Access Management System (AMS) version 4.0.1 RELEASE NOTES

2022-06

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

Document history.

Version	Description
1	2022-06-09 approved version

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 catalogue 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 BIS 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 20H2 and 21H1 – 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 20H2 and 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 20H2 and 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 (for Visitor management)	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 4.0.1 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 Exclusive use of SQL Server intances

In accordance with best security practices, do not use the SQL Server instances that are installed by AMS and its add-ons for the installation of 3rd-party or other products.

1.6 Update of AMS 1.0 to AMS 4.0.1

1. Upgrade from 1.0 to 2.0 as described in the AMS 2.0 installation guide.
2. Upgrade 2.0 to 4.0.1, as described below.

1.7 Update of AMS 2.0, 3.0, 3.0.1, 4.0, to AMS 4.0.1

1. Create a backup of the old AMS installation.
2. Update directly to AMS 4.0.1, 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**
For BIS: Command in the Device tree: **Allow sending of the secure key to the AMC**
Follow this procedure also whenever you have cleared the DCP using the AMCIPConfig tool or cleared the key via AMC's LCD display button.

1.8 Languages

Supported languages in AMS 4.0.1:

- EN-US
- FR-FR

1.8.1 Settings required for Arabic installations (AMS 4.0)

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)'.

1.8.2 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).

2 New Features in AMS 4.0.1

2.1 Request for exit “REX” shunt

At entrances where there is no security risk in opening a door manually from the inside, a motion detector often takes the place of a REX button, to unlock the door. For this common scenario, the ACS provides a simple means of extending the duration of the REX signal from the motion detector, while simultaneously shunting (suspending) the Door forced open alarm.

2.2 Support for the B901 door controller

B901 Access Control Interface Modules can be controlled via the AMS Map View.
The B901 is a simple door controller that a system administrator connects to Bosch intrusion panels.
The B901 can lock/unlock, secure/unsecure, and cycle doors, but it provides limited state information to the access control system.

2.3 Visitor Management enhancements

AMS 4.0.1 is the second third version to support the web based Visitor Management module.
The Visitor Management server setup must be executed on the same computer as the AMS server.
Visitor Management is now available in all languages AMS supported by AMS.
The Visitor Management version is specific to the AMS version with which it is delivered.

The latest Visitor Management V 1.0.1 is part of the AMS 4.0.1 package.

Enhancements:

- Checking visitors in and out without cards.
- Searching for the numbers of free cards.
- Distinguishing between different hosts with the same name.
- (Performance enhancement) Finer granularity of dialog refresh.

3 New Features in AMS 4.0

3.1 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 „**Restore configuration**" command.
At this point the mode settings made in the device editor, such as time models, are restored to the devices.

AMS 4.0 Map View now fully supports Mode override with graphics and context-menu commands.

3.2 Integration of OSS-SO offline locking systems

OSS-SO standard offline locking systems are now supported by AMS. In this first version of OSS-SO integration we have tested OSS-SO hardware and software from Uhlmann&Zacher with MIFARE DESFire EV1 cards, and LECTUS select readers as card updaters.
AMS offers an intuitive modern web-based configuration tool to map an OSS-SO site definition from the U&Z tools with the full offline locking system and personnel data in AMS.

Limitations in this first version:

- No divisions supported
- No hierarchical DMS systems
- No OSO battery states
- No OSO logbook
- No OSO blacklist
- No audit trail
- No OSO reports
- One lock system only (.e. one OSS-SO site)
- One card technology "MIFARE DESFire".
- OSO card initialization of OSO file 1 and 2 is done externally (for example in Uhlman&Zacher tools)
- File must be 288 bytes where 3 time models with 2 week models and 2 intervals and up to 72 permissions
- Max 10 update readers of type "LECTUS select"
- No states of update readers displayed
- No ACE SDK support
- No persons of type Visitor supported

- No import/export of OSO cardholders supported
- System tested with up to 1000 locks. Performance problems could occur if more locks are configured.

Note: According to the OSS-SO standard the site ID cannot be 0. Always use an alternative to the default Uhlmann&Zacher site ID (0).

3.3 Secure DTLS protocol for MAC/AMC communication

In AMS 4.0 and later, AMC controllers communicate with MACs via the secure DTLS protocol. For this, every AMC controller that is enabled requires a device communication password (DCP). You can set DCPs for all AMCs in a top-down manner in the device editor. Alternatively you can set individual DCPs initially using the AMCIPconfig tool, and add the DCPs in the device editor afterwards.
See the AMS and/or AMCIPConfig manuals for detailed instructions.

3.4 Access control hardware devices

With DTLS-Support AMC will no longer support RS485 or RS232 connections between host (MAC) and AMC.
Disable or remove from your configuration all AMCs that are configured on COM ports. Until you do this the device editor cannot finalize the migration, that is, it cannot save the configuration.

