Grasbrunn
October 2019

Release notes for Access Management System (AMS) Version 2.0

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

Table of Contents:

1 Installation Notes

1.1 Supported operating systems

AMS runs on the following operating systems:

	AMS Server	AMS Client
Windows 10 (64 bit, Enterprise LTSC)	Yes	Yes
Windows 10 (64 bit, Pro)	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 an AMS client

Minimum hardware requirements	• Intel i5 processor (4 Core) or greater • 8GB RAM • 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

1.4 Update of AMS 1.0 to AMS 2.0

Importing Certificates:

BVMS and AMS Client Update: After an update please follow the instructions in chapter "**Client Installation: Import the HTTPS Certificate**" of the Installation Guide to install the certificates in BVMS and AMS clients.

Migrating to new hardware:

1) Create a backup of AMS 1.0 on the old hardware (see installation Guide)
2) Install new server AMS 2.0 on the new hardware.
3) Restore the AMS 1.0 backup on the new hardware.
4) On the new hardware, run a repair installation of AMS 2.0 to unite the new software with the AMS 1.0 backup files.
5) Shut down the AMS 1.0 system before running the AMS 2.0 system.

Administrator password reset:

After an upgrade of AMS from an older to a newer version, the Administrator password is reset to the default password. This is desired behavior, and was implemented to allow recovery after loss of the administrator password (#214209).

2 New Features in AMS 2.0

2.1 AMS Milestone XProtect Corporate 2019 R2 Integration

AMS now integrates with Milestone XProtect Corporate 2019 R2 as a Video Management System (VMS). Operators can monitor alarms, events and device states from the AMS on the XProtect Smart Client, as well as send commands to AMS devices via the Smart Client. The XProtect integration supports Video Verification of persons entering the building: the operator can compare live images of persons entering with the persons' ID photos.
XProtect and AMS exchange the following kinds of information:

- Configuration resources
- Events
- States
- Credential holders data
- Commands

2.2 Map View Enhancements

The AMS Map View has been enhanced in a number of ways, detailed below.

2.2.1 DIP/DOPs

AMS 2.0 supports digital input (DIP) and output devices (DOP) representing the inputs and outputs of an AMC or extension board. Operators can now see the current state of DIPs and DOPs on the Map or view them in the device tree. The states of a DIP/DOP on the Map can be controlled through the map, and visualized through colors and icons, e.g. light bulb on/off or switch on/off. Permissions for these and other Map View enhancements are governed centrally from the main AMS dialog manager.

2.2.2 Areas

Areas are depicted in a matrix in the Map View, containing the area's state and current population (number of vehicles in the case of parking lots).

2.2.3 Swipe Ticker

The Swipe Ticker is a real-time display of the 50 newest access events of the last 10 minutes. Clicking on an access event highlights the corresponding reader on the map. The ticker can be paused, duplicated and undocked from the main window.

2.2.4 Contextual Filtering

Intelligent contextual filtering ensures that menus contain only those commands that are applicable in a given situation.

.

2.2.5 Improved Alarm handling

AMS alarm handling enhancements:

- Multiple operators on multiple workstations handling alarms synchronously.
- All alarm handling logged system wide.
- Synchronization of alarms with the Map View
- Customizable sound files for alarm types.

2.3 Divisions

AMS 2.0 supports multiple autonomous tenants ("Divisions") within the same AMS system.
The inter-visibility of operators, devices, alarms and events is normally restricted to their own Divisions. Nevertheless all visibility is subject to fine-grained control by system permissions.

2.4 AMS Server now supports Windows 10

AMS 2.0 client and server now both run on Windows 10. No special manual configuration steps are required to run the AMS sever on a Windows 10 operating system.

2.5 Self-certification according to EN 60839-11

AMS 2.0 has reached grade 2 for the EN 60839-11 self-certification.

2.6 Threat Level Management

AMS 2.0 introduces the Feature "Threat Level Management". The goal of threat level management is to respond effectively to an emergency or foreseen situation by making an instant change to the behavior of entrances throughout the affected area. Examples are:

- Lockout: Only first responders, with high security levels, can enter.
- Lockdown: All doors are locked. Both ingress and egress are denied to all credentials below a configured security level.
- Evacuation: All exit doors are unlocked.

