

# Release notes for Building Integration System (BIS) Version 4.5

Grasbrunn  
2017-10-26

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

## Table of Contents:

1	Installation Notes .....	2
1.1	Supported operating systems .....	2
1.2	Server .....	2
1.3	Client .....	3
1.4	Updating BIS to Version 4.5 .....	4
2	New features in version 4.5 .....	5
2.1	Platform .....	5
2.2	Access Engine (ACE) .....	9
2.3	Video Engine .....	15
3	Issues resolved in BIS version 4.5.....	16
3.1	Platform .....	16
3.2	Access Engine (ACE) .....	17
4	Known limitations in BIS version 4.5.....	18
4.1	Platform (BIS) .....	18
4.2	Access Engine (ACE) .....	19

## 1 Installation Notes

### 1.1 Supported operating systems

The BIS system runs on these operating systems:

	<b>BIS Login Server</b>	<b>BIS Connection Servers</b>	<b>BIS Client</b>	<b>BIS VIE Client</b>
Windows 7 SP1 (32 bit) Professional or Enterprise	Yes	Yes	Yes	Not recommended
Windows 7 SP1 (64 bit) Professional or Enterprise	Yes	Yes	Yes	Yes
Windows 8.1 (32 bit) Professional or Enterprise	No	No	Yes	Not recommended
Windows 8.1 (64 bit) Professional or Enterprise	Yes	Yes	Yes	Yes
Windows 10 (64 bit, Pro or Enterprise LTSB)	Yes	Yes	Yes	No
Windows 10 (32 bit, Pro or Enterprise LTSB)	No	No	Yes	No
Windows Server 2008 R2 SP1 (64bit) Standard or Datacenter (*)	Yes	Yes	Yes	No
Windows Server 2012 R2 SP1 (64bit) Standard or Datacenter (*)	Yes	Yes	Yes	No
Windows Server 2016 (64bit) Standard or Datacenter (*) English and German alone	Yes	Yes	Yes	No
(*) Not as domain controller				

### 1.2 Server

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

Supporting Software on Windows and Windows Server	<ul style="list-style-type: none"> <li>• IIS 7.0 or 7.5 for Windows 7 and Windows 2008 Server R2</li> <li>• IIS 8.5 for Windows 8.1 and Windows 2012 Server R2</li> </ul>
---------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Operating Systems	<ul style="list-style-type: none"> <li>• IIS 10 for Windows 10 and Windows 2016 Server</li> </ul> <p>Note: IIS is not necessary on BIS connection servers</p> <ul style="list-style-type: none"> <li>• Internet Explorer 9, 10 or 11 in compatibility mode</li> <li>• .NET for various operating systems:                             <ul style="list-style-type: none"> <li>○ On Windows 7 and Server 2008: .NET 3.51 and .NET 4.0</li> <li>○ On Windows 8.1 and Server 2012: .NET 3.51 and .NET 4.5.1 (includes .NET 4.0)</li> <li>○ On Windows 10: .NET 3.51 and .NET 4.6.1 (includes .NET 4.0)</li> <li>○ On Windows Server 2016: .NET 3.51, .NET 4.6.1 and .NET 4.6.2 (includes .NET 4.0)</li> </ul> </li> </ul> <p>Latest drivers and OS updates are highly recommended.</p>
Minimum hardware requirements	<ul style="list-style-type: none"> <li>• Intel i5 processor or higher. Intel Core 2 Duo 2.66 GHz (4 Core) or greater</li> <li>• 4 GB RAM (8 GB recommended)</li> <li>• 80GB of free hard disk space</li> <li>• VGA graphics adapter with 256 MB RAM, a resolution of 1280 x 1024 and at least 32k colors</li> <li>• 100 Mbit/s Ethernet card (PCI)</li> <li>• 1 free USB port or network share for installation</li> </ul>