With AMS 4.0 the bootloader has been updated to version `00.62 v02.30.00 LCM.`
AMCs will be updated automatically by AMS 4.0.
If you wish to update AMCs manually using the Bosch.AMCIPConfig-Tool:
If the AMC has Bootloader `V00.49` and earlier, you must first update to `V00.61v01.47.00`
And from there to `00.62 v02.30.00 LCM`

Firmware downgrades: If you wish to use an AMC that has been upgraded to BIS 4.9.1 or AMS 4.0 on an older access control system (ACE, AMS or APE) then an AMC firmware downgrade is necessary: Firmware versions `V00.62` must first be downgraded to `V00.61` before they can be downgraded to older versions.

3.5 IDEMIA “Universal BioBridge" Integration

IDEMIA (formerly Morpho) is a multinational company specializing in security and identity solutions and an IPP partner of Bosch BT
MorphoManager is a biometric access control application from IDEMIA.
BioBridge is the interface software connecting MorphoManager with Bosch access control system.

Consult the White Paper for instructions on configuration

Limitations:

- IDEMIA software supports up to 100.000 cards only
- IDEMIA software does not support divisions
- Use IDEMIA software on Windows 10 only, because older operating systems are not supported by AMS.
- Duress finger functionality is currently not supported with IDEMIA devices.
- Only one IDEMIA system per BIS ACE is supported.

Notice:
The deletion of biometry data must be configured on the IDEMIA side. Use IDEMIA readers only in accordance with the data-protection laws of your country. We recommend that you set a deletion cycle of 2 days.

If multiple cards are assigned to one cardholder in the access system, only the oldest of the valid access cards of a cardholder is synchronized with the IDEMIA system. This is because the IDEMIA system is restricted to one card per cardholder,

If you restore in AMS a backup of a system where IDEMIA was used, go to AMS main menu > **Configuration** > **Tools** > **IDEMIA database configuration**; there delete and recreate the IDEMIA database.

Cardholder ID photos can be transferred for enrollment to the IDEMIA system. The quality of the cardholder pictures in the AMS may be insufficient for accurate face recognition by IDEMIA. The more secure variant is to enroll picture templates on the IDEMIA devices themselves. But if no high-security face-recognition is needed, the transfer of AMS photos can be activated in the tool **IDEMIA database configuration**.

3.6 OTIS Elevator integration

Compass is a Destination Management System from the Otis Elevator Company. Its function is to manage multiple banks of elevators, dispatching elevators to passengers so that they can reach their destinations as efficiently as possible. To provide the necessary data, passengers no longer simply press **Up** or **Down** keys, but request their destinations at card-reader, touchscreen or keypad terminals.
Integration with Bosch access control systems adds security. Based on their credentials and the time models in operation, passengers are transported to their home floors and other authorized destinations efficiently. The system will not accept requests for floors that are not in the passenger's authorization profiles, or at a time of day that is outside the current time model.

Overview of integration in the access control system

Administrators of the access control system integrate Compass in the following steps:

1. Configure the Compass hardware upon a single MAC in the Device Editor.
2. Configure customized fields for Otis-specific cardholder properties such as home floor.
3. Create Authorization profiles that govern access to specific elevator destinations.
4. Assign authorization profiles to the appropriate cardholders

For details, see the AMS Configuration and Operation manual.

3.7 Occupancy Monitor

AMS 4.0 supports the Occupancy Monitor where the current populations of configured areas (including parking areas) are displayed. For areas the count reflects persons, for parking areas it reflects vehicles.

The Occupancy Monitor setup is found in `AddOns\ACE\OccupancyMonitor` and must be installed on the AMS server after installation of AMS.

Limitations:

- Released for SQL Server 2019 only.
- Occupancy Monitor does not distinguish between divisions. The areas of all divisions are shown

3.8 Temporary cards for intrusion systems

Temporary cards are now supported for intrusion panels.
If a card was assigned to intrusion system and afterwards replaced by a temporary card the temporary card is send to the intrusion system. If the original card is reinstated, then the temporary card will be removed from the panel, and replaced by the original card.
Prerequisite: The temporary card must have the same encoding as the original card.

3.9 PegaSys and LEGIC advant cards

In PegaSys systems where LEGIC advant cards are used, the Dialog Manager can now create missing LEGIC segments, provided that the IAM cards are available and your enrollment reader supports the writing of segments

3.10 Key Management Tool for LECTUS select and MIFARE DESFire

This tool allows the customization of the following access parameters of MIFARE DESFire credentials:

- The application ID
- The DESFire file number
- The file read key.

