

Access Management System (AMS) version 5.5 Release Notes

This document is intended to familiarize you with your new AMS version.

Document history.

| Version | Description |
|---------|--|
| 1 | 2024-02 Readme of Access Management System 5.5 |
| 2 | 2024-05 Implementation of technical review |
| 3 | 2024-05 Final and revised version of the Release notes |
| 4 | 2024-10 Update information on Server requirements |

Table of Contents

- 1 Installation Notes 4
 - 1.1 Documentation 4
 - 1.2 Server requirements 4
 - 1.3 Client requirements 5
 - 1.4 Databases: support for MS SQL 2019 6
 - 1.5 Update of AMS 1.0 to AMS 5.5 6
 - 1.6 Update of AMS 2.0 and later to AMS 5.5..... 6
 - 1.7 Languages..... 6
 - 1.7.1 Locale setting required for non-English installations..... 7
 - 1.7.2 AMS Setup languages and Operating Systems 7
 - 1.8 Compatibility List of Software Components for AMS 5.5 8
- 2 New Features in AMS 5.5..... 9
 - 2.1 Multi User Manager 9
 - 2.1.1 Backup and Restore 9
 - 2.2 Mobile Access, Credential Management, Visitor Management 9
 - 2.2.1 Splitting of API in Back-channel and Front-channel..... 9
 - 2.2.2 Synchronization between AMS and Credential Management..... 10
 - 2.3 Access Management System 11

| | | |
|-------|---|----|
| 2.3.1 | CEPAS card support..... | 11 |
| 2.3.2 | API operator protection | 11 |
| 3 | Mandatory installation steps for Intrusion integration | 12 |
| 3.1 | Supported panels and panel extensions..... | 12 |
| 4 | Optional post-installation steps..... | 13 |
| 4.1 | Security recommendations for user authorizations | 13 |
| 4.2 | Retention time of system events..... | 13 |
| 5 | Resolved issues in AMS 5.5..... | 14 |
| 6 | Recommended practices | 16 |
| 6.1 | Intrusion integration..... | 16 |
| 6.2 | Reactive Firewall after Client Workstation Installation | 17 |
| 6.3 | Reload button in Map View | 17 |
| 6.4 | Signature Pad | 17 |
| 6.5 | Milestone Xprotect | 17 |
| 6.6 | Credential Management and Visitor Management | 17 |
| 6.7 | Mobile Access requires .NET 8..... | 18 |
| 7 | Known limitations and workarounds..... | 19 |
| 7.1 | AMS Setup and Update..... | 19 |
| 7.2 | Multi User Manager limitations..... | 19 |
| 7.3 | Multi User Manager backup and restore alternative | 20 |
| 7.4 | Restore Settings | 22 |
| 7.4 | Mobile Access | 23 |
| 8 | Additional information..... | 24 |
| 8.1 | AMS general..... | 24 |
| 8.1.1 | Cybersecurity guidebook location | 24 |
| 8.1.2 | Event viewer (AMC/MAC messages not visible) | 24 |
| 8.1.3 | Known bugs in AMS 5.5 | 25 |
| 8.1.4 | Remarks - PCS INTUS 1600 | 27 |
| 8.1.5 | Achieving EN 60839 (AMS 5.5)..... | 27 |
| 8.1.6 | Windows system time change | 28 |
| 8.1.7 | Backup file location..... | 28 |
| 8.1.8 | Access control hardware devices..... | 28 |

| | | |
|--------|--|----|
| 8.2 | Intrusion..... | 30 |
| 8.2.1 | Intrusion event limitation: | 30 |
| 8.2.2 | Intrusion cardholder synchronization limitation: | 30 |
| 8.3 | MapView and Services | 31 |
| 8.3.1 | Initial States..... | 31 |
| 8.4 | Dialog Manager | 31 |
| 8.4.1 | Guard tour and SimonsVoss readers | 31 |
| 8.4.2 | BioIPconfig Tool | 31 |
| 8.5 | Microsoft SQL Express..... | 31 |
| 8.6 | Visitor Management | 32 |
| 8.6.1 | Visitor Management 5.0.1 | 33 |
| 8.7 | Milestone Plugin | 34 |
| 8.8 | SimonsVoss | 34 |
| 8.9 | OTIS | 34 |
| 8.10 | OSS-SO Configuration | 35 |
| 8.11 | Hardware supported by Windows 11 | 35 |
| 8.11.1 | Readers | 35 |
| 8.11.2 | Hardware..... | 35 |

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

Hardware and software requirements for an AMS server:

| | |
|--|---|
| <p style="text-align: center;">2024-10 Upd</p> <p>Supported operating systems (standalone or client/server mode)</p> <p>Installations of AMS on other operating systems may succeed, but are entirely without warranty</p> | <ul style="list-style-type: none"> • Windows 11 Professional and Enterprise 23H2 • Windows Server 2019 (Version 1809) (64bit, Standard, Datacenter) • Windows Server 2022 (64bit, Standard, Datacenter) • Windows 10 Professional and Enterprise 22H2; Windows 10 21H2 LTSC <p>Ensure that the latest Windows updates are installed.</p> <p>Note: The default database delivered with this system is SQL Server 2019 Express edition with advanced services.</p> |
| <p>Minimum hardware requirements</p> | <ul style="list-style-type: none"> • Intel i7 processor generation 10 • 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: <ul style="list-style-type: none"> ○ 256 MB RAM, ○ a resolution of 1280x1024 ○ at least 32 k colors • 1 Gbit/s Ethernet card • An available 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 | <ul style="list-style-type: none"> • Windows 11 Professional and Enterprise 23H2 • Windows Server 2019 (Version 1809) (64bit, Standard, Datacenter); Windows Server 2022 (64bit, Standard, Datacenter) • Windows 10 Professional and Enterprise 22H2; Windows 10 21H2 LTSC <p>Ensure that the latest Windows updates are installed.</p> |