### 1.3 Client

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

Supporting Software	<ul style="list-style-type: none"> <li>• ASP.NET</li> <li>• Internet Explorer 9, 10 or 11 in compatibility mode (Note: The SEE client requires IE 9.0)</li> <li>• .NET for various operating systems:                             <ul style="list-style-type: none"> <li>○ On Windows 7 and Server 2008: .NET 3.51 (for Video Engine with DiBos),and .NET 4.0</li> <li>○ On Windows 8.1 and Server 2012: .NET 3.51 (for Video Engine with DiBos),and .NET 4.5.1 (includes .NET 4.0)</li> <li>○ On Windows 10: .NET 3.51 and .NET 4.6.1 (includes .NET 4.0)</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>○ On Windows Server 2016: .NET 3.51, .NET 4.6.1 and .NET 4.6.2 (includes .NET 4.0)</li> </ul>
Minimum hardware requirements	<ul style="list-style-type: none"> <li>• Intel i5 or higher, Intel Core 2 Duo 2.66 GHz (Dual Core) or greater</li> <li>• 4GB RAM (8 GB recommended)</li> <li>• 20GB free hard disk space</li> <li>• Graphics adapter with 1280 x1024 resolution, 32k colors, 256MB dedicated memory with OpenGL 1.2 or later</li> <li>• 100 Mbit/s Ethernet card</li> </ul>
Additional minimum requirements for VIE (Video Engine) clients	<ul style="list-style-type: none"> <li>• No Windows Server operating systems</li> <li>• No Windows 10</li> <li>• Intel i5 processor or higher</li> <li>• For camera sequencing, virtual matrix or Multiview add 4GB RAM</li> <li>• Latest video drivers are highly recommended. Use the Windows dxdiag tool to make sure drivers are no more than 1 year old.</li> </ul>

## 1.4 Updating BIS to Version 4.5

The setup program identifies any currently installed version of BIS.

- If setup detects a version equal to or older than BIS 3.0 then the upgrade process is aborted. Setup will prompt you for permission to remove the older and install the new version, but preserving the existing customer configurations.
- If the setup program identifies a currently installed version of 4.0 or higher, then the update will proceed as normal, preserving all customer-specific files and configurations on the same computer. These will be available again upon successful completion.
- Before upgrade BIS to a newer version be sure that all events are written to database.
- Check folder Mgts\EventlogEntries
- Upgrade from previous BIS version with SQL server 2005 will not work, need to upgrade to SQL server 2008 or later before upgrading BIS

## 2 New features in version 4.5

**Note:** The limitations cited in this document are the maximum values that we have tested at the time of publication. They do not necessarily reflect the absolute maxima for the system.

### 2.1 Platform

#### 2.1.1 Audit trail

The Audit trail feature in BIS enables operators to investigate the changes made to the BIS system installed. The Audit trail feature is configured and operated from the BIS Configuration Browser; it tracks both changes made in the BIS Configuration Browser and changes made to files in the configuration folders.

**Note:**

- All the audit trail records are stored in the SQL database, if the SQL database is full or the SQL service is down, then no changes are trailed. It is the customer's responsibility to ensure that the SQL service is running before making any configuration changes.
- Audit trail uses the web service to communicate with the SQL service, hence the customer should ensure that IIS and web service are running before making any configuration changes

**Limitation:**

- 3<sup>rd</sup> party OPC server configuration changes are not trailed
- Configuration changes under tools menu are not trailed
- Access right configuration is not possible for Audit trail configuration and Audit trail report pages, all the BIS Configuration browser user can configure and view Audit trail

#### 2.1.1.1 Audit trail of configuration file and folder changes

When the audit trail is activated, then a windows service named A1\_BisAuditTrailWatcherService becomes active and monitors all the changes in the customer configuration folders and run-time configuration folders. Any additions, modifications or deletions are recorded in the audit trail database.

**Limitation:**

- Only the names of the modified files and folders are recorded, not the modified content.

**Note:**

Due to the large number of files copied, the performance of the Audit trail feature is adversely affected by the creation, loading and unloading of whole configurations. Consider suspending the Audit trail feature before making such large-scale changes.

### 2.1.1.2 Audit trail report generation

Audit trail report is viewed from the configuration browser, the following information can be retrieved:

- On what configuration the change was made
- In which BIS menu and screen the change was made
- What kind of change was made
- When exactly the change was made and
- by which operator
- The values of the changed fields, both before and after the change

