Access Management System (AMS) version 6.0
Release notes

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

Document history.

Version	Description
1	2025-04 Readme of Access Management System 6.0
2	2025-05 Review

Table of Contents

1 Installation Notes

1.1 Documentation

Due to potential updates, the technical documentation for this product in the online catalog is considered the authoritative source. Consult the online catalog for the latest and most accurate technical information.

1.2 Server requirements

Hardware and software requirements for an AMS server:

Supported operating systems (standalone or client/server mode) Installations of AMS on other operating systems may succeed, but are entirely without warranty	• Windows 11 Professional and Enterprise 24H2 (x64) • Windows 11 Enterprise LTSC 24H2 (x64) • Windows Server 2019 (Version 1809 LTSC) (64bit, Standard, Datacenter) • Windows Server 2022 (64bit, Standard, Datacenter) • Windows 10 Enterprise LTSC 2021 (x64) **Ensure that the latest Windows 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 10 (gen 13 recommended)
	• 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
	• 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	• Windows 11 Professional and Enterprise 23H2 (x64) • Windows Server 2019 (Version 1809) (64bit, Standard, Datacenter) • Windows Server 2022 (64bit, Standard, Datacenter) • Windows 10 Professional and Enterprise 22H2 (x64 • Windows 10 21H2 LTSC (x64) **Ensure that the latest Windows updates are installed.**
Minimum hardware requirements	• 60 GB of free hard disk space • Graphics adapter with 256 MB RAM • A resolution of 1280x1024 • At least 32 k colors • 1 Gbit/s Ethernet card

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	• Windows 11 Professional and Enterprise 24H2 (x64) • Windows 11 Enterprise LTSC 24H2 (x64) • Windows Server 2019 (Version 1809 LTSC) (64bit, Standard, Datacenter) • Windows Server 2022 (64bit, Standard, Datacenter) • Windows 10 Enterprise LTSC 2021 (x64) **Ensure that the latest Windows updates are installed.** **Note:** with AMS Pro, 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

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 1280x1024
	  ○ 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: Widescreen 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 MSQL 2019

For new installations of AMS 6.0, if a pre-existing SQL Server instance is not detected, SQL Server 2019 Express edition will be installed.
During an upgrade from AMS 3.0.1, if the existing SQL Server 2017 instance was initially deployed by the AMS installer, it will be automatically upgraded to SQL Server 2019.
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 6.0

Update to AMS 6.0 requires a valid SMA. Licenses can be updated at Bosch Remote portal.
Upgrade from 1.0 to 2.0 as described in the AMS 2.0 installation guide.
Upgrade 2.0 to 6.0 as described below.

1.6 Update of AMS 2.0 and later to AMS 6.0

1. Create a backup of the old AMS installation.
2. Update directly to AMS 6.0 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 after 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 6.0

- 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

1.7.1 Locale setting required for non-English installations.

The AMS application relies on the Windows system locale to properly display non-English characters (including those used in languages like Arabic and Russian, as well as Latin characters with diacritics).

If the system locale is not correctly configured, AMS reports and dialog controls may display placeholder characters instead of the intended text.
Note: On operating systems utilizing multi-language packs, installing a language pack does not automatically modify the system locale. Manual configuration of the system locale is required.

For example, in the case of Arabic:

- **Regional Settings** > **Administration** > Language **for non-Unicode programs** > **Change system locale** and select an Arabic locale.
- Verify that the SQL server collation is set to “Arabic_CI_AS”.

Alternatively, run the 'Set-WinSystemLocale' cmdlet with Administrator permissions. For example, Set-WinSystemLocale "ar-SA" sets the System Locale to 'Arabic (Saudi Arabia)'.

1.7.2 AMS Setup languages and Operating Systems

The language of the AMS Setup UI uses the current UI culture of the OS. For example, if the UI culture of the OS is Portuguese Brazil (pt-BR), the AMS Setup UI will be also in Portuguese Brazil. The current UI culture of the OS can be checked by the PowerShell command *Get-UICulture*. If the OS UI culture does not match the locale of the AMS Setup exactly, then the AMS Setup UI will be in English (en-US).

