Security Systems

Release notes for Building Integration System (BIS) Version 4.6

Grasbrunn
2018-07

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

Table of Contents:

1 General

1.1 Supported operating systems

The BIS system runs on these operating systems:

	BIS Login Server	**BIS Connection Servers**	**BIS Client**	**BIS VIE Client**
Windows 7 SP1 (32 bit) Professional or Enterprise	Yes	Yes	Yes	Not recommended
Windows 7 SP1 (64 bit) Professional or Enterprise	Yes	Yes	Yes	Not recommended
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, Enterprise LTSB - Version 1607)	Yes	Yes	Yes	Yes
Windows 10 (64 bit, Pro)	No	No	Yes	Yes
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 (*)	Yes	Yes	Yes	No
(*) Not as domain controller				

1.2 Server requirements

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

Supporting Software on Windows and Windows Server Operating Systems	• IIS 7.0 or 7.5 for Windows 7 and Windows 2008 Server R2 • IIS 8.5 for Windows 8.1 and Windows 2012 Server R2 • IIS 10 for Windows 10 and Windows 2016 Server

	Note: IIS is not necessary on BIS connection servers
	
	• Internet Explorer 9, 10 or 11 in compatibility mode *
	• .NET for various operating systems:
	  ○ On Windows 7 and Server 2008: .NET 3.51 and .NET 4.0
	  ○ On Windows 8.1 and Server 2012: .NET 3.51 and .NET 4.5.1 (includes .NET 4.0)
	  ○ On Windows 10: .NET 3.51 and .NET 4.6.1 (includes .NET 4.0)
	  ○ On Windows Server 2016: .NET 3.51, .NET 4.6.1 and .NET 4.6.2 (includes .NET 4.0)
	
	Latest drivers and OS updates are highly recommended.
	If HTML5 is enabled in IE 11, then Video will not be displayed

Minimum hardware requirements	• Intel i5 processor (4 Core) or greater • **8** GB RAM or greater • **80**GB of free hard disk space => 200 GB (SSD recommended) • VGA graphics adapter with 256 MB RAM, a resolution of 1280 x 1024 and at least 32k colors • 1 Gbit/s Ethernet card (PCI) • 1 free USB port or network share for installation

1.3 Client requirements

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

Supporting Software	• ASP.NET
	• Internet Explorer 9, 10 or 11 in compatibility mode *
	(Note: The SEE client requires IE 9.0)
	• .NET for various operating systems:
	  ○ On Windows 7 : .NET 3.51 (for Video Engine with DiBos),and .NET 4.0
	  ○ On Windows 8.1 and Server 2012: .NET 3.51 (for Video Engine with DiBos),and .NET 4.5.1 (includes .NET 4.0)
	  ○ On Windows 10: .NET 3.51 and .NET 4.6.1 (includes .NET 4.0)
	
	  ○ On Windows Server 2016: .NET 3.51, .NET 4.6.1 and .NET 4.6.2 (includes .NET 4.0)

Minimum hardware requirements	• Intel i5 processor (4 Core) or greater • 8GB RAM • **20**GB free hard disk space • Graphics adapter with 1280 x1024 resolution, 32k colors, 256MB dedicated memory with OpenGL 1.2 or later • 1 Gbit/s Ethernet card
Additional minimum requirements for VIE (Video Engine) clients	• No Windows Server operating systems • Intel i5 processor or higher • For camera sequencing, virtual matrix or Multiview add 4GB RAM • Latest video drivers are highly recommended. Use the Windows dxdiag tool to make sure drivers are no more than 1 year old.

1.4 Updating BIS to Version 4.6

The setup program identifies any currently installed version of BIS.

- If setup detects a version 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 3.0 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 upgrading BIS to a newer version be sure that all events are written to the database.
  Check folder Mgts\EventlogEntries
- Upgrade from previous BIS version with SQL server 2005 will not work. Upgrade to SQL server 2008 R2 or later before upgrading BIS.

1.5 Security advice: BIS Version 4.6.

- **For reasons of data security it is recommended that you change the default password of the BIS generated user Mgts-Service immediately after installation, using the ChangePassword Tool.**

2 BIS version 4.6

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 OPC UA

OPC UA is the next generation of OPC technology. OPC UA is a more secure, open, reliable mechanism for transferring information between servers and clients. It provides more open transports, better security and a more complete information model than the original OPC, "OPC Classic". From the version 4.6 onwards, BIS supports communication with remote devices via OPC UA. The connection to the OPC UA server is made directly from the BIS login server, and not via a connection server.

Secure use of OPC UA

1) OPC UA is, by default, not secured; if a secure OPC UA connection is required, use either HTTPS or certificate-based authentication.