#### Limitations:

- Due to the usage of SSRS report generation initial loading of report will take few minutes, but subsequent report generation will be faster
- If the SQL service is down, Audit trail report will not work. Remedy: close the configuration browser, start the SQL service, start the configuration browser and open the Audit trail report
- Exports to Excel spreadsheets will fail if any retuned value exceeds the maximum Excel cell size of 32767 characters. Workaround: Export to Word or PDF instead.
- Wild-card characters such as %, \* ,etc... are not supported in search strings
- If any color value is modified then report will show the color values in that color itself. To search for color values use their numeric values as by the [Microsoft HTML Color table](#).
- For date time filtering only operator '=', '<' and '>' are supported. The operator '=' handles only dates in the format (DD/MM/YYYY) but the '<' and '>' operators can also handle date-times in the format (DD/MM/YYYY HH:MM)
- A maximum of 6 filter conditions is possible, and the only logical conjunction supported is AND.
- Filter conditions are not saved between sessions
- For better performance, the filter should contain a minimum of 3 characters
- The logical NOT operator is not supported
- Password changes are trailed with the old password and the new password displayed as (literally) "Old Password" and "New Password".

#### Note:

- Audit trailing is not limited to current configuration. Changes that affect the current configuration are marked **System** in the **Configuration** column. Changes to other configurations on the disk contain the name of the configuration folder in the **Configuration** column. Therefore to search for changes to the current configuration, use the word **System** in the **Configuration** column.

### 2.1.1.3 Audit trail records deletion

To save storage space, the administrator of the system can configure the retention time of the audit data, and whether the purging of outdated information should be performed automatically by the BIS system or manually by an operator

The **Purge expired records** button will be available for execution only if expired records are present in the database

An **Automatic purge** function is available to delete expired records every day at a scheduled time (HH:MM). If automatic purge is configured then a job named **AuditTrailDeleteScheduler** will be started to execute at the configured time to delete all the expired records

**Note:**

If the “AuditTrailDeleteScheduler” task fails or is stopped manually, it will not be started automatically until the automatic purge is reconfigured. To do this, clear and reselect the check box **Schedule an automatic purge** in the BIS Configuration browser under **System > Audit trail configuration**. No more expired records will be purged until then.

### 2.1.2 Event log negated filters

Many filter settings can be logically negated by selecting the **NOT** check box next to their hyperlinks. A negated filter will allow all records to pass that do not have any of the values contained in that filter.

For example, a filter is defined to catch all records where the Operator is OP1 or OP2.

- Where the **NOT** check box is cleared, only records that contain the Operator name OP1 or OP2 will pass the filter.
- Where the **NOT** check box is selected, only records that do not contain the Operator name OP1 or OP2 will pass the filter.

**Limitation:**

- Visible columns and Access Engine are not negatable, because both contain multiple filter criteria.

### 2.1.3 Event log filter result back and forward navigation

This feature is to move back and forth within the current session’s history of search results. When you do this, the name of the filter used, and the date and time of its execution, is displayed along with the search button.

**Limitation:**

- Navigating back or forward will re-apply the filter and get the currently matching result, it is not possible to modify the old filter or save it.
- The filter result is displayed in the currently configured columns, not necessarily the columns that were configured at the time the filter was first used.
- Only the last 10 filters are stored. The 11<sup>th</sup> and subsequent filters will always overwrite the oldest filter that is currently in the store.

### 2.1.4 Configuration collector support for Connection servers

Configuration collector is a tool used to collect the information required by technical support for their investigations. This tool can now be used on Connection servers, not just the main BIS server. Detail information about purpose and usage of the tool can be found in the tool's online help, or in the BIS installation folder (`Mgts\Tools\BugReporter`)

### 2.1.5 HTML5 support

Support for HTML5 will be available from this BIS version onwards. A tool is available on the installation media under `Tools\HTML5Converter` to convert the existing HTML4 files to HTML5, with an option to roll back if required. See the BIS Configuration help file for more details.

#### Limitation:

- Only BIS system HTML4 files are converted, any files added by user are not converted
- Any modifications to BIS JavaScript files will be overwritten by the conversion. Make backups of the modified JavaScript files and reapply the modifications after running the converter tool.
- Future versions of BIS will also assume HTML4. For this reason the converter tool will need to be run after every BIS upgrade, if the configurations have already been converted to HTML5.
- In Multi BIS system, both provider and consumer servers must use the same version of HTML. Installations using mixed HTML versions are not supported
- Do not run the tool from the MgtS folder or a non writeable location

#### Potential Risks:

- HTML5 does not support encrypted java script, so non-encrypted java script files will be used.
- Unqualified or malicious use of the tool can seriously damage a BIS installation.
- Non-encrypted java script files are susceptible to misuse by unqualified or malicious computer users.