1.8 Compatibility List of Software Components for AMS 6.0

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	6.0	AMS Media Package Folder: AddOns/Advanced/BioConfig
IPConfig (AMC)	1.14.3	AMS Media Package Folder: AddOns/Standard/AccessIpConfig
SDK Version	6.0	AMS Media Package Folder: AddOns/Advanced/API
MAC Installer	6.0	AMS Media Package Folder: AddOns/Advanced/MultiMAC
Key Management Tool	2.8.2	AMS Media Package Folder: AddOns/Advanced/ReaderConfigTool
Inrusion RPS API	2.2.27914	AMS Media Package Folder: AddOns/Advanced/Intrusion-RPS-API
Milestone PlugIn	5.5	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 6.0

2.1 Single Sign on (=SSO)

AMS 6.0 supports integration with external identity providers (IdPs), enabling users of those IdPs to authenticate as operators within AMS. Initially, these operators have no assigned privileges. User profiles can be associated with these operators in two distinct ways:

- **Role-Based Profile Mapping (External IdP Managed Profiles):** When in a user profile is designated as "managed by external IdP”– checkbox available on a user profile, it will be automatically mapped to an operator if the value of the "roles" claim in the operator's IdP token exactly matches the profile's role attribute.
- **Manual Profile Assignment:** If a user profile is not designated as "managed by external IdP," it can be manually associated with the operator after their first authentication.

Upon successful configuration of an external IdP, a new login option will be presented within the AMS login dialog.
Note: When integrated with BIS 6.0, the external identity provider should be configured within BIS 6.0. AMS leverages BIS 6.0's single sign-on (SSO) functionality for authentication.

2.2 Report Management

Report Management was developed to optimize the process of creating and customizing time and attendance reports, while also ensuring that all reports maintain a consistent and professional branding. With its user-friendly interface and integration with existing data sources from Access Management System, administrators can easily personalize reports to meet their organization's specific branding guidelines. Additionally, the feature's multilanguage support and security measures make it a valuable tool for global teams looking to maintain a cohesive brand identity across different regions and languages.

2.3 Mobile Access, Credential Management, Visitor Management

2.3.1 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.

When 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.

2.3.2 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.

2.4 Access Management System

2.4.1 Client Server security improved

The client server connection protection was improved. Programs using old SDKs (=ACE API) cannot connect to the new AMS server anymore. They must be updated with the new SDK files provided in AddOns directory of AMS setup. More information can be found in API description and the compatibility overview.

2.4.2 Licensing in DialogManager

Upon expiration of the 5-hour demo license, initiating the Dialog Manager will only present the license acquisition dialog. After a valid license is successfully applied, the Dialog Manager will restart, activating all licensed functionality. The Support and Maintenance Agreement (SMA) end date is also presented within the license information.

2.4.3 Events in AMS

The events are no longer saved in SQL database. Instead, event files are saved on hard disk on the AMS server backend. The max number of events is restricted to hard disk space now instead of the SQL database limitation.
The events are saved in %programdata%\Bosch\BAS\Databases\Bosch.Events.API.
As default the events of the last 365 days are saved there. The configuration how many events are saved can be configured in the appsettings.json of “Events API” (Path: Programfiles(x86)\Bosch Sicherheitssysteme\Access Management System\Events API).
Make sure to provide enough hard disk space otherwise the AMS backend will stop if the free space gets critical.

2.4.4 Key cabinet

Changes in the Deister key cabinet interface:

- The Deister key cabinet terminals are supported including encryption. The encryption must be enabled in Deister config tools and in the AMS Deister configuration dialog.
- Cardholder cards of type HID 26, 35 and 37 bits are integrated now. The configuration in the registry must be set in the server what card type shall be transferred to the Deister terminal. In the dialog manager the cards must be enrolled with the same type too.
- The cabinet types “FlexxDD” and “Flexx16” are available as new second version variants “FlexxDDv2” and “Flexx16v2” to support newer Deister cabinet hardware but with different interface. These new cabinets are shown in the dialog manager key cabinet overview as 4 rows with 8 keys instead of 2 rows with 16 keys.