1.3 Client requirements

Hardware and software requirements for an AMS client:

| | |
|--|--|
| Supported operating systems (standalone or client/server mode) Installations of AMS on other operating systems may succeed, but are entirely without warranty | <ul style="list-style-type: none"> • Windows 11 Professional and Enterprise 23H2 • Windows 10 Professional and Enterprise 22H2; Windows 10 21H2 LTSC <p>Ensure that the latest Windows updates are installed.</p> <p>Note: with AMS Pro, updates must be deferred until 8 months after the release of the AMS version. For further information see the Microsoft Technet page at https://technet.microsoft.com/en-us/itpro/windows/manage/introduction-to-windows-10-servicing</p> |
| Minimum hardware requirements | <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> ○ 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 | 126 or higher |
| Microsoft Edge | 124 or higher |
| Mozilla Firefox | 125 or higher |

1.4 Databases: support for MS SQL 2019

For new installations of AMS 5.5, 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 becomes updated to SQL Server 2019 if database was installed by AMS setup.

After SQL update, the database backups are then found in the USE\Documents\Backups folder. Refer to Backup file location for more information.

1.5 Update of AMS 1.0 to AMS 5.5

In order to update to AMS 5.5, you need a valid SMA and update the licenses at Bosch Remote portal.

Upgrade from 1.0 to 2.0 as described in the AMS 2.0 installation guide.

Upgrade 2.0 to 5.5 as described below.

1.6 Update of AMS 2.0 and later to AMS 5.5

1. Create a backup of the old AMS installation.
2. Update directly to AMS 5.5 as described in the installation guide.

Before enabling the AMCs host communication 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 the host communication has been enabled. AMCs that are not reachable within these 15 minutes will not receive the firmware update. To restart the provisioning phase from dialog manager:

1. Clear the **Enable** check box of host communication and save the configuration.
2. Select the **Enable** check box of host communication and save again.

Alternatively, the provisioning phase can be activated using the AMCs context menu in MAP View Client:

- For AMS.
 1. 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

GUI supported languages in core AMS 5.5

- AR-EG
- DE-DE
- EN-US
- ES-AR

- FR-FR
- HU-HU
- JP-JP
- NL-NL
- PL-PL
- PT-BR
- RO-RO
- RU-RU
- TR-TR
- ZH-CN
- ZH-TW

Note: AMS 5.5 add-ons do not support all the languages supported by AMS 5.5. Refer to the datasheet for more information.

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 the AMS reports and some dialog controls will show placeholder characters instead.

Note: If the operating system is using a multi-language pack, installing the 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-UILocale`. 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 5.5

| Component | Build version | Location |
|----------------------|----------------------|---|
| Importer/Exporter | 1.3.8 | AMS Media Package Folder: AddOns/Standard/ImportExport |
| Occupancy Monitor | 1.3.5 | AMS Media Package Folder: AddOns/Advanced/OccupancyMonitor |
| AECT Tool | 1.0.0.7 | AMS Media Package Folder: AddOns/Advanced/AECT |
| Bio IP Config Tool | 5.5 | AMS Media Package Folder: AddOns/Advanced/BioConfig |
| IPConfig (AMC) | 1.14.3 | AMS Media Package Folder: AddOns/Standard/AccessIpConfig |
| SDK Version | 5.5 | AMS Media Package Folder: AddOns/Advanced/API |
| MAC Installer | 5.5 | AMS Media Package Folder: AddOns/Advanced/MultiMAC |
| Key Management Tool | 2.8.2 | AMS Media Package Folder: AddOns/Advanced/ReaderConfigTool |
| Intrusion RPS API | 2.2.27914 | AMS Media Package Folder: AddOns/Advanced/Intrusion-RPS-API |
| Milestone PlugIn | 5.5 | AMS Setup Folder: <Language>\ServerPlugin |
| BVMS Version | 11.1.1 | Download Store /Product Catalogue |
| VisitorManagement | 6.0.* | Download Store /Product Catalogue |
| CredentialManagement | 2.0.* | Download Store /Product Catalogue |
| MobileAccess | 3.0.* | Download Store /Product Catalogue |
| Peripheral Devices | 5.2.* | Download Store /Product Catalogue |
| Milestone Xprotect | 2020 R3 | Download Store Milestone |

— Note: All applications based on ACE API SDK need to be recompiled with latest SDK provided with this version. Application based on REST API should continue working.

2 New Features in AMS 5.5

2.1 *Multi User Manager*

2.1.1 Backup and Restore

Multi User Manager is an additional AMS feature. This web-based service allows administration of MAP 5000 panels users via an IP connection. It is designed for customers running several MAP 5000 panels to administrate the users on all the panels.

In AMS 5.5, Multi User Manager adds integrated Backup and Restore functionality for panel and user data. For most use cases, this supplants the previous manual backup procedure based on SQL Server Management Studio (SSMS). Administrators can schedule periodic backups and trigger on-demand backups from the Web user interface of the application, review available backups and related event history, and restore data from a backup as needed.

Multi User Manager securely encrypts backup files using an administrator-provided password and stores them in a configurable location in the file system. Therefore, it is strongly advised to:

- Store the encryption password in a secure location. Multi User Manager will prompt for the password when restoring a backup. Without the password, there is no way to recover the contents of a backup file.
- Ensure that the service account for the Multi User Manager server application has sufficient permissions to read and write from/to the backup location, in particular if this location resides in a mapped network drive. Check the backup event history in the Multi User Manager user interface to identify errors related to backup creation.

