after an update, ensure the AMC is physically connected to the network and that the device communication password (DCP) has been set.
The automatic provisioning phase of firmware to the AMCs lasts 15 minutes from the time of saving the changes made in the device editor. AMCs that are not reachable within these 15 minutes will not be receive the firmware update.

To restart the provisioning phase,

1. Clear the **Enable** check box and save the configuration, then
2. Select the **Enable** check box and save again.

Alternatively the provisioning phase can be activated using the AMCs context menu:
For AMS: Command in the MAP View: **Send TLS key**
Follow this procedure also whenever you have cleared the DCP using the AMCIPConfig tool or cleared the key via AMC's LCD display button.

1.7 Languages

Supported languages in AMS 5.0.1:

- AR-EG
- EN-US
- ES-AR
- DE-DE
- FR-FR
- HU-HU
- NL-NL
- PL-PL
- PT-BR
- RO-RO
- RU-RU
- TR-TR

- ZH-CN,
- ZH-TW

1.7.1 Locale setting required for non-English installations

For non-English characters, such as Arabic, Russian and diacritic Latin characters, AMS requires the Windows system locale to be set to the chosen language. Otherwise AMS reports and some dialog controls will show placeholder characters instead.
This is important if the operating system is using a multi-language pack. Installing a language pack does not update the System Locale, so it must be set manually.

For example, in the case of Arabic:

- **Regional Settings** > **Administration** > **Language for non-Unicode programs** > **Change system locale** and select an Arabic locale
- 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)`'.

1.7.2 AMS Setup languages and Operating Systems

The language of the AMS Setup UI uses 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 exactly, then the AMS Setup UI will be in English (en-US).

1.8 Compatibility List of Software Components for AMS 5.0.1

Component	Version	Location
Importer/Exporter	1.1.18	AMS Media Package Folder: AddOns/Standard/ImportExport
Occupancy Monitor	1.1.13	AMS Media Package Folder: AddOns/Advanced/OccupancyMonitor
AECT Tool	1.0.0.7	AMS Media Package Folder: AddOns/Advanced/AECT
Bio IP Config Tool	5.0.1	AMS Media Package Folder: AddOns/Advanced/BioConfig
IPConfig (AMC)	1.12	AMS Media Package Folder: AddOns/Standard/AccessIpConfig
SDK Version	5.0/5.0.1	AMS Media Package Folder: AddOns/Advanced/API
MAC Installer	5.0.1	AMS Media Package Folder: AddOns/Advanced/MultiMAC
Key Management Tool	2.4.9	AMS Media Package Folder: AddOns/Advanced/ReaderConfigTool
Inrusion RPS API	2.2.27914	AMS Media Package Folder: AddOns/Advanced/Intrusion-RPS-API
Milestone PlugIn	5.0	AMS Setup Folder: <Language>\ServerPlugin
BVMS Version	11.1.1	Download Store /Product Catalogue
VisitorManagement	5.0.1	Download Store /Product Catalogue
CredentialManagement	5.0	Download Store /Product Catalogue
MobileAccess	5.0	Download Store /Product Catalogue
Milestone Xprotect	2020 R3	Download Store Milestone

2 New Features in AMS 5.0

2.1 Extended Integration of OSS-SO offline locking systems

AMS 5.0 is the second version to support the OSS-SO integration. New enhancements in AMS 5.0:

- Support up to 50 updaters (Tested successfully with 60 updaters)
- The import of 2000 locks, 1000 groups and 50 groups per lock needs about 2 minutes
- Search and filter improved in OSS-SO Configurator dialogs
- Performance increased of reading and updating information on OSS-SO cards
- Multi vendor support:
  - OSS-SO vendor identification can be configured to by used in xml export file
  - XML Export and OSS-SO card permissions tested with Uhlmann&Zacher and Allegion (Normbau)
- Integrated MIFARE Desfire function for coding cards without OSS-SO files
  Bosch coded cards without OSS-SO files can be used now. The missing OSS-SO files are created automatic including file for battery events. This lead to a longer write time the first time (some additional seconds).
- Online status of updater connection in overview of OSO Configurator tool has been improved
- Battery status of OSS-SO locks is shown in the OSO Configurator tool including printer output
- New OSS-SO Authorization Report in the OSO Configurator tool:
  Cardholders with their assigned OSS-SO lock permissions are shown and can be printed