In order to prevent unauthorized, unqualified or malicious use it is recommended that the HTML5 converter tool be deleted from the BIS system after use, and kept only on the installation media.

### 2.1.6 AVIOTEC camera support

The AVIOTEC camera has an intelligent analytics feature that detects flame and smoke. The camera is supported by this and later BIS versions, and detected flame and smoke events can be used to generate BIS alarms. Prerequisite: enable advanced tamper detection in the BVIP OPC server. Other tamper-detection functions (image too dark, too noisy, or too bright) are not supported by this version.



### 2.1.7 BIS SDK with sample application

A help file will be provided by this and later BIS versions, which will list the supported SDK options in BIS, and ways to use the SDK. A simple sample application is also provided, which can be used to familiarize oneself with the implementation and usage.

### 2.1.8 BIS Client logout without prompt

A new BIS Client COM method is added to log a user off the BIS Client without prompting for the confirmation. See the Client Object Model (COM) document for more details.

### 2.1.9 Windows server 2016 support

This version of BIS can also be installed on Windows Server 2016.

#### Limitations:

- During BIS installation, the setup dialog wrongly shows Windows Server 2016 as Windows 10. This has no impact on the operation.
- If BIS client is used on Windows Server 2016, then a pop-up window will request the user to acknowledge a possible security issue. Extensive testing has revealed no such security issue.
- If a BIS client is running under Windows 2016 on a consumer server in a multi-server BIS environment, then the provider server's IP address must be added as a trusted site of the browser. If not added then the Action Plans and Miscellaneous Documents will fail to display on the BIS client of the consumer machine.
- Supported languages: Currently Windows Server 2016 is only supported on the following languages
  - English (BIS and ACE)
  - German (BIS and ACE)
  - Traditional Chinese (BIS)
  - Polish (BIS)
- Access Engine under Windows Server 2016 does not support external USB devices such as signature pads, cameras and Enrollment readers.

## 2.2 Access Engine (ACE)

### 2.2.1 Host Secure Support

The communication between AMC and MAC is enhanced by AES encryption and a dynamic session-based key exchange. This prevents man-in-the middle and replay attacks on this communication channel.

With release BIS 4.5, this host secure protocol is enabled by default.

#### Note:

In ACE 4.5, all AMCs need to be updated to firmware version 6x32 or later for 4R4, and version 3751 for Wiegand AMCs.

**Upgrading AMC firmware with the enhanced Access IP Config Tool:**

If the AMC is already connected to a BIS of version 4.5 or higher, the AMC runs in host secure mode and cannot be upgraded by the tool directly.

To upgrade the firmware with the Access IP Config tool, perform the following steps first:

1. Disable the AMC configuration in the Access Engine
2. Execute a hard reset on the AMC.

**2.2.2 Enrollment readers supported**

The following enrollment readers are currently supported by BIS ACE 4.5

- LECTUS enroll 5000 MD
- BoschRdr
- IBprRdr
- ProxPro
- RDR-7080AFK-BOS
- DELTA 1200 MF RS232 BKL
- DELTA 1200 HI1 RS232 BKL
- DELTA 1200 LE RS232 BKL
- DELTA 1200 Prox RS232 BKL
- DELTA 1200 iClass RS232 BKL
- DELTA 1200 LE BKL USB
- DELTA 1200 HI1 BKL USB
- DELTA 1200 MF BKL USB
- ARD-1200EM-USB
- ARD-FPBEW2
- PegaSys MF-BC-USB
- PegaSys MF-SN-USB
- PegaSys HITAG-BC-USB
- PegaSys HITAG-SN-USB
- PegaSys Legic-BC-USB
- PegaSys Legic-SN-USB
- PegaSys LegicAdvant-BC-USB
- PegaSys MF-Desfire-BC-USB
- PegaSys MF-Desfire-SN-USB

**Note:** as of this version, access readers can also be used for enrollment purposes.

**2.2.3 Integration of fingerprint readers**

The ACE supports the integration of the BioEntry W2 Fingerprint Reader (ARD-FPBEW2-IC).

The fingerprint reader integration includes:

- Enrollment of the fingerprints of a cardholder in the person and visitor dialogs.
  - Up to 10 fingerprints per person can be enrolled
  - Any enrolled fingerprint can be classified as a duress finger.