2.2 *Mobile Access, Credential Management, Visitor Management*

2.2.1 Splitting of API in Back-channel and Front-channel

Support from the release of Mobile Access 5.2, Credential Management 5.2 and Visitor Management 5.2 and later

The API of the Mobile Access Backend has split into a front-channel part and a back-channel part. The front-channel is supposed to communicate with mobile phones while the backchannel communicates with Credential Management and/or Visitor Management.

This allows now to set firewall rules and routes to regiment network traffic to strengthen IT security. The split of the API comes with two separate port numbers. That is, the mobile phones continue communicating to port number 5700, while Credential Management and Visitor Management address port 5701.

Both Credential Management and Visitor Management have now two separate settings for the front-channel URL and the back-channel URL respectively. The user interface calls them "Administrative service address" (back-channel) and "Registration service address" (front-channel).

The default port for "Administrative service address" (back-channel) is 5701. In a customer-specific firewall rule that port should be configured to only communicate with the AMS Server machine.

The default port for the "Registration service address" (front-channel) is 5700. In a customer-specific firewall rule this port should be configured to be reachable from the Mobile Access apps. In many scenarios that end-point would be accessible from outside. However, this is highly dependent on customer scenario.

If you are updating from an earlier version to AMS 5.2 and later, then the settings of Credential Management and Visitor Management need to be adjusted. This setting is accessible for the Administrator role for Visitor Management and Credential Management. The backchannel should be secured to not be reachable from the public / any unauthorized network.

Note that old invites (QR-Codes and Mail-links) can still be accepted after the update.

2.2.2 Synchronization between AMS and Credential Management

Synchronization between AMS and Credential Management has been optimized. This results in more frequent updates and increases the accuracy of data. Data that is being modified and saved in Credential Management is available in AMS immediately. Part of the data that was previously kept in the Credential Management database will be moved to AMS database. As a result, the Credential Management database will be smaller in size.

For consistency with AMS the Credential Management data fields "Assistant" and "Supervisor" were removed.

Existing data is automatically migrated after updating AMS and Credential Management update, no user interaction is required. Make sure to update both AMS and Credential Management to the latest version and update the products in this order.

2.3 Access Management System

2.3.1 CEPAS card support

The Singapore CEPAS cards are supported now in AMS 5.5. This is a project specific implementation. Be aware that CEPAS cards cannot be combined with any other card types since they cannot be distinguished by the access system. Card duplicates are possible. The AMS will not check if multiple card types are used and if they can be used together or not.

2.3.2 API operator protection

To avoid problems where important operators are deleted, an operator gets delete protection if the API permission is assigned. If the permission is removed, then the operator can be deleted again.

Security Advice: API operators must not get dialog permissions in DialogManager! All operators using the APIs like for

VisitorManagement/CredentialManagement/ImporterExporter or external API addons created by 3rdParty should not be extended.

In previous versions, it was deleted without notice. Needs to change to no access in the API limits rights.

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 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** communication protocol must be enabled and **AutomationPasscode** has to be set 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 the computer
- SQL Server database has never been installed on the computer
- RPS must be installed before AMS

3.1 Supported panels and panel extensions

The following B/G intrusion detection panels are supported by AMS 5.5:

- 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 intending to change the AMS setup (files, certificates, registry and licenses), and assign 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. This setting has no impact on the *Event viewer*. This only affects *Entrance events* and *Audit trail*.

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_\Log
gifier\SysKeep
3. Double click value “@value” (shown in the right pane) and enter a new value.

Note: The retention time has a major impact on the size of the backup files being created. The value choice should be as low as possible.

5 Resolved issues in AMS 5.5

#443565 Changed identification PIN input sequence not announced and documented

Fixed Problem: Due to necessary changes in the AMC Firmware, the Input Sequence for Identification PIN and Office Mode for Wiegand protocol was changed, so that the Sequence is now identical to OSDP protocol and LBUS protocol.

AMS Help files "PIN codes for personnel" and "Authorizing persons to set Office mode" are updated.

Update for "PIN codes for personnel": "For all protocols (RS485, Wiegand and LBUS): The cardholder enters: 4 # <the PIN>".

Update for "Authorizing persons to set Office mode" : "To start stop office mode at an entrance, the cardholder presses the number 3 # on the keypad, and then presents their specially authorized card at the reader. The entrance remains unlocked until an authorized cardholder presses 3 # and presents the card again".

#426195 AMS allows configuration of door model 10/14 with manual card number entry

Fixed Problem: The combination of Feature Identification PIN with Feature Arming and Feature Office Mode is not disabled in the User Interface but results to complex input sequences for the customer. Since this combinations are not foreseen, they are not tested and thus the AMS Help file "PIN codes for personnel" is complemented with the sentence: "Arming and Office mode is only supported with physical cards."

#397466 Special day configuration reset to default by update from earlier AMS Version to AMS 5.2

AMS languages with preconfigured special days, the special day configuration is updated in next AMS version again. If the customer changed the existing new year, they are restored to the definition of the AMS setup again.

Fixed: Special days are not updated anymore. If you change the configuration the setup will not touch the configuration anymore.

#340759

AMC - IO Function fails to react to the To Inspect event.

#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, the MAC setup fails.

#389610 Custom field 'persclass' can be set "not required"

The field 'persclass' can no longer set to "not required".

#410291 Windows Apps & features repair setup

Licenses no longer work after running a repair setup, if you use Windows **Apps & features**.

#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.

Bug fixed - If a door model 14 was configured before using shared signals, then, after an AMS Upgrade the door signal configuration must be checked and reconfigured if needed.

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 occurs 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. In 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 a keypad via card is not possible for areas that are in the background.