2.2 Remote SQL Server Support

Support of a remote SQL Server 2019 on a separate server for AMS.
This computer will host databases from multiple AMS applications and should be secured against unauthorized access. The AMS backup is split in this case. The backup information file is found on the AMS server and the backup data itself is found on the remote server where the SQL Server resides. For an AMS restore you need the backup information file from the AMS server and the database backup files from the remote SQL server.

2.3 Support for Visitor Management 5.0

Support of the new release of Visitor Management.

- E-Mail integration
- Informing the host by mail when their visitor checks in.

- Visitor can select a host during self-registration
- Receptionist can print a "visitor pass" for the visitor.
- Application can be customized with the logo of the operating company
- Excel and CSV exports of filtered data from the dashboard
- Bulk operations on many data records simultaneously.
- Printing of visitor cards, for example with the Evolis “Tattoo Rewrite” card printer.
- Support of iClass enrollment readers such as the HID OMNIKEY
- Update of the SDK for ARH passport scanners

2.4 Improved UX

Improvements for User Experience in configuration and setup.
Some details:

- The first setup page shows a QR code link to YouTube videos for installation and configuration.
- Edit controls in the Dialog Manager use different background colors for selected (blue) or required (yellow).
- Readers provided in Bosch catalog are displayed with photo and CTN number in the device configurator. The CTN number of BOSCH dialog station readers is shown in the first column.
- Setup checks the SQL Server password strength, peventing the SQL Server installation from failing.

2.5 Access Control API

AMS 5.0 introduces REST and gRPC network interfaces to support a range of integration scenarios, such as:

- Creating, reading, updating, and deleting employee-related information
- Creating, reading, updating, and deleting access cards
- Associating and deassociating access cards for employees
- Associating and deassociating access authorizations for employees
- Reading basic device information, available commands, etc.
- Reading both historical and live-streaming events from the access control system
- Sending commands to access-control devices

These APIs present an alternative to the existing binary SDK and enable integrators to embed AMS in advanced workflows that may span multiple systems, for example, automatic synchronization of employees and access authorizations, command and control through third-party software.

2.6 New Sentinel License System

The SLMS license system has been replaced with the Sentinel license system. CTN numbers are no longer shown in the license dialog. When a license is active, only the features that it licenses are displayed. The installation manual has been updated accordingly.

Limitation:
The license menu does not show the expiration date-time for limited licenses (e.g. emergency and sales demo licenses). These license will expire without prior warning.
After a Base edition license (PRO, PLUS, or LITE) is assigned to a computer (via its *System Fingerprint*) it is not possible to switch to a different base license. The only exception is the emergency license.
It is not possible to mix license extensions between editions (PRO, PLUS, or LITE).

To remove the emergency license from the computer, delete the file `lservrc` from the folder "<installation folder>`\Bosch Sicherheitssysteme\Access Management System\License API`" and restart the computer. After this, other license files can be imported.

2.7 Romanian Language support

The Romanian language is now supported in the user interface of the AMS 5.0

2.8 Swipe Ticker for B901 Modules in MAP View

Swipe Ticker now also displays door events related to B901 Modules from B/G Intrusion panels.

Limitations:
For this feature to work fully, the door numbers need to be associated with the corresponding point numbers in RPS configuration i.e.: Door1 associated with Point1.
The B901 modules do not provide information regarding the actual opening of the door strike, so all we can only determine whether the door was unlocked or not.