2) The BIS setup program and Configuration Browser place certificates for OPC UA server in the folder `<BIS installation drive>:\Mgts\PKI`
   For security, allow only "BISUsers" and "Administrators" to access this folder. For example, use the following procedure:
   a. Right click the PKI folder.
   b. From the context menu, select "Properties" and then the "Security" tab.
   c. Click the buttons "Advanced" and then "Change permissions"
   d. Select "Disable inheritance" and select "Convert inherited permissions into explicit permissions on this object"
   e. Select each group except "BISUsers" and "Administrators" in the Principal column, and remove them all.
      Only "BISUsers" and "Administrators" should remain in the permissions table.

3) If the file `\MgtS\ConfigurationBrowser\BoschST.BIS.ConfigurationBrowser.exe.config"` has been modified since the last installation, then the upgrade installation will not adapt it to work with OPC UA. In this case, make the following changes manually:

   Add the two elements below after the `<Configuration>` tag in the `.config` file:

```
<configSections>
  <section name="Bis.Opc.Ua.Client" type=
"Softing.Opc.Ua.Sdk.ApplicationConfigurationSection,Softing.Opc.Ua.Sdk.Core"/>
</configSections>


<Bis.Opc.Ua.Client>
  <ConfigurationLocation xmlns=
"http://opcfoundation.org/UA/SDK/Configuration.xsd">
    <FilePath>BisOpcUaClient.Config.xml</FilePath>
  </ConfigurationLocation>
</Bis.Opc.Ua.Client>
```

Performance:

- If only OPC Classic is used, then the existing limitation on number of detectors remains unaffected (200,000).
- If OPC UA is used alone, or if mixed with Classic, then the limitation on the total number of detectors (Classic and UA) is 120,000.
- The existing maximum number of events per second (400) pertains unchanged for both OPC UA and Classic.

2.2 AVIOTEC Sound alarm

The special sound-detection feature of the AVIOTEC camera can now be used within BIS to generate events.

2.3 Security improvements

2.3.1 Active Directory and LDAP

Active Directory (AD) users can log in from BIS client or BIS manager. AD users and their AD groups need to be associated with a BIS authorization in the BIS configuration. The users' access to BIS pages is governed by the privileges of their AD group.

2.3.2 Change-password tool

The ChangePassword tool is used by system administrators to manage the passwords of BIS-internal system users, that is both Windows operating system (OS) and SQL users. This single tool supersedes all previous tools, and must be used to change any BIS-internal system users. No additional steps are required.

2.3.3 Custom SQL account

When installing BIS on an existing SQL Server instance, any database username that has the same privileges as the `sa` user may be selected. It is no longer necessary to select the `sa` user itself.

2.3.4 Running BIS without Windows Administrator privileges

To enhance security, a set of scripts is provided that will enable the BIS administrator users `Mgts-Service` and `Mgts-SSRS-Viewer` to run without Windows administrator privileges. These scripts will work for any BIS version.

2.4 Resolved issues in BIS

Logging stopped if available disk space is less than 10% of total capacity (# 127154)
Logging will now continue if less than 10% of the total hard disk, or less than 1 GB is remaining.

Access Engine event log problem (# 183721)
Event log window can now be opened from Access Engine dialog without problems, even after changing the default filter.

Backup and restore do not contain user.crp (# 185450)
BIS client passwords are stored in user.crp file, and when the backup is done, these passwords also backed up, but it will not be restored automatically upon restore. The file will remain in the backup location. If previous passwords are required, the file must be restored manually.

Restored BIS Event log do not work (#196211)
The scripts used for restoring a BIS event log have been corrected.

Show Logbook from ACE dialog with more than one badge (#170523)
The BIS event log now correctly displays all data records for persons having more than one card: If no card number is entered, then all records for that person are displayed. If a card number is entered, then only events concerning that card.
The Event log uses unique internal IDs to distinguish between persons having the same first name and surname.

BIS freezes when a configuration loaded twice within a short time (#159725)
The Load button in the BIS manager is now disabled until BIS starts completely or for 6 minutes (6 minutes is the maximum time attempted by BIS server to connect to OPC servers).

2.5 Known limitations in BIS

If HTTPS is enabled for Audit Trail and an upgrade (modify/repair) is performed, the service will not start (#199188)
Workaround: Disable HTTPS before upgrade and enable HTTPS after upgrade.

Updating the BIS-ACE fails due to A1_BISAudit TrailWatcherService (#188581)
Workaround: Stop the task AuditTrailFilewatcherservice.exe in Task manager before upgrading BIS ACE.