In case “Arm” and “Disarm” via card should be shown on keypad, ensure that the 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 cannot be deleted.

Note: For the command and 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 Reactive Firewall after Client Workstation Installation

In section 4.4 in the Map View Operation manual the statements suggest deactivating the firewall prior installation of the client workstation. This measure is only temporary, i.e., after successful installation of the clients, the firewall must be reactivated again.

6.3 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 several 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.

6.4 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

6.5 Milestone Xprotect

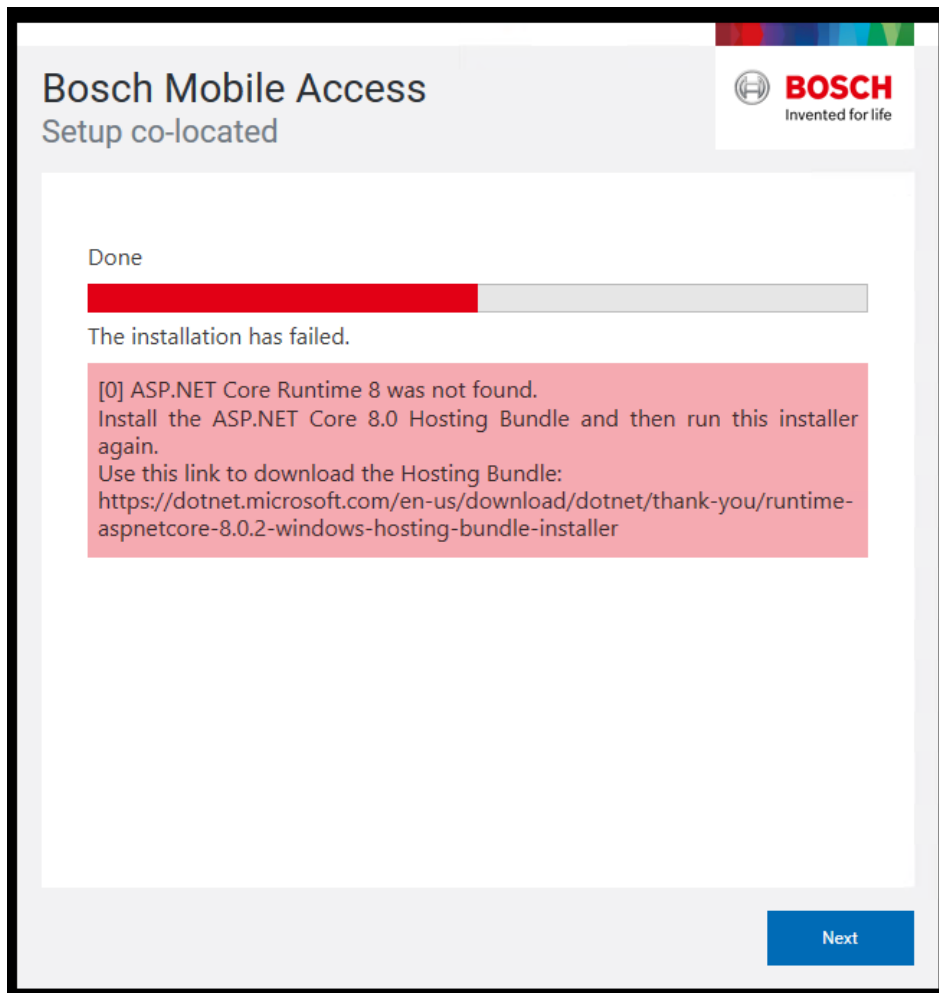
Supported XProtect versions: Corporate 2020 R1 and higher.

6.6 Credential Management and Visitor Management

To ensure secured connection to e-mail server when extra certificate is needed: In case the external mail server requires an extra SSL/TLS certificate, then import it to the machine running the mobile access backend. After importing it, the restart of BoschAceCredentialManagement and BoschAceVisitorManagement is required.

6.7 Mobile Access requires .NET 8

The mobile access backend requires the latest .NET version. The setup program will check if this is installed and inform the user if not. In a co-located setup the AMS will bring the required .NET packages, but in a distributed setup the installer must take care of this.



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 accessing dialog manager, sometimes only the “common” division is available to the BadgeDesigner menus.

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

#430471 AMS 5.2: Badgedesigner on Client - layouts cannot be saved

Workaround: Use the BadgeDesigner on the server.

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

7.2 Multi User Manager limitations

- **Synchronization Period Clarification**

When synchronizing user data from Multi User Manager to AMS, this change occurs immediately. When synchronizing user data from AMS to Multi User Manager, changes will be obtained when the synchronization interval is met. For example, every five minutes.

- **Time Zone Setting**

Time is reported to the panel in UTC format, and it is upon the panel to convert time to the local time. Therefore, users need to configure the right time zone on the panels.

- **Error Messages in OS Language**

Some error messages might be displayed in the Operative System configured language (e.g. "No connection could be established because the target machine actively refused it").

- **Lack of Division Support**

The use of Divisions as supported in AMS is currently not available in Multi User Manager.

- **User Name Synchronization**

Users which names contain the character "*" will not be synchronized by Multi User Manager, as this character is forbidden in AMS.

- **Risk of Removing Key Person**

It is possible to delete from the User who holds the OII credentials from the panel, which stops the communication with the MAP panel. Users must make sure this "user" is not deleted.

- **Panel User Data Synchronization**

Once a panel user is synchronized with Multi User Manager, any modification performed in the panel to the user data will not be synchronized (e.g. First name, last name). The only exception is the passcode.