Known limitation:
Some of the cabinet types do not support the “release key” command from the dialog manager dialog.

2.4.5 AMS 6.0 is ready for BIS 6.0

The AMS 6.0 is prepared to work with the BIS 6.0 where no access is integrated anymore. The old ACE database of older BIS\ACE Versions can be integrated in the AMS 6.0 with a backup\restore and an AMS 6.0 repair installation to upgrade the old database.
We recommend upgrading older BIS\ACE Versions to 5.0 before migration to AMS 6.0.
Known limitation:

- Hierarchical BIS/ACE Version are not supported in AMS 6.0. Probably AMS 6.1 will support hierarchical systems too.

- Operator passwords cannot be copied to AMS so these operators must get a new password by the Administrator. The Administrator can be set during AMS installation as Admin of the AMS server.
- The BIS can use “SQL Availability Groups”, but the AMS 6.0 setup does not allow such database connections. After the installation the configuration how, the AMS connects to an SQL server can be changed in registry to connect to such “SQL Availability Groups” too. After a restart of the AMS system the new configured SQL connection is used.

2.4.6 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.

2.4.7 Single Sign on Operator compatibility

The Access API (=SDK) interface found in AddOns directory does not support SSO operators. Only operators created in AMS directly and configured with the right permission can be used within the SDK. The same for all internal operators needed for software packages like ImporterExporter, VisitorManagement, CredentialManagement and so on.

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 panels extensions

The following B/G intrusion detection panels are supported by AMS 6.0:

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

4 Optional post-installation steps

4.1 Security recommendations for user authorizations

On the AMS server, define only Windows users who are 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_\Loggifier\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 6.0

#430471 AMS 5.2: Badge designer on Client - layouts cannot be saved.

#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 will change the person's original card-validity period if the person class is locked to one authorization.

#432492 Supported Deister devices
The AMS does support Deister terminals with firmware 2.8 or later.

#448969 AMS 6.0: strange error message from device editor when Demo mode expires.
If 5 hours demo mode expires and dialog manager is started, then the operator must set license first.

#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.

#452946 AMS 6.0: 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.

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/ à TWAIN and WIA Driver

6.5 Milestone Xprotect

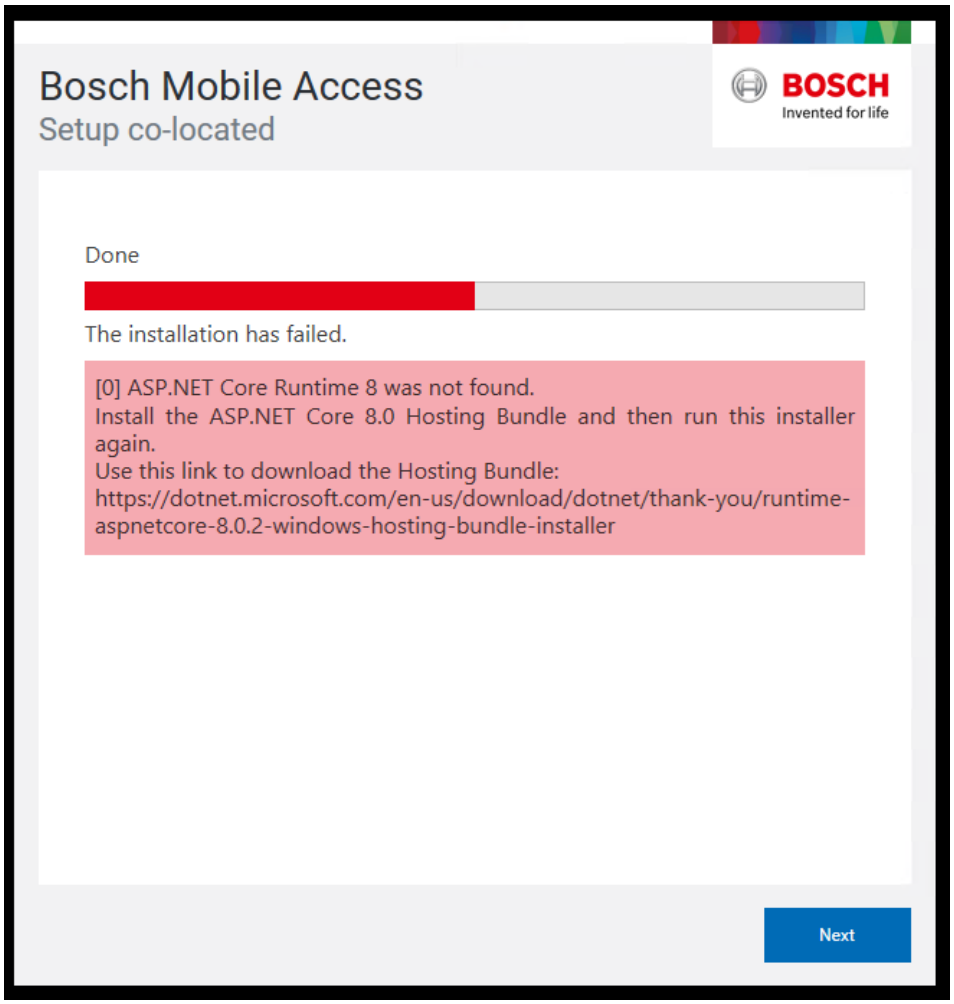
Supported XProtect versions: Corporate 2020 R1 and higher.