- Fingerprints in the form of hash values, not pictures, are stored in the SQL database.
- The fingerprint reader can also be used to enroll cards, that is, as a normal enrollment reader.
- At least one other fingerprint reader will be required as an access reader with the additional fingerprint check.
- The FPBE W2 fingerprint reader can be connected via OSDP v1/v2 or Wiegand interface to an AMC.
- Many cards are supported: EM, MIFARE Classic, MIFARE DESFire EV1, HID Prox, iClass.
- One of the card types must be selected on first configuration with Access IP Config Tool (see below).

**Supported cards:**

- EM
- MIFARE Classic  
**Note:** reads CSN or Bosch code
- MIFARE DESFire EV1  
**Note:** reads CSN or Bosch code
- HID Prox 26 bit / 37 bit  
**Note:** Enrollment of 37 bit cards is NOT supported
- HID iCLASS 26 bit / 35 bit / 37 bit / 48 bit
- HID iCLASS SE 26 bit / 37 bit  
**Note:** reads SIO (Secure Identity Object)
- HID iCLASS Seos 26 bit / 37 bit  
**Note:** reads CSN

**Limitations:**

For iClass/Prox and EM only the standard card types are supported (see ACE card definition dialog). This excludes customized code lengths and non-standard facility/card-number separation.

If the door is set to long-term unlock, then the fingerprint reader's LED is set to green for the duration of the setting.

If a cardholder presents an unauthorized card to the reader, the LED is set to red and does not revert to green. This occurs only with MIFARE Classic CSN, iClass, EM and Prox cards.

**2.2.4 New Access IP Config Tool to configure the BioEntry W2 fingerprint reader**

The Access IP Config Tool has been enhanced to configure the new BioEntry W2 fingerprint readers.

Functions of the tool with respect to the FPBE W2 fingerprint reader are:

- Scanning for FPBE W2 fingerprint reader in the same subnet.

- Configuration of static IP settings if DHCP (the default setting) is not required.
- Configuration of fingerprint readers as either Enrollment or access readers
- Configuration of card types such as EM, MIFARE, HID Prox, and HID iClass.
- Configuration of the reader for OSDP or Wiegand protocols
- Upgrade of reader firmware
- Diagnostics for LED and buzzer
- Resetting readers to default settings

**Limitations:**

- After a cold start of a fingerprint reader wait for 3 minutes. Further changes to the reader settings can fail if the device had not completed its cold start.
- If the reader's settings fail to change, execute a reset through the Access IP config tool and repeat the configuration.
- If the tool is installed in a language other than English or German the toolbar for upgrading the firmware may fail to appear.  
Workaround: Select the upgrade function from the menu instead of the toolbar.
- Configure a device by IP address:  
If the function *Manual Fingerprint IP Settings* is selected to configure a fingerprint reader, the interface configuration cannot be set back from Wiegand to OSDP.  
Workaround: Reset the device. The default setting after reset is the OSDP interface.
- The stand-alone version is only available in English.

**Notes:**

To install the Access IP Config tool on a stand-alone PC without BIS client or BIS server installation:

- 1) Prerequisite software:  
If not already installed on the target PC, install the Microsoft .NET Framework 4 Redistributable Package and the Microsoft Visual C++ Redistributable Packages  
Packages can be found on the BIS installation medium under:  
\_Install\3rd\_Party\VC2015  
\_Install\3rd\_Party\dotNET\4.0
- 2) Installation and start:  
Copy the folder \_Install\AddOns\ACE\AccessIPConfig to the target PC  
Start the program by executing the file `AccessIPConfig.exe`

**Changing an existing fingerprint reader configuration.**

Before changing the configuration of a fingerprint reader which is currently in use, using the Access IP Config tool, first stop BIS and ACE services.

### 2.2.5 New Badge designer

ACE Card Personalization has been completely redesigned, avoiding the need for special configuration and setup. All web cameras and Canon cameras found on the local machine are usable in the ACE dialogs.

The new Badge Designer supports variables to trigger different backgrounds and contents, so that one badge layout can serve for multiple cardholder types or classes of persons. The layouts are saved to a gallery in `MgtS\AccessEngine\AC\Layouts` from where they can be reused and customized in the Badge Designer tool as desired. Cardholder images are found under `MgtS\AccessEngine\CardHolderImages\` on the ACE server.