- **Multi User Manager to MAP Panel User Data Synchronization**

Once a panel user is synchronized with Multi User Manager, any modification performed to the user data through the Multi User Manager UI will not be synchronized (e.g. First name, last name). The only exception is the passcode.

2024-10 Update information on

- **Hardware Requirements**

The current hardware requirements may not support the capacity needed for 800 panels. Update and communicate the hardware requirements to ensure that they effectively meet the demands of supporting 800 panels

- **Network Constraints**

The system performance can be affected by network constraints in a client-server architecture relying on HTTPS communication. Provide guidance on network configurations and best practices to mitigate the impact of network constraints on system performance and stability.

7.3 Multi User Manager backup and restore alternative

Note that the following restoration process is specifically designed for Multi User Manager databases with their inherent encryption. Due to this encryption, successful restoration is ensured only if the restore is executed on the same system where the backup was initially created.

Restoring on a different system may result in inaccessible or corrupted data due to encryption key mismatches derived from the original system.

Warnings:

- Ensure there are no Multi User Manager operations ongoing or occurring updates during the backup. This ensures a consistent database state.
- Alert users or administrators about the impending backup operation and any associated downtime.

Database Backup procedure:

1. Launch SSMS:
 - 1.1. Start SQL Server Management Studio. If it's not installed, you can download it from Microsoft's website.
2. Connect to the Database:
 - 2.1. When the "Connect to Server" window pops up, enter the server's name (e.g., WORKSTATIONNAME\ACE) and choose SQL Server Authentication. Enter the credentials (the same defined during AMS installation) and click on "Connect."
3. Backup the Database:
 - 3.1. Once connected, in the Object Explorer, expand the "Databases" node by right-clicking on the **Bosch.MUMDb** database.
 - 3.2. From the dropdown menu, navigate to: **Tasks > Back Up**.
 - 3.3. The "Back Up Database" window will appear. Ensure the "Database" field is showing the correct database name **Bosch.MUMDb**.
 - 3.4. In the "Backup type" dropdown, select "Full."
 - 3.5. For the "Backup component", ensure "Database" is selected.
 - 3.6. In the "Destination" section, you can see where the backup will be saved. If you want to change this location:
 - 3.6.1. Click on "Remove" to remove the existing path.
 - 3.6.2. Click on "Add..." and choose a new location.
 - 3.7. Make sure the file name ends with a .bak extension. Ideally, include a timestamp in the name as mentioned before (e.g., MUM_backup_YYYYMMDD_HHMMSS.bak).
 - 3.8. Once everything is ready, click on "OK" to start the backup process.
4. Completion:
 - 4.1. After the backup completes, you should see a message stating that the backup completed successfully. Click "OK" to close this message.
 - 4.2. You can now navigate to the backup location in the file system to confirm the backup file's presence.

Documentation:

- Document the exact date and time of the backup.
- Note down any special considerations or observations during the backup process.

Secure the Backups:

- Store the backup files in a safe location on the system.
- Ideally, make a secondary copy on an external drive or secure network location as a redundancy measure, even though the restoration can only happen on the original system.

Restore:

1. Preparation:
 - 1.1. Alert users or administrators about the impending restore operation and any associated downtime.
 - 1.2. Ensure no active users or operations are accessing Multi User Manager.
2. Database Restoration:
 - 2.1. Launch SSMS: start SQL Server Management Studio.
3. Connect to the Server:
 - 3.1. Upon launching SSMS, the "Connect to Server" window will appear. Enter the server name and choose the appropriate authentication method (Windows Authentication or SQL Server Authentication).
 - 3.2. Enter your credentials if necessary and click on "Connect."
 - 3.3. Initiate the Restore Process: in the Object Explorer, right-click on the Databases node (or directly on your Multi User Manager database if it's still present) and navigate to: **Restore > Database**.
4. Restore Settings:
 - 4.1. In the "Destination:" field, either select your **Bosch.MUMDb** database from the dropdown list or type in its name.
 - 4.2. In the "Source" section, select "Device:" and click on the "..." button to its right.
 - 4.3. A window named "Select backup devices" will pop up. Click on the "Add" button.
 - 4.4. Browse to the location where your .bak backup file is saved, select it, and click "OK."
 - 4.5. In the "Select backup devices" window, click "OK" again to confirm the backup file's selection.
 - 4.6. You should now see the backup sets available for restore in the "Restore Plan" section. Ensure the checkboxes next to the backup sets are selected.
5. Options Configuration:
 - 5.1. Navigate to the "Options" page on the left sidebar.
 - 5.2. In the "Restore options" section, ensure "Overwrite the existing database (WITH REPLACE)" is checked. This is crucial if you're restoring over an existing database.
 - 5.3. In the "Recovery state" section, you can usually leave it at the default setting ("Leave the database ready to use by rolling back uncommitted transactions. Additional transaction logs cannot be restored. (RESTORE WITH RECOVERY)"). However, if you have specific requirements, adjust accordingly.
6. Execute Restore:
 - 6.1. Once all settings look correct, click on "OK" to begin the restore process.

Warning: Restoring a database from a backup will overwrite the existing data, so always be sure you want to perform this operation and double-check the backup file you're restoring from.

5. Completion:
 - 5.1. Once the restoration process completes, you should see a message stating that the database has been successfully restored. Click "OK" to close this message.

5.2. You can now navigate to the Databases node in SSMS to see your restored Multi User Manager database.

6. Validation:

Once the restore process is complete, launch and test Multi User Manager to ensure the restoration was successful and that data integrity is maintained.

Review any restore logs or application logs for errors or inconsistencies.

7. Communication:

Inform users or administrators that the restore process is complete and that they can resume their activities.

8. Documentation:

Document the exact date and time of the restoration.

Note any issues, solutions, or observations made during the restore process.

