Release notes for Access Management System (AMS) Version 1.0

Bosch
Sicherheitssysteme GmbH
Postfach 1111
85626 Grasbrunn
Germany
Visitors:
Robert-Bosch-Ring 5
85630 Grasbrunn
Tel +49 89 6290 -0
www.boschsecurity.com

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

13 December 2018

Table of Contents:

1 Installation Notes

1.1 Supported operating systems

AMS runs on the following operating systems:

	AMS Server	AMS Client
Windows 10 (64 bit, Enterprise LTSB - Version 1607)	No*	Yes
Windows 10 (64 bit, Pro)	No*	Yes
Windows Server 2016 (64bit) Standard or Datacenter	Yes	Yes
Latest drivers and OS updates are highly recommended.		

(*) But Server on Windows 10 is possible with manual configuration.

1.2 Server

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

Minimum hardware requirements	Intel i5 processor with at least 4 physical cores
	• 8 GB RAM (32 GB recommended)
	• 200 GB of free hard disk space (SSD recommended)
	• Graphics adapter with
	  ○ 256 MB RAM,
	  ○ a resolution of 1280x1024
	  ○ at least 32 k colors
	• 1 Gbit/s Ethernet card
	• A free USB port or network share for installation files

1.3 Client

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

Minimum hardware requirements	• Intel i5 processor (4 Core) or greater • 8GB RAM • **20**GB free hard disk space • Graphics adapter with 1920 x1080 resolution, 32k colors, 256MB dedicated memory with DirectX 11 or later • 1 Gbit/s Ethernet card • Free USB port for Dialog Reader or camera

2 Optional post-installation steps

2.1 Retention Time of System Events

The retention time for system events is configurable. The default is set to 30 days, which means that events that are older than 30 days are deleted automatically.
To specify a different value, follow these steps:

1. Start the registry editor (press [Windows]+[R], enter "`regedit.exe`")
2. In the registry editor Navigate to path `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Micos\SPS\DEFAULT_\Loggifier\SysKeep`
3. Double click value "`@value`" (shown in the right pane) and enter a new value.

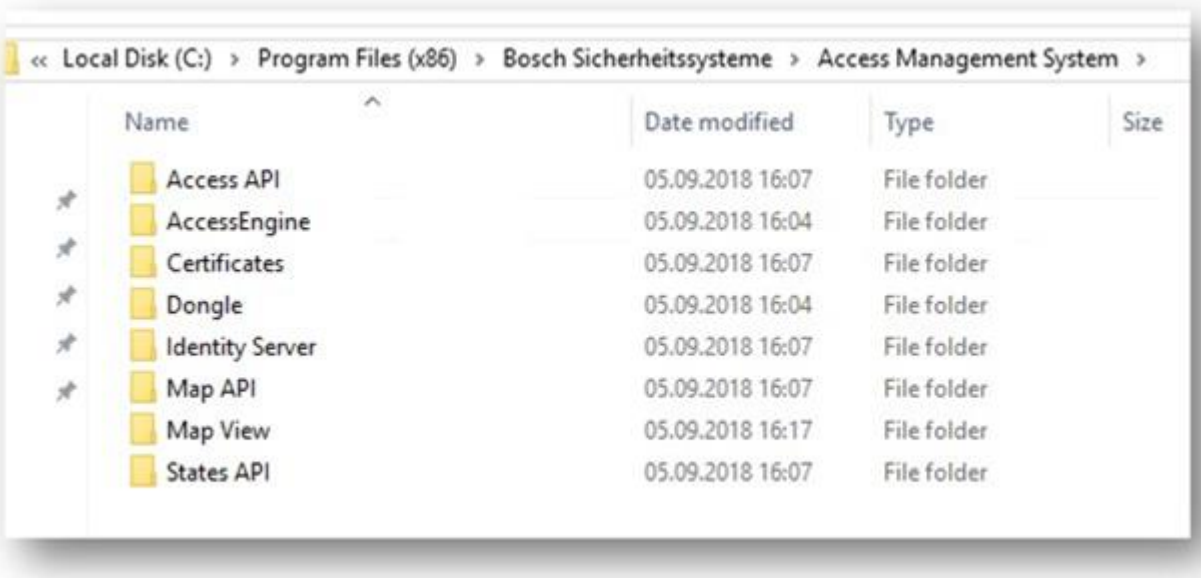
Note that the retention time has a major impact on the size of the backup files being created. So please choose a value that is as low as possible.