Barcodes and QR-codes are also supported.

The print form layout contains a further example of how all person-related fields (even the customer-defined ACE personnel data fields) can be used in an html file and printed from the ACE dialog. All form files of type `.html` are found under `MgtS\AccessEngine\AC\Forms` on the ACE server and are selectable from the ACE client in the **Print badges** dialog.

#### Limitations:

- The badge layouts of previous ACE versions are not supported by the new badge designer, however, the old badge designer executable is still available under `MgtS\AccessEngine\AC\BIN` path so the old layouts can be viewed for reference.
- If multiple web cameras of the same type are attached to the same computer the **Print badges** dialog may select a different default web cam in the next session.
- Up to 10 ACE customer-defined personnel data fields can be included in a new badge layout. These must be marked as **Reportable**.
- If the Badge Designer is to be used on a remote workstation, the layout files need to be copied to the ACE server manually.
- Support for TWAIN scanners has been discontinued

### 2.2.6 Customizable Persons dialogs with up to 80 custom fields.

ACE has been enhanced to provide up to 80 custom fields for personnel data. The placement of these fields is also fully customizable, and existing system-defined fields can be renamed, hidden, moved or replaced by custom fields.

Customer fields can be of different data formats such as:

- Text
- Date-time and Time
- Check box
- List box

Custom fields have additional properties such as:

- Mandatory – whether or not the operator must supply a value for the field
- Unique – whether the value must be unique
- Reportable (1..10) – whether the value may appear on reports or badges
- Position and length – on which dialog the field should appear, and where.

Up to 10 custom fields, marked as **Reportable**, can be used in the ACE report dialogs as search and filter criteria.

**Limitations:**

- Existing personal data is not automatically converted if the value or datatype are subsequently modified.  
For example: at the moment when the **Unique** property of a custom field is set there could already be non-unique data for that field in the database. The data within that custom field is checked for uniqueness only at the moment when the person data is saved.
- The Import/Export tool can only insert and update custom fields marked as **Reportable**.
- No more than 10 Reportable custom fields are supported.
- Custom fields, their values and their properties are not replicated in hierarchical systems.

**2.2.7 Enhanced guard tour.**

The existing feature guard tour has been enhanced by a new set of functions:

- The granularity of the time interval between readers has been changed from minutes to seconds. This allows a more precise planning and execution of a guard tour.
- A patrol can be initiated manually or by a pre-defined schedule.
- The pre-assignment of up to five guard-cards is now supported.
- New patrol states have been added for use in BIS **Associations**.

**Limitations:**

- Each patrol requires the assignment of at least one guard card.
- If multiple guard cards are assigned to a patrol the card used to start the patrol at the first reader must be used throughout the patrol.

**2.2.8 Readers connected to AMCs can now be used for enrollment**

BIS 4.5 supports the use of access readers, connected to an AMC, for card enrollment, so that the reader can be used for both access control and enrollment alternately.

**Recommendation:**

For ease of configuration, use only readers of door models 1 or 3 for enrollment purposes.

**Limitation:**

Only one access reader per workstation can be configured.

**2.2.9 Additional card definitions**

“HID 48 Corporate 1000” and “56 bit CSN” for MIFARE DESFire EV1 are now supported card types.

### **2.2.10 Person data overview**

A data sheet can be customized to contain all the person data you require.

The reference document serves as template to print all data of a person. Duplicate this file and put the copy in the directory `C:\MgtS\AccessEngine\AC\Forms`.

This template was created using Microsoft Word. After editing ensure that the file is saved in Unicode (UTF-8) format.

## **2.3 Video Engine**

### **2.3.1 Video SDK 6.11.0060 Support**

The VIE Multiview Bosch Video Cameo now uses Video SDK 6.11.0060

A list of devices tested with the 6.11 SDK is available from your Bosch sales representative.

## 3 Issues resolved in BIS version 4.5

### 3.1 Platform

#### **BIS Manager – database capacity displayed incorrectly**

The **Event log** tab of the BIS Manager now displays correct values for database capacity and SQL server version. Changing the retention time will have no impact on the database size settings.

#### **BIS Event log - Attribute tab opens too slowly.**

The **Attributes** tab of the Event log filter will no longer hang even if there are more than 100,000 records in the attributes table. The display now processes the data in chunks of 100 records per page.