7.4 Mobile Access

#451123 CFS: Mobile access app "setup access" cannot access reader that was configured with the very same app just before

Workaround: host names must not contain underscore characters.

After uninstalling Mobile Access backend, some traces of configuration are left.

Workaround: Remove them manually, if desired.

MAUser – this user remains after uninstallation. An administrator must remove it manually.

Cetificates – use *Manager computer certificates* to manually remove all certificates installed due to Mobile Access installation.

ID server configuration for Mobile Access – the file

appsettings.Extension.MobileAccessBackend remains after uninstalling the backend. Delete it manually.

"Repairing" distributed MA Backend after upgrading AMS

Workaround: It is necessary to run the MA Backend installer. First, update AMS to latest version (AMS 5.5). Then, run the latest MA Backend installer (shipped with AMS 5.5). In the distributed installation case this may require running the companion installer on AMS to collect system settings.

8 Additional information

8.1 AMS general

8.1.1 Cybersecurity guidebook location

After the execution of the AMS Server setup, a desktop link named *AMS documentation* can be found. Double-click on Windows Explorer, it will redirect to the directory where the Cybersecurity guidebook and further documentation can be found.

8.1.2 Event viewer (AMC/MAC messages not visible)

The following error/info events from AMC/MAC subsystem are invisible (not shown in event viewer) but found in debug logging and old LogViewer application details for the support team.

- `MSG_ACS_CARD_DATA_FRAME_CORRUPTED` = 0x01000A00;

This event is generated when a frame containing card data is received from a reader that is somehow corrupted (e.g. incomplete or too large).

- `MSG_ACS_CARD_DATA_CONFIGURATION_INVALID` = 0x01000A01;

The AMC is trying to apply a card data definition that is not valid (e.g. with an unsupported code data mode or a bit length that is incorrect for the conversion mode).

- `MSG_ACS_CARD_DATA_PARITY_ERROR` = 0x01000A02;

An error was detected while validating the parity data embedded in the card data. (In the past MLD_LESEFEHLER1)

- `MSG_ACS_CARD_DATA_DOES_NOT_MATCH_CONFIG` = 0x01000A03;

None of the card data definitions configured in the system match the card data provided by the reader.

- `MSG_ACS_CARD_DATA_INVALID_FIELD_VALUE` = 0x01000A04;

The fields in the card data have some values that are outside the allowed range or generally have corrupted a value (e.g. letters in fields that can only contain numbers).

- `MSG_ACS_CARD_DATA_INTERNAL_ERROR` = 0x01000A05;

This message should not be generated. If it occurs then there is an AMC-internal logic error.

- `-MSG_ACS_OFFICEMODE_DENIED` = 0x01000977;

OFFICE MODE permission denied. (Card does not have correct authorizations to perform office mode toggle).

- MSG_ACS_OSDPSC_REJECTEDBYREADER = 0x01000667;

OSDP secure connection rejected by reader.

Note: Translation to other languages are not available. It is available in English only.

8.1.3 Known bugs in AMS 5.5

#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

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.

#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.

#371585 AMC memory fills up if wrong password is configured

AMC – Offline/online messages fill up the AMC's flashCard if (e.g.) the DTLS password is incorrect.

#356203 AMCIConfig note

IPConfig does not always show the current firmware version when attempting a bulk firmware update.

#349902 AMCIConfig note

AMCIPConfig no longer allows access with the correct password after running for several hours.

Workaround: Always close the tool after use.

#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. This behavior will never be fixed. However, it is noted in documentation so the operator can be aware of it.

#389164 Server setup does not check for required reboot

Workaround: Always reboot the system and temporarily disable Windows updates before performing an AMS setup.

#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.

#432492 Supported Deister devices

The AMS does not support Deister terminals and devices with firmware 2.8 or later.

#447067 AMS 5.5: Event viewer shows English date and time selection in German version

Sometimes the Microsoft date time controls do not follow the local system setting and are using the english AM/PM format instead of 24 hours format.

The functionality to filter the event list works fine.

#450518 AMS 5.5: The CEPAS reader is not part of the Access reader

The enrolment of CEPAS cards does not work by Access readers because the card type is not set correctly and then the display of the card number will not be in the same way as for CEPAS cards who are enrolled by the USB/keyboard enrollment reader.

#439713 AMS restore on a fresh installed AMS with backup from a system with IDEMIA database leads to exception

If the backup contains a configuration where the IDEMIA database is used as interface, then the restore of this backup file will fail.

Workaround: Configure the IDEMIA database interface with your wanted 'database password' and then start the restore of the old backup then the restore will restore the full IDEMIA configuration too.

#440279 AMS: no debug logging when switching to another windows user

On windows 11 client machine: If debug files are created for one windows operator and then the operator is switched, then the dialog manager cannot access the old files and will **not** continue to write there anything.

Workaround: move the old debug files to another directory then the logging will be done for next new operator one time again.

#443141 AMS 5.2 upgrade to AMS 5.5: Rollback after failure in MAC MSI caused uninstallation of most AMS parts

If MAC update fails and a rollback is done, some parts get removed completely and not rolled back to AMS 5.2.

Hint: A Backup of AMS 5.2 must be done before upgrading.

#448969 AMS 5.5: strange error message from device editor when Demo mode expires

If 5 hours demo mode expires and device editor is started, then the error message number "15081536" could be shown.

Workaround: Do not work more than 5 hours without a license or reboot the computer after 5 hours.

#452946 AMS 5.5: Message text not clear when one tries to delete a user with API rights

Operators with permission to use the API cannot be deleted if they have such right. If the delete button is used, the error message is not detailed enough.