2.2 Trace Level of Services used by Map View

The services used by the Map Viewer Application use a logging interface that is independent from the logging of the other backend services. This section describes how this logging can be configured.

The logging configuration can be found on the server in the individual API folders in a file called `appsettings.json`. If installed under the default directory, this file can only be changed by user with administrative rights.

- Access API
- States API
- Map API
- Identity Server



The *appsettings.json* can be opened with a text editor and the relevant logging configuration section is as follows:

Default logging configuration:

```
"Serilog": {
    "MinimumLevel": {
        "Default": "Debug",
        "Override": {
            "Microsoft": "Information",
            "System": "Warning"
        }
    }
}
```

We use Serilog for logging. It defines the following levels:
Verbose, Debug, Information, Warning, Error and Fatal.
The "MinimumLevel" settings ("Debug" in the screenshot) applies to all log sources (i.e. which component that is writing the log).

The "Override" section applies to specific log sources. For example in the screenshot, from components whose namespace starts with "Microsoft" only messages of level "Information" or higher will be logged. Similarly from .NET

framework (i.e. namespace starting with “System”), only messages of level “Warning” or higher will be logged.

A minimal configuration would be:

```
“Serilog”: {
    “MinimumLevel”: {
        “Default”: “Fatal”
    }
}
```

This is likely to result in almost no log entries, except for the last error that crashed the runtime. There is no switch in the API to completely disable logging.

3 Known limitations in AMS 1.0

3.1 Languages

3.1.1 Settings required for Arabic installations

AMS requires the Windows System Locale to be set to Arabic. Otherwise AMS reports and some dialog controls will show invalid characters instead of Arabic characters.

This is especially important if the operating system was not originally Arabic and the support for Arabic language was added by installing a language pack. Installing a language pack does not update the System Locale, so it must be set manually:

- Regional Settings / Administration / Language for non-Unicode programs / Change system locale: select an Arabic language

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

3.1.2 AMS languages and operating systems

Language of AMS installation has to be the same as the one of the Operating System. The only exception is Turkish. There the OS has to be in English. Please note that also Client and Server Installations should have the same language as otherwise the texts in the clients will contain a mix of languages.

3.2 Remarks and limitations regarding Map View and services

3.2.1 Configuration of Critical events

The template "`CriticalAccessEvents_Default.csv`" for the configuration of critical events is stored locally under `%ProgramData%Bosch Sicherheitssysteme\Access Management System\Config` on each computer where a Map View application is installed. The template is created when the Map View application is started the first time. A custom configuration can be derived from this file by creating a copy called "`CriticalAccessEvents.csv`".
Please note that the custom configuration is applicable for a given client machine, i.e. the file "`CriticalAccessEvents.csv`" has to be created on each machine and is specific to this machine. This means also that if two machines run a MapView and should have the same configuration the file "`CriticalAccessEvents.csv`" has to be created on one and copied to the other machine. The custom configuration

"CriticalAccessEvents.csv" is loaded by the Map View on the start of the Map View application and defines:

a) Which events are to be shown in the Critical event Viewer and the criticality of the event
b) Which events are not be shown

The file "CriticalAccessEvents.csv" consists of a list of events that have the following structure: *<id>;<symbol>;<category>*
where <category> can be one of:
None | Warning | Alarm
In order to change the file "CriticalAccessEvents.csv" open the file in a text editor such as Notepad. Events that are not defined or defined as "None" in "CriticalAccessEvents.csv" will not be shown in the critical event bar of the Map View.
Events that are defined as alarms, e.g. "16777730;ACS_DOOR_OPEN_TOO_LONG;Alarm" will be shown as an alarm in the critical events bar. An example of an adapted "CriticalAccessEvents.csv" is shown in Figure 1.