#### **BIS Client - Dead link found, Links of Graphic removed without message to User**

If the configuration browser loads a known (previously loaded) graphic file from which a link has been removed, then a message informs the user that a “dead link” has been removed. The details of which link, and which location was involved, will now appear correctly in the configuration browser log file.

#### **BIS Event log - Crash after new installation**

The event log **Attributes** tab has been modified to prevent a potential access violation.

#### **BIS Event log - Clear event log of unused attributes**

The backup script has been made more efficient, so that when a backup of the event log database is triggered with the **Delete** option, then unused attributes are deleted along with event log entries.

#### **BIS Event log - Error message in Report server on some ACE devices**

Device names containing commas are now properly displayed in the Event log.

#### **BIS Client - Execute URL command exits the BIS client unexpected**

The handling of the **Open URL-Window** command has been corrected to prevent possible failures of the BIS client.



## **3.2 Access Engine (ACE)**

### **ACE Configuration - Door model 14b Entry in disarming authority is empty.**

The Configuration Browser has been corrected to prevent the value of disarming authority from appearing empty.

### **ACE API - visitor phone (PHONEPRIVATE) value is updated**

The value PHONEPRIVATE is now updated correctly by the API.

### **ACE PegaSys - Improved writing of PegaSys card information on AMC**

Improved update and delete procedures for PegaSys cards.

### **ACE Device Edit - Outputs of AMC2-4R4 controlled by internal logic set after power cycle**

Output signals now recovered correctly after a power cycle.

### **ACE - Renaming a division with Unicode Characters in name is supported**

Division names containing Unicode characters are now editable.

### **ACE MAC - MAC switching to master mode improved**

MAC switching to master mode has been improved to better handle the disconnection of an R-MAC from the network.

### **ACE MAC - OPC tree view updated, if MAC or RMAC is disconnected**

MAC status in OPC tree improved, state is correctly toggled between online/offline.

### **ACE Client - Logging at Client :Configbrowser.log added**

On a client installation, setting the debug level to standard is correctly logged.

### **ACE Client - Areas support in non-hierarchical systems**

The update of area information in non-hierarchical systems has been improved.

### **ACE MAC - Improved MAC Installer, if port is left blank**

MAC installer is improved to allow a blank field for port number.

### **ACE Dialog Manager - Improved screen layout of Dialog Manager for large screens**

For large screens the Dialog Manager is shown full screen mode.

## 4 Known limitations in BIS version 4.5

### 4.1 Platform (BIS)

#### **.NET 4.6 is not supported**

If additional software is installed on the BIS server, and this software includes .Net 4.6, uninstall .Net 4.6 and upgrade to .Net 4.6.2.

#### **SQL Server Express 2012 supports database size up to 10 GB, but BIS does not**

In this version of BIS, for SQL Server Express 2012 and above, it is not possible to set the database size to the maximum 10 GB from the DB Admin tab (only up to 4 GB is allowed). If required, use the SQL Server Management Studio.

#### **Untranslated strings**

The following strings are available only in English and German language, in other languages they are not localized, some of these are state strings and some are display strings.

1	NOT
2	System
3	ADD
4	MODIFY
5	DELETE
6	FIELD
7	OPERATION
8	<UNUSED>
9	WINDOWS
10	BIS
11	CLEARED
12	SELECTED
13	Error: Audit trail is not success

## **4.2 Access Engine (ACE)**

### **Russian setup reports errors**

The default special day “new year” and the day models for “holiday/none” are not correctly imported. The default entries are missing on first installation, but can be created by the BIS user.

### **DlgMgrAX.log is not available in BIS 4.5**

The DlgMgrAX.log is created on Workstations. On the server the debug log is written to the ConfigurationBrowser.log file instead.

### **Export Tool: of Person.ReserveX fields not supported in BIS 4.5**

If a database field Person.Reserve1 to Person.Reserve10 was used in the previous BIS versions, the export of these fields is not supported in BIS 4.5.

### **AMC using serial connection**

Due to improved high-security encryption, AMC protocols Wiegand and OSDP no longer support serial connections to the host.

### **Online help in traditional Chinese**

The help button (labeled with a question-mark) fails to start online help from the traditional Chinese user interface of ACE.