#455482 & #456045 Connection to server lost

If the client configuration application is open more than 2 days, some dialogs do not reconnect to server. Some server services throw out connections if they are not used more than 24 hours.

Workaround: Do not use device editor and dialog manager longer than 24 hours without logoff and login. After you leave your work, please logoff then the bug will not occur.

#454930 Input to activate the TLM is not always available

In device editor the Input for TLM activation is not shown if a new alarm level in TLM was added but not saved already.

Workaround: Save newly created TLM activation levels directly.

#455223 Wrong output consumption count

In some cases, the available used outputs are not calculated correctly in device editor.

8.1.4 Rermarks - PCS INTUS 1600

- The former PCS INTUS 1600 reader is no longer supported.
- The former PCS INTUS 1600 reader is replaced during upgrade by the generic LBUS (=IBPR) reader, therefore the device configuration is valid again.
- The INTUS 1600 reader can have different firmware versions.
- The ready may work but cannot be guaranteed, because it no longer can be tested (former hardware is not available).

8.1.5 Achieving EN 60839 (AMS 5.5)

Achieving EN 60839 access-control standards: EN 60839 is a family of European international standards for the hardware and software of Intrusion detection and Access

control systems. Measures to ensure compliance of your Access control system with EN 60839 are described in the AMS Configuration online help. The following remarks did not make the editorial deadline for the online help, therefore they are listed here:

- The status of all entry points, primarily doors and windows, must be monitored. For example, through electric contacts.
- A system with mobile access cards only is not intended for EN certification.
- The Multi User Manager application is not part of the certification.
- If the applications Mobile Access and or Multi User Manager are installed, the AMS no longer meets the EN 60839 requirements.

8.1.6 Windows system time change

If Windows time is changed manually, the AMS system should be closed and the Windows time should be also set on all clients before starting AMS again. It is strongly advised to use a valid NTP time server on all computers including additional MACs and AMS Clients.

8.1.7 Backup file location

AMS Backup directory with all files are now found in documents directory "`<documents>\Backups\<timestamp>`" of the operator who started the backup.

Note: If the SQL Server database is found on another computer, the database '*.bak' files are found on the remote SQL Server backup folders. In such case, both directories should be saved, and are required for the restore application.

8.1.8 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.

8.2 Intrusion

8.2.1 Intrusion event limitation:

Receiving of events and alarms depends on the network and system availability. Events and alarms are not repeated if the Intrusion panel was offline at that time, therefore AMS will 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 (maximum 2 million events can be stored in the event database)
- SQL Server 2019 Standard version: 150 events/sec

Note: AMS can process maximum of 100 events/sec. overall from the Access Control System, such as, door open/close, access, audit trail and so on. If Intrusion integration is used, one point change can create 3 events (e.g. Point shorted, Area not ready to arm, Point state changed).

8.2.2 Intrusion cardholder synchronization limitation:

- In combination with intrusion, these default card definitions are supported:
 - 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 a 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).

8.3 MapView and Services

8.3.1 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.

Workaround: To refresh the states, coldstart the system (DMS, MAC, AMCs, Readers etc.) to force a MAC-switch.

#389803 Swipe Ticker - Picture takes a longer time to display

Under heavy server or network load, the cardholder pictures in the Swipe Ticker might not display immediately.

8.4 Dialog Manager

8.4.1 Guard tour and SimonsVoss readers

Readers from SimonsVoss are not supported for guard tours.

8.4.2 BioIPconfig Tool

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

8.5 Microsoft SQL Express

Microsoft SQL Express limitation:

SQL Express DB installed with AMS 5.0 and later supports up to 2 million events. The default retention time is 30 days. Old events are deleted if:

- DB is at 2.000.000 events.
- retention period has expired.

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

Adjustments can be done in the json file - Folder: C:\Program Files (x86)\Bosch

Sicherheitssysteme\Access Management System\Events API

File: appsettings.json

Warning

- Before editing json files, do a backup copy of this file.
- Be aware not to destroy the json format.

Configurable attributes:

DaysToKeep= 0-9.999 (Number of days. Default: 30 days) (0=unlimited).

MaxDbEvents= 10.000-99.999.999 (Default: 2.000.000, this is the maximum for MSDN Database).

DeletionSize= 5.000-1.000.000 (Max number of elements to delete in one step advised value= 10000).

all values have to be entered without the dot "."

Example with default values:

```
"EventsApiOptions": {  
  "DaysToKeep": 30,  
  "ExpireFrequency": 60,  
  "MaxDbEvents": 2000000,  
  "DeletionSize": 10000,  
  "DeletionTimeout": 300  
},
```

8.6 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 enrollment 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, 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 Visitor Management: 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.

8.6.1 Visitor Management 5.0.1**#395279 PNG file format for picture not supported**

The file format PNG for user photographs is not supported in Visitor Management. 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 issue occurs when a Peripheral Device (PD) certificate is missing from the internal Firefox certificate store.

Workaround:

1. Open the **Certificate Manager** tool from wWndows (on the machine where the PD tool has been installed).
2. Open **Trusted Root Certification Authorities**.
3. Select the PD certification named:
`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 certificate into the internal Firefox certification store.
7. Restart Firefox.

#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. Fo example, 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.

Workaround: **Exp. Departure** and **Time** should not be empty. If it is left empty, the default state is that the visitor will be invalid after 8 hours.

8.7 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.

8.8 SimonsVoss

#206393 Sequence monitoring mode 1 does not function correctly when a SimonsVoss lock goes offline

In Access Sequence Monitoring mode 1, monitoring should be deactivated when a lock goes offline. This deactivation is currently not functioning for SimonsVoss SmartIntego devices.