2.9 Buzzer Alarm for Door forced open and Door held open

For the following door states, the ACS provides a means of sounding the alarms in all the readers connected to the door.

For state **Door forced open**
Local alarm response: The alarm sounds for 17 seconds or until the door closes.

For state **Door held open**:
Local alarm response: The alarm sounds until the door closes.

Prerequisites
– The readers use either OSDP or Wiegand protocol
– Alarm sounders are present in the readers, and for Wiegand, electrically connected to the door controller.
– AMC firmware version 02.38 or later, as delivered with AMS 5.0.

The following reader types are not supported:
– IDEMIA readers
– Suprema readers with Wiegand protocol

2.10 Customizable Time and Attendance reports

Card usage at entry- and exit-readers is recorded by the system, and reports can be exported to customizable CSV-files.

2.11 New Features in AMS 5.0.1

AMS 5.0.1 supports Visitor- and Credential-Management with Mobile Access. New licenses have been added for Credential Management 5.0 and Mobile Access 5.0

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 5.0:

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

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.

5 Resolved issues in AMS 5.0/5.0.1

5.1 Resolved issues in AMS 5.0

#249850: **Fingerprint W2 reader firmware stops reading cards if the reader is not used for long periods (>= 2 weeks).**
Only affects some card types in special configurations.
Provided firmware "`bew2-oap_v1_1_5_bosch_20210419_170700_sign.bin`" must be updated manually to avoid this error. It is located in the same folder as the BioIPConfig tool in the installation media.

For MAC and AMC fixed in AMS 5.0:

#383433: CFS: Office Mode no longer blocks the activating card
#375654: Logfile sizes have been increased for `DMSTELE.log GatewayCommand.log` and `GatewayData.log`
#373409: BIS ACE 4.9.1 AMC IP Config logfiles are are now filled correctly
#370407: CFS: Access no longer delayed after reading card in rare circumstances.
#360073: Device editor no longer shows "The device is not in configuration mode" without good reason.
#358993: MAC Info logs are now correctly recycled

For the data management service fixed in AMS 5.0:
#210697 Password dialog has improved
#266957 AMS Map View: Users are now informed if their permissions have been withdrawn. Exceptions are no longer generated.
#281358 CFS – New AMS threat-level message: “Threat level at MAC <name> was deactivated by operator”.
#339756 Reader input/output signals for **LECTUS select** (LCTSL) are no longer editable. (Entrance node > **Terminals** tab).
#328222 The swapping of IP-Adresses between AMCs no longer causes the MAC synchronization to fail.

5.2 Resolved issues in AMS 5.0.1

#395922 CFS: BVMS & Milestone integration can now send door commands to AMS
#392315 CFS: Occupancy Monitor now shows the area counters in all supported languages
#396041 CFS: Device editor now allows the changing of reader types for door model 01b
#405744 Certificate tool now generates Google-Chrome-compatible certificates.

If you need to create a new root certificate to enable Chrome support, this must be done before installing Mobile Access. It will not be done automatically during update. Use the following procedure:

1. Open the computer certificate store: Press the Windows key + R to bring up the Run command, type `certlm.msc` and press Enter.
2. Delete the AMS root certificate from the certificate store as follows:
   Go to Tusted Root Certificate Authorizations
   Select Bosch Security System Internal CA-BISAMS and delete this certificate
3. Delete the AMS certificate from certificate store:
   Go to Personal
   Select Bosch Security System Internal CA-BISAMS and delete this certificate
4. Run certificate tool located in INSTALLFOLDER/Bosch Sicherheitssysteme/Access Management System/Certificates/BoschCertificateTool.exe
5. Install the new certificate on all clients as described in AMS installation manual

#405522 CFS: LDAP support in the ImportExport tool now works correctly.
#400061 CFS: The IO-functions can be configured in the Device Editor in all supported languages.
#371946 CFS: Added support for the older PegaSys time-model cards, used in MIFARE systems. If the registry value
`PegaSys >MFOldTimeInitCard >@value` is set to `1` (=true)
then the old format of time model cards is written. The complete path is:
`[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Micos\SPS\DEFAULT\PegaSys\MFOldTimeInitCard]`

5.3 Resolved issues in Visitor Management 5.0.1

Updated API calls to Mobile Access
Mobile Access requires the updated Visitor Management Version 5.0.1.