Typical low threat levels might be configured as follows:

- Sports event: Doors to sports areas are unlocked, all other areas are secured.
- Parents' evening: Only selected classrooms and main entrance are accessible.

Up to 15 different threat levels can be defined for the system. Suitably authorized persons can trigger a threat alert with a momentary action, for

example through the operator's UI, through a hardware signal (e.g. push button), or by presenting a special alert card at any reader.
Threat levels can be set for each MAC independently. When a threat level is deactivated, entrances revert to their original states and behaviors.

2.7 Improvements on W2 fingerprint reader integration

The W2 fingerprint reader integration has been improved.

- Bug fixes in connection management between ACE and W2 reader
- Improved "Template on Device" handling, management the update and upload on fingerprint templates. Increased the time to update new cardholder data on the W2 reader.
- Bug fix for 37 bit HID cards using Bosch coded cards, if enrolment is done on W2 reader.
- Stability fixes of handling the application services for fingerprint management.
- Improved usage of CPU load in mode "Template on Device"
- Improved real time synchronization between ACE and W2 reader.
- In case of "Template on Device", cards are accepted if valid in the future.
- Faster connection times to execute fingerprint verification on W2 devices

2.8 Support new ADS-AMC2-2W controller (China only)

The AMC2 -2W controller supports two Wiegand reader ports and an extension module. It is already available for the Chinese market.
An AMC2-2W global variant is scheduled for 2019-12.
Check product catalog for availability.

2.9 ACE SDK

Applications using API from AMS V2.0 are compatible with BISACE 4.6.2 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 Optional post-installation steps

3.1 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. This is relevant to comply with data privacy regulations.
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.

As the retention time has a major impact on the size of the backup files, choose a size that is as low as practically possible.

4 Known limitations in AMS 2.0

4.1 Languages

4.1.1 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)'.

4.1.2 AMS languages and Operating Systems

Language of AMS installation has to be the same as that 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.

4.2 License Manager

- The Licence manager is available in English only.
- Log on to the Dialog Manager as Administrator in order to use the licence manager.

4.3 Map View and Services

4.3.1 Initial States

The states initially displayed by the system immediately after installation are not necessarily correct.
Workaround: Cold-start the system (DMS, MAC, AMCs, readers, etc.).

4.3.2 AMS Services

The API services are not started automatically after performing an AMS update or a system repair:

- Access Management System Access API
- Access Management System Identity Server
- Access Management System Map API
- Access Management System States API

Workaround: Reboot the server.

4.3.3 Simultaneous edits in Map View and device editor

Making device changes simultaneously in the device editor and the Map View can lead to inconsistent displays.

Workaround:

Use the device editor if possible only outside of business hours, and close it as soon as changes are complete. **(#224650)**

4.4 Dialog Manager

4.4.1 Signature Pad

Make sure that the latest signature pad firmware is installed on the 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/`

Note that a signature can only be deleted if the SignoPad hardware is physically connected.

4.4.2 Guard tour and SimonsVoss readers

Readers from SimonsVoss are not supported for guard tours.

4.4.3 Access IPconfig Tool

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

4.4.4 Configuration of new dialog station readers

Restart the Dialog Manager after installing a new dialog station reader (#216761).

4.4.5 Reliability of the BioIdentify process if a person has more than eight cards

The recommended maximum number of cards per person is 4. Tests have shown that the BioIdentify process can be unreliable if a person is assigned more than 8 cards of types supported by the W2 reader (#231091).

4.5 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.

4.6 Divisions with BVMS or Milestone Xprotect

The Divisions feature cannot be used in combination with Bosch Video Management System (BVMS) or Milestone XProtect Integrations.

4.7 Security issue in Milestone Xprotect

There is a bug in Milestone XProtect 2019 R2 and Corporate editions which causes the certificate validation to fail, making network communication insecure.

The AMS – XProtect plugin communicates with AMS services using HTTPS. If the XProtect server and AMS server are on separate computers, 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 may also be affected.

This bug is not present in:

- XProtect 2018 R3 Professional and possibly older versions

We recommend importing the AMS certificate regardless, so that once the bug is fixed by Milestone the integration will continue to function.