Since these parameters contain security relevant information, they are stored in a password-secured, encrypted file. This file, called the parameter file, can be then imported into the access control system through the Device Editor, and used to configure readers.

3.11 ID verification using 3rd party devices such as face and numberplate readers

The API-SDK and the AMC have been enhanced to support access verification requests from 3rd party systems. See the Access Engine configuration help for details.

The precompiled sample application provided in the API-SDK directory can be used to try the new 3rdParty validation request:

```
\AddOns\ACE\API\C++API\bin\ClientACEInterfaceCS.exe
```

Many new integrations based on this SDK extensions are already developed and tested, for example ISS an Oosto (formerly Anyvision) biometric solutions for face and license plate recognition.

3.12 Enhanced editing of AMC devices in the device editor

The device editor allows the copying and pasting of entire AMC subtrees across MACs or within a single MAC. The complete device configuration is copied except for parameters like names and IP-addresses, which must be adjusted afterwards.

All AMCs below a DMS or MAC can be activated/deactivated with a single configuration command **Activate / Deactivate all LACs** from the context menu of a DMS or MAC in the device editor.

3.13 ACE API/SDK

The “**RestoreConfiguration**” command is available in the AMS API/SDK, and behaves in the same way as in the user interface.

The new AMS API/SDK is backwards-compatible with AMS versions depending on the features available to those versions.

The SDKs in AMS 4.0 and BIS 4.9.1 are identical.
Changes to the API are documented in detail in the files, "`ACE API.pdf`" and `ACE API Database- xxx.pdf`.
A complete matrix overview about the compatibility can be found in "`ACE API.pdf`".

3.14 Extended filters

The ACE dialogs “Group of persons” and “Group authorizations” have been enhanced. They now contain a maximum of 5 selectable additional fields for filtering and finding persons by custom fields.

3.15 Updated Import-Export tool

The new Import-Export tool including documentation is available in the `\AddOns\ACE\ImportExport` directory. Person data can be imported and exported.
Notice:

- No API-SDK license is needed any longer to use the new Importer-Exporter tool
- Persons of type Guard (W) are not supported.

3.16 Performance of fingerprint verification (BioEntry)

For every MAC a dedicated interface process is started for biometric verification requests. For bigger systems we therefore recommend using multiple MACs and distributing the fingerprint readers over the MACs.
Recommended: Maximum 100 fingerprint readers per MAC, if fingerprints are rarely used. If frequently used, 50 per MAC.

3.17 New monitoring tools for MAC and DMS

After installation there are 2 new applications available on the desktop: **MAC Control Console** (MAC) and **ACE Process Control** (DMS). Administrators can use these to verify the state of the internal processes.

Limitations:
The debug trace level of the new ‘netcore’ services found in **ACE process control** cannot be changed at runtime.

Workaround: First change of the trace level in the Configuration Browser and then restart the processes in the **ACE process control** (DMS).

3.18 Door model 14 enhancement

The door model 14 has been enhanced. Now the behavior can be configured to grant access and disarm the alarm system in one step. The possible device configurations are described in detail in the AMS configuration manual.

3.19 Timeout for automatic transfer to “Outside” area

For each MAC in the device editor, tab: **Global access settings**, you can configure the timeout for setting the location of a cardholder to the “Outside” area. The control is called **Area dwell time of person expires after**:
The default value is 24 (hours). A setting of 0 deactivates the timeout.

4 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 an **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

4.1 Supported panels and panel extensions

The following B/G intrusion detection panels are supported by AMS 4.0:

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

5 Optional post-installation steps

5.1 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.

5.2 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.

6 Resolved issues in AMS 4.0.1

Resolved issue **#368881**:
The latest firmware for W2 fingerprint readers is now included, and can be found at:
`\AddOns\BioConfig\`
firmware file `bew2-oapb_v1_1_5_bosch_20210706_213500_sign.bin`

Resolved issue #**380152**:
The **Cards** dialog has been changed, so that customers without an OSO license no longer see the OSO tab.

Resolved issue **#376130**: **Problem adding cards with access reader as enrollment reader**.
When an access reader used as an enrollment reader, the **Cards** dialog, **Assign cards** function now accepts all kinds of card number.

Registry entries now exist to support the following card types:
`0`=Unknown,
`1`=EM26,
`2`=iClass26,
`3`=iClass37,
`4`=HIDProx26
The registry path for them is
`[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Micos\SPS\DEFAULT\CardData\DefaultCardType]`
The default value is `0`, as in previous versions.

Resolved issue #**367866**: The Backup-Restore patch is now included in the standard software.

Resolved issue **#371989**: The AMC Access Delay patch is now included in the standard software.

6.1 Resolved issues in AMS 4.0

Resolved issue #**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.