Some URLs in the Mobile Access backend's REST-API have been harmonized with other Bosch APIs.

6 Recommended practices

6.1 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.

6.2 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 application.
Do not use it to view the latest state changes, as these are automatically updated by the Map View application.

6.3 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.signotec.com/service/downloads/treiber/ (German) or https://en.signotec.com/service/downloads/drivers/ → TWAIN and WIA Driver

6.4 Milestone Xprotect

Supported XProtect versions: Corporate 2020 R1 and higher.

7 Known limitations and workarounds

7.1 AMS Setup and Update

#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.

#357322 MAC setup is available in English only (English is the default).

#409697: AMS 5.0.1 update from AMS 5.0 authorization profiles assigned to Persclass (person class) is no longer working for default person classes, including visitors and external employees.
Workaround: In the Person Classes dialog, reassign the authorization profiles to those classes.

#410291: Licenses no longer work after running a repair setup, if you use Windows **Apps & features**.
Workaround: Do not use the **Modify** button in Windows **Apps & features**.
Always run the AMS server's `Installer.exe` to repair the system.

7.2 AMS General

7.2.1 AMS 5.0

#240264
For AMCs input/output signals only conditions of type "state" can be used for the FOLLOW_STATE function.
The following conditions are of type "event", and cannot be used with the FOLLOW_STATE function.

```
11 - Door n forced open alarm
12 - Door n left open
13 - Reader shows access granted
14 - Reader shows access denied
23 – Messages to readers
```

```
24 – Messages to devices
25 - remote control Function set
```

#248582: CFS – Random screening
The random screening timeout below 10 minutes is configurable but does not work.
Workaround: Use only realistic values of 10 minutes and above.

#268652: AMS 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.

#342685:Microsoft print to PDF and Microsoft XPS document writer
Microsoft PDF print does not work from .NET dialogs on any operating system.
Workaround: use other PDF printer drivers, such as doPDF.

#323446: Readers of type LECTUS select or LECTUS duo appear online but do not react to AMC communication
Disabling the secure OSDP channel checkbox in the device editor does not disable the secure channel on the reader; it will only cause the access control system to use unencrypted communication. The reader can still be polled and appears to be online, but it continues to reject any unencrypted communication.
Workaround: Either re-enable secure communication or reset the reader hardware to its factory default state, which allows unencrypted communication. To reset the reader please refer to the reader manual and reset the OSDP secure channel using the reader’s DIP-Switches.

#371589: Gateway - Exception message instead of log message is delivered when a configured AMC is disconnected
#363278: ACE 4.9.1: AMCIPConfig help is not up-to-date
#371585 AMC – Offline/online messages fill up the AMC’s flashCard if (e.g.) the DTLS password is incorrect.
#375360: CFS – The new AMCIPConfig software may display the message Invalid IPEndPoint type if old AMC firmware is used in a network without DHCP server.
#340759: AMC - IO Function fails to react to the To Inspect event.

#356203: IPConfig does not always the show the current firmware version when attempting a bulk firmware update
#349902: AMCIPConfig no longer allows access with the correct password after running for several hours.
Workaround: Always close the tool after use.