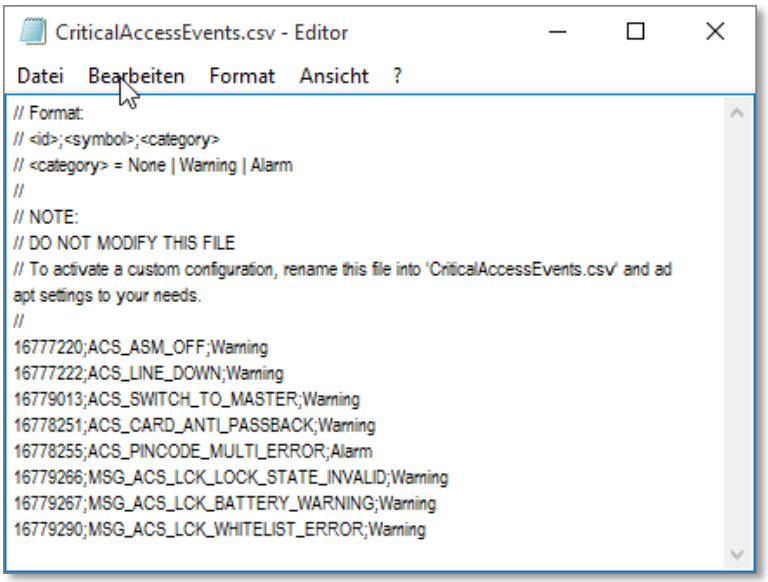


Figure 1: Adapted CriticalAccessEvents.csv

Please note that the template as well as the custom configuration files are accessible to any operator with the proper permissions and could be modified/corrupted intentionally/accidentally.

3.2.2 **Initial States**

Please note that the states initially displayed by the system immediately after installation are not necessarily correct. The reason for this behavior is that the system stores the states of the devices during operation, and on startup displays the states last seen. However some device states might have changed between the last shutdown and the current installation of the AMS Software.

An example of this behavior is where MAC and Twin MAC are initially both displayed with a slave symbol. Only after a MAC-switch are the correct master and slave symbols displayed.
One workaround, to refresh the states, is to coldstart the system (DMS, MAC, AMCs, Readers etc..) and so force a MAC-switch.

3.2.3 AMS Services

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

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

A workaround for this issue is to start the services manually or perform a reboot.

3.3 AMS Client Limitations

Make sure that the latest signature pad firmware is installed on the corresponding client machine. The firmware installation file is located within the delivered AddOns folder (Firmware File: signotec:TWAIN_8.0.0.exe). The latest driver can be downloaded from https://www.signotex.com/download/treiber/twain-wia-treiber/

3.3.1 Guard tour and SimonsVoss readers

Readers from SimonsVoss are not supported for guard tours.

3.3.2 Access Ipconfig Tool

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

3.3.3 Temporary Cards

The report state for “temporary cards” is not shown in as much detail in reports as it is in the cards dialog (#215890).

3.4 SQL Server

The SQL Server has to be run on the same machines as the AMS server. It is not possible to have an SQL Server on a machine other than the AMS Server.

4 Additional Notes

4.1 Tools in Start Menu (Server)

The following tools are provided in the Access Manager Menu:

4.1.1 Access IP Config

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

4.1.2 Configuration Collector

The *Configuration Collector* is a tool which is installed on the AMS server. It guides you through collecting configuration information which is being stored into a ZIP file. This ZIP file can then be sent to Bosch Technical Support for troubleshooting.
The Configuration Collector provides an online help which can be invoked from any of its tab pages.

4.1.3 DB Password Change

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

4.1.4 Backup

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

4.1.5 Restore

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

4.2 Web Service

The Access Management System optionally provides a Web Service which can be used to retrieve specific data.
By default, the web service is disabled. To enable the service, follow these steps:

1. On the server, open the following file in a text editor: `\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\AccessEngine\AC\Cfg\ PrcTable.tbl`

2. Locate the following section:

```
;set /executable=websrv-1.exe
;set /ready=0
;set /parameter=""
;set /restartlimit=3
;set /type=normal
;set /errorReset=100
;set /exitNumber=5000
;set /parameter=""
;add
```

3. Remove the semicolons at the beginning of each line
4. Save the file and restart the server.

After you have done the changes, the web service is enabled. More details about using and configuring the service can be found in '`AddOns\ACE\AdditionalHTML-Docs`' on the AMS installation medium.

4.3 Forms Dialog

The AMS Client provides a dialog to edit templates for printable forms e.g. an acknowledgement form.
The dialog can be found in the menu **Configuration > Settings,** dialog item **Forms**.
This dialog can be used to import and export custom HTML forms. The AMS has two forms pre-installed which can be exported and customized.