Resolved issue **#246461: Card types not correctly activated after update**
On AMS/ACE update the active card types are no longer overwritten.

Resolved issue #**268298**:
The UP and DOWN buttons in dialog "**Administration of alarm panels**" can now be used.

Resolved issue #**269523 MAC offline / down status is not visualized in maps and device tree**
MAC online\offline state is now shown correctly.

Resolved issue #**270449: Temporary cards are not assigned to intrusion panels.**
Temporary cards will now be assigned to intrusion panels if the card type is supported and this card replaces the intrusion card.

Resolved issue #**272849**:
Area counters for parking spaces are shown in summary line also.

Resolved issue #**280440** AMC4W cannot detect the state open on an input

Resolved issue #**287009**: **ACE failed after setup when the server name contained the letters "APP"**
Server name can now contain the character string "APP".

Resolved issue #**326143: During the repair setup, the setup of the certificate tool fails**
On repair setup the certificate setup works again.

Resolved issue #**335631**: **It isn't possible to change a reader type to a reader type using another firmware at one AMC in the device editor.**
The reader type can now be switched to other protocols by removing the AMC firmware version and replacing with new one in device editor.

Resolved issue **#336792: Additional cipher suites**
RabbitMQ has now been updated to support additional secure cipher suites "ECDHE-RSA-AES256-GCM-SHA384" and "ECDHE-RSA-AES256-SHA384". Thus cipher suites "AES256-SHA256" and "AES256-GCM-SHA384" can now be disabled in case of security concerns.

Resolved issue **#340743: ACE-Authorizations: no Otis elevator shown**
In the cards dialog Otis elevator authorizations are now shown.

7 Known limitations in AMS 4.0

7.1 Intrusion

7.1.1 Intrusion event limitation:

Receiving of events and alarms depends on the network and system availability.
Events and alarms are not repeated if they occurred when intrusion panel was offline. AMS will therefore not receive them.

Max events per second overall on a system the recommended specifications.

- 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. from the access 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)

7.1.2 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

The cards must be enrolled by an OmniKey reader, or manually in the **Cards** dialog, so that the card type with its bit length is made known to the system. A workaround exists for cases where an access reader is used (#376130): here a default can be configured in the registry for unknown card types read by an access reader. See 6 Resolved issues in AMS 4.0.1

7.2 Remarks and Limitations on Map View and Services

7.2.1 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 cold-start the system (DMS, MAC, AMCs, Readers etc..) and so force a MAC-switch.

7.3 Dialog Manager limitations

7.3.1 Guard tour and SimonsVoss readers

Readers from SimonsVoss are not supported for guard tours.

7.3.2 BioIPconfig Tool

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

7.4 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.

.

7.5 Microsoft SQL Express

Microsoft SQL Express limitation:

Please note that the SQL Express DB installed with AMS 4.0 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.

8 Recommended practices

8.1 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 been cleared.

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.

8.2 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.
Do not use it to view the latest state changes, as these are automatically processed by the Map View application.

8.3 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.signotex.com/download/treiber/twain-wia-treiber/`

8.4 Milestone Xprotect

Supported XProtect versions: Corporate 2020 R1 and higher.

9 Known issues and workarounds

9.1 AMS Setup and Update

#329012 AMS setup does not work if 8.3 filenames are disabled
Despite an apparently successful setup, AMS 4.0 Map View does not operate correctly if filename format 8.3 is disabled in Windows.
Workaround:
Before installing AMS 4.0 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.

#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.

9.2 AMS General

#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.

#240264 FOLLOW_STATE function only with type “state”
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.

#266957 AMS 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.

#281358 CFS – AMS threat-level text incorrect
On deactivation of a threat level the Map View application shows a message without a threat-level name. In all threat level activation messages the threat-level name is shown.

#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.

#339756 LECTUS select reader input/output signals cannot be configured
Reader input/output signals for **LECTUS select** (LCTSL) cannot be configured in the device editor (Entrance node > **Terminals** tab).

#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.

#328222 AMC controllers - Reassigning names or IP addresses

When reassigning the names or IP-addresses of AMCs in the device editor, make sure that you never have two or more AMCs with the same name or IP-address simultaneously. If you want to swap the name or address of two AMCs, the recommended procedure is:

1. Reassign one of the AMCs involved to an unused dummy name or address, save it.
2. Reassign the other AMC to the intended name or address, save it.
3. Reassign the first AMC from the dummy name/address to its intended name/address.

9.3 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 two separate enrolment readers, one for the Dialog Manager, and one for 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

9.4 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.

9.5 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.

9.6 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 been executed successfully.

#206988 SimonsVoss delete Construction Whitelist
If the Construction Whitelist had been used before being integrated into AMS then the MAC may not be 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 a SimonsVoss reader type.