#240264 AMC IO events 13 (Reader access granted) and 14 (reader access denied) are not always processed if the events follow each other within 2 seconds.
#323446: An OSDP reader may continue to appear online after the installer has switched it from secure to unsecure, and not yet reset the reader.
#244001: Map View - Areas: All non-parking areas fail to show the states FULL/EMPTY
#357428 The validity period of the cardholder is not updated in all cases
The card-validity period of a person is assigned when the person first receives an access profile. Subsequently changing a person's profile does not extend the person's original card-validity period.
Workaround: Assign the intended validity period manually for the person that you have modified.
#380155 client setup does not perform a reboot in all cases
In some situations the setup will not force a reboot.
Workaround: Restart the computer after client setup.
#389164 Server setup does not check for required reboot
Workaround: Always reboot the system, and temporarily disable Windows updates, before performing an AMS setup.
#389612 AMS 5.0 Configuration Collector does not collect the license file.
Workaround: Add the license file manually to the data that you send to technical support.
#389613 Configuration Collector fails if run without Admin rights
#388922 Unable to have the twin MAC installed
If a Microsoft .NET 6.0 package without hosting bundle was installed before the Microsoft .NET 6.0 version provided by MAC setup, then the MAC setup fails.
Workaround: Uninstall any previously installed .NET 6.0 packages before running the MAC setup.
#389609 Custom fields: 'lastname' can be set "not required" and not "visible"
The field 'lastname' can be configured thus, but this leads to errors.
Workaround: The Lastname field must always be "required" and "visible".
#389610 Custom field 'persclass' can be set "not required"
The field 'persclass' can be configured in such a way but this leads to errors.
Workaround: If you want to set this field "not required" then make sure that it is also "not visible"
#389696 Defining 9c door models on different AMCs for the same parking lot, leads to error.
Deletion is no longer possible.
Workaround: Always use door model 9c within the same AMC for one parking lot
#385841 Arming the outputs of a door model 14(b) not working correctly
If multiple door models of type 14(b) are created, and they share input-\output-contacts, then the intrusion system will not correctly arm and disarm the area.
Workaround: Always use pulse signals, not constant signals, to arm an intrusion area via an AMC.

7.2.2 AMS 5.0.1

#409808: Biometric access control (e.g. IDEMIA readers) cannot be used in combination with mobile access for the same user.
#409910: No demo license is automatically activated after a completely new setup. Select the demo license manually, or use a purchased license.

7.3 Intrusion

7.3.1 Intrusion event limitation:

Receiving of events and alarms depends on the network and system availability.
Events and alarms are not repeated if the intrusion panel was offline at that time, and AMS will therefore not receive them.

Max events per second over all on a system with the recommended specifications (see datasheet).

- SQL Server 2019 Express version: 70 events/sec (Max 2 million events can be stored in the event database)
- SQL Server 2019 Standard version: 150 events/sec

Note:
AMS can process max. 100 events/sec. overall from the access control system. Events are door open/close, access, audit trail etc.
If intrusion integration is used, one point change can create 3 events (e.g. Point shorted, Area not ready to arm, Point state changed)

7.3.2 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

#263421 It is possible, but damaging, to modify/delete cardholders directly on panel
Workaround: All user management should be performed by the ACS, not by the panel.

#389827 Synchronization between AMS and B/G panels
If an operator changes cardholder data in AMS, there may be a temporary discrepancy between the cardholder data displayed by the Swipe Ticker and the data in the AMS dialogs, until AMS synchronizes with the B/G panel. The delay is typically a few minutes.

If an operator reassigns a card from one person to another immediately, the synchronization between AMS and the B/G panel may fail, due to deadlock.

Workaround: the operator assigns to the second person only cards that have been free for longer than one synchronization cycle (typically a few minutes).
To be certain that no synchronization is pending, check the panel status in the **Configuration** > **Panels** > **Panel Administration** dialog for the status **synched** (green). It should not be **synch pending** (yellow).

7.4 MapView and Services

7.4.1 Initial States

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.

#389803 Swipe Ticker - Picture takes a longer time to display
Under extremely heavy server or network load, the cardholder pictures in the Swipe Ticker may not display immediately.

7.5 Dialog Manager

7.5.1 Guard tour and SimonsVoss readers

Readers from SimonsVoss are not supported for guard tours.