Prerequisites window shows "Windows 10" on installation of Windows Server 2016 (#181056)
Workaround: Ignore the message and proceed.

The setup program does not check if there is enough space for the 4GB audit trail database (#178991)
Workaround: check disk space manually before starting setup.

BVIP OPC scanning of devices may be incomplete for newer devices (#186441)
Workaround: Manually edit the BVIP `.config` file and rescan.

NET 4.6 is not supported. (#169416)
If additional software is installed on the BIS server, and that software includes .NET 4.6, then remove .NET 4.6 and upgrade to .NET 4.6.2

3 ACE

3.1 New office features

3.1.1 Fingerprint identification with BIoEntry W2 reader in offline mode

The ACE supports identification, and verification of identities, by fingerprint, using the BioEntry W2 Fingerprint Reader (model ARD-FPBEW2-IC), also if the network is not available (i.e. in offline mode). In this case the fingerprint patterns are read from the reader.

Previously implemented fingerprint modes are not affected and remain available.
The AccessIPConfig tool has been enhanced to configure the new FPBE W2 fingerprint reader and the AMC. A setup is now available to install this tool on a remote PC.

3.1.2 Office mode

Office mode is the suspension of access control at an entrance during office or business hours. The entrance remains unlocked for these hours, to allow unhindered public access. Outside of these hours Normal mode applies, that is, access is granted only to persons who present valid credentials at the reader.
Office mode is a typical requirement of retail, educational and medical facilities.

3.1.3 SimonsVoss SmartIntego

As of version 4.6 ACE supports the SmartIntego digital locking system from SimonsVoss Technologies. BIS ACE supports 1 SmartIntego configuration per MAC .
Access at SmartIntego devices (lock-cylinders, door handles, padlocks) is managed in ACE.
For offline situations a whitelist is stored locally on the SmartIntego device.

3.1.4 Remote Control (on-card building control)

Up to two AMC output signals can be assigned directly to cards. Where so configured, these output signals are triggered by presenting the card at any reader connected directly to that AMC. They can be used to activate any device that is connected to the AMC.

3.1.5 Muster point reader

A new door model (1r) has been implemented, containing one reader and no door.
This feature supports a security manager in case of evacuation: Evacuated persons present their cards at the reader, which is situated at the mustering point. The reader can thus provide information about which employees have successfully left the building.

3.2 New enrollment functions

3.2.1 Freely configurable Persons dialog

The Persons dialog is now freely customizable.
The existing fields of the person dialog can be renamed, hidden, moved or replaced by customized fields.
The number of control types has increased, and more fields can be positioned on the tabs of the Persons dialog.

3.2.2 New enrollment readers

Two new readers have been added to the portfolio of supported enrollment readers:

- HID OMNIKEY 5427CK for iClass cards, and the CSN of MIFARE Classic and MIFARE DESFire.
- LEGIC desktop readers with both SM-4200 and SM-4500 chipsets are now supported.

3.3 Security improvements

3.3.1 Backup and restore of ACE data

The performance of ACE backups has been improved, and no size limitations are imposed on the database by ACE.
Note however that the free edition of SQL server is limited by Microsoft to 10 GB, therefore a database upgrade is urgently recommended if your data volume is anticipated to exceed that.

3.3.2 Personal graphic files now stored in the ACE database

For enhanced data security, graphic files such as ID-photos, scanned signatures, forms and badge layouts, are now stored exclusively in the ACE database. The update installer handles the migration of these graphic files to the database, initially leaving backup files on the file system. It is the owner's responsibility to destroy or secure these backup files in accordance with local data security laws.
When a personnel record is deleted, the related photos and signatures are deleted from the database, even on hierarchical systems. When a personnel record is created on the top level server in hierarchical systems, its data and photos are replicated to the subordinate servers.

All BIS ACE documents that use ID photos will need to be adapted so that they fetch graphic files from the ACE web service. An example document is provided: `MessageDetails.html`

Badge layouts and forms are now stored by BIS Division, and are now only visible to operators belonging to the same Division.

3.3.3 LBUS encryption

The encryption of LBUS communications between AMC and MAC has been enhanced. No additional configuration effort is required from the system administrator. The encryption status is now visible in BIS.

3.4 API changes

All applications using the Access Engine API V 4.5.9310.0 are compatible with BIS 4.6, except for the Get- and Set photo methods,

3.4.1 Additional attributes

The following attributes of Person have been added:

- Permission to use the new Remote Control feature (see 3.1.4 oben)
- Permission to set Office mode (see 3.1.2 oben)

3.4.2 Additional commands

The following features can be enabled and disabled on readers:

- Anti-passback
- Video verification
- Random Screening (including screening-rate and timeout)

3.4.3 Documentation

Documentation of database changes can be found in the files: `ACE API.docx` and `ACE API Database-*.pdf` files.