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

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

7.2 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.
Certificates – 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 6.0). Then, run the latest MA Backend installer (shipped with AMS 6.0). 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 Not supported features

Starting from Access Management System 6.0 onwards, Multi User Manager is no longer supported.

8.1.2 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.

8.1.3 Clean up after installation

We updated Erlang OTP for Windows. The old version will still be present on the AMS Server but can safely be removed. This step is not required but will keep the system cleaner.
To remove the old version:

In the Windows start menu select Add or remove programs
Search for “Erlang”

8.1.4 Select version 24.0.5 and click “Uninstall”Product Api

The configuration of the Product Api changed. During an upgrade, the configuration will automatically be parsed into the new format, so no action is needed.
For new installations make sure to use the new format:

<AmsInstallationDir>/AMS - Identity Provider/appsettings.Extension.AccessControlApi.json

```
{
 "OpenIdRegistrations": {
  "Applications": {
   "<OPERATOR-USERNAME>": {
    "ClientSecretByOperator": "<OPERATOR-USERNAME>",
    "AllowClientCredentialsFlow": true,
    "AllowedScopes": [ "ProductApi”]
   }
  }
```

}
}

8.1.5 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 is not available. It is available in English only.

8.1.6 Known bugs in AMS 6.0

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

11 - Door n forced open alarm
12 - Door n left open
13 - Reader shows access granted
14 - Reader shows access denied
23 – Messages to readers
24 – Messages to devices
25 - remote control Function set

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

#349902 AMCIPConfig note.
AMCIPConfig no longer allows access with the correct password after running for several hours.
Workaround: Always close the tool after use.

#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.

#447067 AMS 6.0: 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.

#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 6.0: 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 must be done before upgrading.

#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 log off then the bug will not occur.

#455223 Wrong output consumption count
In some cases, the available used outputs are not calculated correctly in device editor.

8.1.7 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 readay may work but cannot be guaranteed, because it no longer can be tested (former hardware is not available).

8.1.8 Achieving EN 60839 (AMS 6.0)

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.
- If the applications e.g. Mobile Access are installed, the AMS no longer meets the EN 60839 requirements.

8.1.9 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.

8.1.10 Backup file location

AMS Backup directory with all files is 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 a case, both directories should be saved, and are required for the restore application.

8.1.11 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 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 an 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.

8.5.1 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.

8.6 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.

8.7 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.

8.8 OTIS

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

8.9 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.

8.10 Hardware supported by Windows 11

8.10.1 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).

8.10.2 Hardware

The following hardwares 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 are 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 EDSDK API Reference (list above from EDSDKv131712).