7.5.2 BioIPconfig Tool

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

7.6 Microsoft SQL Express

Microsoft SQL Express limitation:
Please note that the SQL Express DB installed with AMS 5.0 supports up to 2 million events.
The default retention time is 90 days.
Old events are deleted if:

- the DB is at 85 % of its maximum capacity (max file size 10 GB for SQL Express 2019), or
- the retention period has expired

If more access events are expected then please consider using a full version of Microsoft SQL.

7.7 Visitor Management

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

#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

#356159 Access profiles in VisitorManagement: duration of validity is not set
The default validation time slot configured for a visitor profile in the AMS is not provided to visitors coming from the Visitor Management system.
Workaround: Cardholders that are created by the Visitor Management system should also be maintained by the Visitor Management system.

#381312 Visitor cards expire at end of the day regardless of the expiry time.

#390863 Unexpected token while opening port 5706
After running the setup files of `BoschPeripheralDeviceAddon.exe` and `BoschVisitorManagementServer.exe` when upgrading from AMS401 to AMS50 there is a error message while opening `https://<VisMgmt server computer>:5706`
Workaround: Delete the browser cache on the client PC after an update from a previous Visitor management installation.

7.7.1 Visitor Management 5.0.1

#391881 After installing certificate of external email server, VisitorManagerServer Service needs to be restarted. Otherwise its not possible to use the secured connection to email server.
Workaround: After installing a certificate for external email server, restart the service `VisitorManagerServer`.

#395279 PNG file format for picture not supported
The file format PNG for user photographs is not supported in Visitor Management. Please use JPEG instead.

#401908 No support for Divisions
Visitor Management (VM) does not support AMS Divisions (“Tenants”). Do not use the Visitor Management product together with an AMS system where Divisions have been configured.

#408837 Omnikey Reader not recognized when using Firefox browser
The fault occurs when a Peripheral Device (PD) certificate is missing from the internal Firefox certificate store.
Workaround:

1. Open the "Certificate Manager" tool from windows (on the machine where the PD tool has been installed)
2. Open "**Trusted Root Certification Authorities**
3. Select the PD certification called `BoschAcePeripheralDeviceAddonHardware CA`
4. Right click and export this certificate as "`DER encoded binary X.509 (.CER)`")
5. Start Firefox and open Firefox settings
6. Import the above certificate into the internal Firefox certification store.
7. Restart Firefox.

#403324 Do not delete SDK user
The SDK User, which you create when installing Visitor Management, may appear on the dashboard. Do not delete this user, as that will impact the communication between Visitor Management and the AMS.

#408602 Language switch not immediately applied to pulldown menus
When switching the language of the web user interface the language switch is not applied to items of pulldown menus. This happens for instance in the settings menu.
Workaround: Select the desired language and reload the full page in the browser.

#410593 Expected departure is not synchronized to Visitor Management.
Visitor Management overrides the “authorized until” date for credential holders when the user edits any detail of a visit

7.8 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.

7.9 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.

7.10 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.

7.11 OTIS

#356015 OTIS: ConfigBrowser: You can create only 6 DES devices
Configuration is limited to 6 DES and 2 DER devices.

7.12 OSS-SO

#390502 OSS-SO – preactivated filter in authorization report is not always updated
The filter in the OSS-SO authorization report does not always allow 'Show all' if there is only one authorization.
Workaround: Select the authorization manually.

#390177 OSSO – Automatic refresh of the Authorization report dialog does not always work
Workaround: Press "F5" to refresh the page manually.

#381885: OSS-SO – Incoming state changes are not displayed while the stateAPI is offline
States are not correctly displayed if statesAPI restarts.
Workaround: Restart the OSS-SO service or wait for next update of state

#389017 OSS-SO - License unauthorized after network disconnect and restart
This error may also indicate a network problem. Please check the connection to the network and restart your browser.