3.5 Resolved issues in ACE

The following is a list of the more important issues that have been resolved in the current version.

Badge designer, no authorization assigned to layouts (#188612)
Layouts can be assigned to Divisions in BIS 4.6

Division dialog will stop search (#191973)
Searching in the **Cards** dialog “Available authorizations" now works correctly even if the user has no access to the Division.

PegaSys performance improved for multiple L-BUS readers connected one AMC (#191973)
Performance has been enhanced in the case where multiple L-Bus readers write to a PegaSys card simultaneously.
Nevertheless, for performance reasons we advise against using more than 2 (max 4) readers at one AMC with write mode enabled.

ConfigBrowser instability after assigning an area to Door model 14a\b (#183330)
Areas are now assigned correctly in the Configuration Browser.

ACE reports with more data than expected (#177381)

Issue resolved whereby, on some older windows systems, some reports did not correctly display Divisions.

Maximum tries for PIN code are limited in MAC to 10 (#155738)
Configuration restricts the number of retries to 10.

Offline authorization improved for PegaSys (#170524)
Configuration has been improved for Authorizations that begin in the future.

Some fingerprint messages are forwarded to BIS in decimal (#183928)
The fingerprint messages “Verified” and ”Not verified” are now correctly transmitted as hexadecimals. The default state mapping is now correct.

Reserve fields with line 1 and column 1 on any tab (#183949)
Customizable fields can now be saved correctly at Row 1, Column 1 on the Persons dialog,

Run time error in the Persons dialog leads to instability of the BIS client (#199322)
The Company field in the Persons dialog can be used even if no company exists in the database.

3.6 Known limitations in ACE

IMPORTANT: Only for customers using **Day Models(*)** in **Access Engine**, there is a mandatory patch to correct an error that prevents modified day models from being saved.
(*) الـ يوم نماذج, Tagesmodelle, Modele dzienne, Modelos de dia, Модели дня, Gün Modelleri.

Proceed as follows to install this patch:

1. Download the ZIP file `ACE_DayModelPatch_<LANGUAGE>.ZIP (where <LANGUAGE> is a short abbreviation for the installed BIS language)` from the **Downloads** tab of Building Integration System V4.6 in the online product catalog of Bosch Security Systems, for example from https://emea.boschsecurity.com/en/
2. Rename on the ACE server the “ACSP.exe” to “ACSP.exe_org”. The file can be found in directory “..\Mgts\AccessEngine\AC\Bin”.
3. Extract the new “ACSP.exe” from downloaded ZIP file and copy it to the directory “..\Mgts\AccessEngine\AC\Bin” of the previously renamed “ACSP.exe” file.
4. Reboot the complete ACE server.
5. Optional step: If you have changed day models in BIS 4.6 before patching as described before execute a “Synchronize” command for all MACs from the BIS operator client.

Fingerprint Reader: Wiegand green LED is OFF after red LED is triggered by AMC, for some card types (#184154)
Applies to Wiegand mode for the card types MIFARE Classic CSN, iClass, EM and Prox: If an unauthorized card is used, the green LED is not shown even if the controller has unlocked the door for a set period “permanent open”.

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

Instability of the BIS client due to recording card in Dialog manager of the ACE in the Turkish version (#199275)
This instability can happen only if no dialog reader has been selected prior to reading.
Workaround: Select a dialog reader beforehand.

Export Tool: of Person.Reserve X fields not supported in BIS 4.5 (#183172)
If one or more of the database fields `Person.Reserve1` to `Person.Reserve10` is used in the previous BIS versions, the export of these fields are not supported in BIS 4.5 and 4.6.

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

Visitor card handling recommended to 5 cards (#201465)
Each visitor should have no more than 5 cards assigned to him in the ACE.

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

SimonsVoss construction whitelist is not overruled by ACE (#201468)
If the construction whitelist is newly configured after the data is imported to ACE, and the MAC is cold started, the authorizations of the construction whitelist sometimes overrule the authorizations in the ACE.
Workaround: Delete the construction whitelist using the SimonsVoss tools before activating the SimonsVoss system in the ACE.

SimonsVoss Smarthandle: Deactivate Whitelist command has no effect (#206677)
The command to activate/deactivate a whitelist does not work with SimonsVoss firmware version M 5.2.25.
Workaround: Upgrade the SimonsVoss firmware to the current version.

4 Video Engine

4.1 Video SDK 6.15.0100

The VIE Multiview Bosch Video Cameo is now using Video SDK 6.15.0100