4.8 Microsoft SQL Express

The SQL Express DB installed with AMS 2.0 supports up to 100.000 access events at entrances per month with a default retention time of 1 month. If more access events are expected consider using a full version of Microsoft SQL.

4.9 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.

#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.

#214318 SimonsVoss Whitelist enabled\disabled state is not shown on MapView
Workaround: Customer must use SimonsVoss tools for verification.

#235565 SimonsVoss commands are not greyed out dependent on specific of SimonsVoss device states
All SimonsVoss commands are available if it is reader type of type SimonsVoss.

5 Additional Notes

5.1 Tools in Start Menu (Server)

The following tools are provided in the Access Manager Menu:

5.1.1 Access IP Config

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

5.1.2 Configuration Collector

The *Configuration Collector* is a tool which is installed on the AMS server. It guides you through the collection configuration information which is being stored in 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.

5.1.3 DB Password Change

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

5.1.4 Backup

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

5.1.5 Restore

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

5.2 Web Service

The Access Management System optionally provides a Web Service which can be used to retrieve specific data over http.
By default, the web service is disabled for security reasons. 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.

5.3 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 Known Bugs and Workarounds for AMS 2.0

#243460 Installation
If VC++ 2017 higher version than 14.15.26706..0 is already installed, then installation will fail
Workaround: Manually remove the higher version and install the required version of VC++

#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 the green LED is not shown, even if set permanent open by the controller, if an unauthorized card is used.

#199503 The AMS dialog manager terminates if the fingerprint reader loses its network connection while the system is recording a fingerprint.
For fingerprint enrolment the enrolment reader must be online continuously.

#219598 Displayed status of subsidiary devices when offline
When a device, such as an AMC, is offline then the status of its subsidiary devices, such as extension boards, may not be displayed accurately.
Workaround: Ensure that the main devices are continuously online.

#240773 Set Area dialog
The area of person is sometimes wrongly set when changing the parking area at the same time.
Workaround: Change the person's area back to the previous area afterwards.

#240857 AMC : Arming and Disarming IDS alarm causes inconsistent AMC messages
The number of the previously used card is randomly sent with the GMA activation/deactivation messages
Sometimes the card number is attached to the message and sometimes not.

#242058 Devices created always for division "COMMON"
If you create new devices then the Division is set to "common" regardless of what you have selected.
Workaround: After creation of devices, save and reload the configuration, then change the division as desired and save again.

#243264/241705 License counts are not updated immediately
Immediately after changing the numbers of licensed divisions or cardholders, the new numbers are not always reflected accurately in the dialogs.
Workaround: After making changes to the numbers of installed licenses, always restart the computer.

#215938 Client connection problems if server is re-installed with a different hostname.
If you reinstall the AMS server with a different hostname, the old hostname still exists in the registry of the clients, and requires a manual edit.
Proceed as follows:
On each client, in RegEdit navigate to "`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Micos\SPS\DEFAULT\Global\PS_MASTER`"
Within the registry key `@Value` replace the old hostname with the new Hostname.

#242850 Sometimes Administrator permission is required to configure dialog station reader on the server
Workaround: Start the Dialog Manager as Administrator and configure the dialog station reader. Afterwards the reader can be used without administrator permissions.

#242210 Bosch Code and serial number enrolment reader can produce duplicate data
If serial number enrolment reader is used first, and then the Bosch Code reader with the same card, then the same serial card number will be found twice in database (one in `codedata` and the other one in `codedata2`). A subsequent search for the card may fail.

#204170 DMS/MAC toolbar icons are passive on Windows Server 2016 and Windows 10
The running state is shown but a double click will not work.
Workaround: Remove these applications from windows startup.

#241435 If a division is removed from the system, the Map View application does not remove it from the maps
Workaround: Avoid deleting divisions at all, or remove all the division's dependencies before deleting it.

#242702 Area counters in Map View not correct

Area counters can sometimes take as much as 15 minutes to refresh.

#243994 MapView history filter does not work
The filter criterion “Alarm category” is not currently used.

#243854 Refresh button causes Map View to display an error message in certain cases
An error message is shown, for example, if an operator who has no permission to see the swipe ticker clicks the main Refresh button. The application is nevertheless fully functional.

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

BT-SC/PAS5