#202508 While deleting a cardholder assigned to a SimonsVoss lock, the error message has limited information

While deleting a SimonsVoss lock, the error message states 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, 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 the device is an SimonsVoss reader type.

8.9 OTIS

#356015 OTIS: ConfigBrowser: You can create only 6 DES devices

Configuration is limited to 6 DES and 2 DER devices.

8.10 OSS-SO Configuration

#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 might also indicate a network problem. Please check the connection to the network and restart your browser.

8.11 Hardware supported by Windows 11

8.11.1 Readers

The following readers were tested successfully under Windows 11:

- Delta 1200 MF BKL USB. DELTA 1200 MF BKL USB /Admitto ARD-EDMCV002-USB (Old readers do not work)
- LECTUS enroll 5000 MD. Admitto Mifare Classic and DesFire EV1
- HID omnikey reader, HID reader for iClass/Prox cards
- ARD-FPBEW2 Fingerprint reader BEW2 (TCP/IP)
- PegaSys MF BC USB. Pegasys Mifare USB Reader (windows 11 approval from manufacturer pending).

8.11.2 Hardware

The following hardware were tested successfully under Windows 11:

- Signature Pad over USB
- Web cam over USB
- Canon camera over USB (using CANON EDSDKv131712. See compatibility list below)
- Idemia biometric devices (using Morphomanager 16.3.0)
- Scanner for ID documents: ARH Combo, ARH Osmond.

List of CANON cameras supported by EDSDK EDSDKv131712 (device list provided by CANON):

- PowerShot V10 (Firmware version 1.1.0 or later)
- EOS R100
- PowerShot ZOOM (Firmware version 1.2.0 or later)
- EOS R50

- EOS R8
- EOS R6 Mark II
- EOS R10
- EOS R7
- EOS R3
- EOS Kiss M2 / EOS M50 Mark II
- EOS R5
- EOS R6
- EOS Kiss X10i / EOS Rebel T8i / EOS 850D
- EOS Ra
- EOS-1D X Mark III
- EOS M200
- EOS M6 Mark II
- EOS 90D
- PowerShot G7X Mark III
- PowerShot G5X Mark II
- EOS Kiss X10 / EOS Rebel SL3 / EOS 250D / EOS 200D II
- EOS RP
- PowerShot SX70 HS
- EOS R
- EOS Kiss M / EOS M50
- EOS Kiss X90 / EOS REBEL T7 / EOS 2000D / EOS 1500D
- EOS REBEL T100/EOS 4000D / EOS 3000D
- EOS M100
- * EOS 6D Mark II
- EOS Kiss X9 / EOS Rebel SL2 / EOS 200D
- EOS Kiss X9i / EOS Rebel T7i / EOS 800D
- EOS 9000D / EOS 77D
- EOS M6
- * EOS M5
- * EOS 5D Mark IV
- EOS-1D X Mark II
- EOS 80D
- EOS Kiss X80 / EOS Rebel T6 / EOS 1300D
- EOS M10
- * EOS 5DS
- EOS 5DS R
- EOS 8000D / EOS REBEL T6sEOS 760D
- EOS Kiss X8i / EOS REBEL T6i / EOS 750D
- EOS M3
- * EOS 7D Mark II
- EOS Kiss X70/EOS 1200D/EOS REBEL T5/EOS Hi
- EOS M2
- * EOS 70D EOS Kiss X7 / EOS 100D / EOS REBEL SL1
- EOS Kiss X7i / EOS 700D / EOS REBEL T5i

- EOS-1D C
- EOS 6D
- EOS M
- * EOS Kiss X6i / EOS 650D / EOS REBEL T4i
- EOS-1D X
- EOS 5D Mark III
- EOS Kiss X50 / EOS REBEL T3 / EOS 1100D
- EOS Kiss X5 / EOS REBEL T3i / EOS 600D
- EOS 60D
- EOS Kiss X4 / EOS REBEL T2i / EOS 550D
- EOS-1D Mark IV
- EOS 7D
- EOS Kiss X3 / EOS REBEL T1i / EOS 500D
- EOS 5D Mark II
- EOS 50D
- EOS DIGITAL REBEL XS / 1000D/ KISS F
- EOS DIGITAL REBEL Xsi / 450D / Kiss X2
- EOS-1Ds Mark III
- EOS 40D
- EOS-1D Mark III

*Remote capture functions are not supported. Cameras not useful in AMS to take photos.

Note: RAW images are not supported by default.

EOS Digital SDK with EDSDK V13.17.10 supports the following cameras:

- PowerShot V10
- EOS R100
- EOS R8
- EOS R50
- EOS R6 Mark II
- EOS R7
- EOS R10
- EOS R3
- EOS M50 Mark II
- EOS R5
- EOS R6
- EOS Ra
- EOS 850D
- EOS-1D X Mark III
- EOS M200
- EOS 90D
- EOS M6 Mark II
- PowerShot G5 X Mark II
- PowerShot G7 X Mark III

- EOS 250D
- EOS RP
- PowerShot SX70 HS
- EOS R
- EOS M50
- EOS 2000D
- ** EOS 4000D
- * EOS M100
- EOS 6D Mark II
- EOS 200D
- EOS 77D
- EOS 800D
- * EOS M6
- * EOS M5
- EOS 5D Mark IV
- EOS-1D X Mark II
- EOS 80D
- EOS 1300D
- * EOS M10
- EOS 5DS
- EOS 5DS R
- EOS 760D
- EOS 750D
- EOS 7D Mark II

*Remote shooting functions are not supported (These cameras are not useful in AMS to take photos)

**There is further notice about compatibility with AC adapter. Please contact the camera manufacturer for more information.

If the target EOS model is not listed above, please refer to EDS DK API Reference (list above from EDS DKv131712).