5 Known Bugs and Workarounds for AMS 1.0

#194304 Login window hangs in an endless initialization loop - hanging process
The ACE-Standalone login window hangs after waking the client machine from sleep mode. This only occurs when hosting the backend as a virtual machine on the same physical machine.
Workaround: Restart the dialog manager process.

#194306 Uninstall routine does not remove all files
Some files are not removed from the installation folder after executing the supported uninstall routine:
- A few log files and xml files within the binary folder.
- Layout folders containing badge-designer layouts.

#198012 Event Viewer: Low performance under load scenarios
The "Event Viewer" takes a long time to filter for specific events (in some scenarios more than 5 minutes). This low performance is only observed with large amounts of event data, or when the system under a heavy workload.

#204170 DMS and MAC background processes cause hangs
Special trace and troubleshooting processes (DMS/MAC) are always started on the server in the background. These processes prompt for user interaction on a regular basis (blinking icon in the task bar). This interaction is not working on Windows Server 2016 and causes temporary hangs.
The system hangs for around 5 minutes when you click the blinking icon/ interaction request.

#210697 Password dialog should be more detailed
The dialog rejects passwords as too short, but does not specify the minimum length.
The minimum length is 6 characters.

#214209 after upgrade/repair setup the Administrator password is reset to default
After an upgrade of the AMS from an older to a newer version the Administrator password is reset to the default password. This is intended behavior to allow recovery after loss of the administrator password (see also #214216 What is the workaround in case customer forgot his administrator password?).

#184154 Fingerprint Reader: Wiegand green LED is OFF after red LED is triggered by AMC (for some card types)
In Wiegand mode for the card types MIFARE Classic CSN, iClass, EM, Prox the green LED is not shown, even if set permanent open by the controller, if an unauthorized card is used.

#199275 & #202554 Instability of the AMS dialog manager due to enrolling card in ACE dialogs
This instability can happen only if no dialog reader is selected.
Workaround: Select a dialog reader to perform enrollments.

#199503 Instability of the AMS dialog manager when trying to record a fingerprint when the reader has lost its network connection
Workaround: For fingerprint enrolment the enrolment reader must be online.

#202508 While deleting a cardholder assigned to a SimonsVoss lock, the error message has limited information
While deleting a SimonsVoss lock, the error message says only that it is assigned to a SmartIntego whitelist authorization, but not which cardholders are affected.

#195988 Fingerprint reader BioEntryW2: Disable reader beep does not mute the sounder completely
Even if the beep for the reader is disabled in the configuration, the sound generated by the fingerprint reader is still audible when the fingerprint is read successfully.

#206393 Sequence monitoring mode 1 does not function correctly when a SimonsVoss lock goes offline
In Access Sequence Monitoring mode 1, monitoring should be deactivated when a lock goes offline. This deactivation is currently not functioning in the case of SimonsVoss Smartintego devices.

#206241 SimonsVoss deletion of a whitelist generates no confirmation
If a whitelist is deleted from a SimonsVoss device, the user receives no confirmation that the command has executed successfully.

#206988 SimonsVoss delete construction WhiteList
If the construction whitelist was used before being integrated into AMS then the MAC may not be not able to delete the construction whitelist.
Workaround: Delete the construction whitelist manually.

#209743 MAP: SimonsVoss commands without function

The following SimonsVoss commands, provided by the Map View, are without function:

Door commands:

- Grant Access Inbound -> Command without function (message GRANTIN SET=1)
- Grant Access Inbound Extended -> Command without function (message GRANTIN SET=2)
- Grant Access Outbound -> Command without function (message GRANTOUT SET=1)
- Grant Access Outbound Extended -> Command without function (message GRANTOUT SET=2)

Reader commands:

- Grant Access Extended -> Access normal (Message GRANTAC SET=2) Extended = Handicapped mode. Not implemented for SimonsVoss
- Enable Manual Mode -> Command without function, sets value ENTRMANL=1
- Disable Manual Mode -> Command without function, sets value ENTRMANL=0

#210928 Incorrect state icon in Map View

If “Permanent Unlock” (long-term unlock) is set for a door, and subsequently manual mode is set for that door, then the state of the door is not shown correctly when manual mode is disabled.

-- End of document --