Release notes for Building Integration System (BIS) Version 4.6.1

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.

27 November 2018

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
	Note that Version 4.6.1 will be the last version to support Windows Server 2008 R2			
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

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: o On Windows 7 and Server 2008: .NET 3.51 and .NET 4.0 o On Windows 8.1 and Server 2012: .NET 3.51 and .NET 4.5.1 (includes .NET 4.0) o On Windows 10: .NET 3.51 and .NET 4.6.1 (includes .NET 4.0) o 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 with at least 4 physical cores • 8 GB RAM (32 GB recommended) • 200 GB of free hard disk space (SSD recommended) • Graphics adapter with o 256 MB RAM, o a resolution of 1280x1024 o at least 32 k colors o OpenGL® 2.1 and DirectX® 11 • 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

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: o On Windows 7 : .NET 3.51 (for Video Engine with DiBos),and .NET 4.0 o On Windows 8.1 and Server 2012: .NET 3.51 (for Video Engine with DiBos),and .NET 4.5.1 (includes .NET 4.0) o On Windows 10: .NET 3.51 and .NET 4.6.1 (includes .NET 4.0) o 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 4.6.1

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 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 R2 or later before upgrading BIS
- If upgrade to 4.6.1 fails and rolls back to the previous version, we recommend that the rolled back version be started manually.

1.5 Supported localization of BIS Version 4.6.1

BIS 4.6.1 is localized in the following languages:

- English
- German
- Dutch
- Turkish

The following languages will be released in January 2019:
Arabic, French, Hungarian, Polish, Portuguese, Russian, Spanish, Chinese (Simplified and Traditional)

1.6 Security advice: BIS Version 4.6.1.

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

1.7 Settings required for Arabic installations

Access Engine requires the Windows System Locale to be set to Arabic. Otherwise the Access Engine reports errors, 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 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)'.
- Verify that the windows Gregorian calendar is configured and used.

2 New features in version 4.6.1

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 Newly created operators have “No authorization” by default

In accordance with the principles of *Security by default*, and the minimization of operator privileges: whenever a new operator is created then the void authorization **No authorization** will be assigned to him by default. Assign a non-void authorization to any new operators to enable them to access and modify the BIS system.

Note on naming-clashes:

- If a BIS system with a version earlier than 4.6.1 contains by chance a user-defined authorization named **No authorization**, then after upgrading to 4.6.1, there will be both the user-defined and the system defined authorizations called **No authorization**. This would cause serious problems.
  Workaround: Rename or delete the user-defined **No authorization**.

2.1.2 Workstation-based authorizations for operators

By default an operator’s authorizations apply to all workstations. As of this version, authorizations can optionally be made dependent on the workstation where the operator is logged on.

Note:

- If workstation-based authorization has been selected for an operator, then they will only be able to log on to workstations for which they have explicit authorization.
- The BIS server machine itself counts as a workstation.
- If the BIS server or another workstation has multiple definitions in the system, then the order of preference for finding workstation-based authorizations is the following:
  1. Local IP address (127.0.0.1)
  2. localhost
  3. IP address
  4. Hostname

Limitation:

- Active directory operators cannot be configured for workstation-based authorization.
- Only IPV4 is supported.

2.1.3 Access to the Event log from the BIS client is itself recorded as an event

This event will be generated every time any operator clicks the event log button.

Note:

- Sometimes the event log display may lag behind the incoming events and require a manual refresh.

2.2 Access Engine (ACE)

2.2.1 Integration of PCS Intus controllers for palm vein readers

PCS controllers, with up to 2 palm vein readers each, can be configured per MAC to provide additional biometric verification for other readers of the same MAC. This additional biometric verification is only available if the whole ACE system is running and online.
The palm vein pattern needs to have been enrolled, that is assigned to a cardholder, using a separate palm vein reader configured as dialog reader.
The ACE **Persons** dialog contains a special tab to enroll the palm vein patterns. Up to 2 palm vein patterns can be enrolled per person. The patterns are saved in the ACE database only.

2.2.2 BIS integration

The BIS provides two additional ACE commands for configurations containing palm vein readers:

- **Palm vein verification on**
- **Palm vein verification off**

For the PCS palm vein devices in the BIS device tree, messages like SABO\Online\Offline and verification requests are sent by ACE.

2.2.3 Encryption of PCS interface and password

The communication between DMS and PCS controller is encrypted for ID verification, but not for enrolment.

During configuration of the PCS controller (with the PCS tool) you can define a password.
This password has to be entered if you define a new PCS reader on the controller.

2.2.4 PCS controller license

Palm vein scanner devices must be licensed before the devices can be set up in ACE.

2.2.5 Limitation

The combination of fingerprint and palm vein verification at the same W2 fingerprint reader is not configurable.

2.2.6 Supported PCS hardware and firmware

At BIS 4.6.1 PCS palm vein controller *INTUS PS Controller V / Type S3840-525* with firmware version 12.6 or 12.7 is supported. Firmware ID is “INTUS PS IV/V OSDP /Type S3841-035”

2.2.7 Temporary cards

A temporary card is a temporary replacement for a card that has been misplaced by a regular cardholder. It is a duplicate that contains all the authorizations and limitations of the original, including rights for offline doors. To prevent abuse, the system can optionally block one or all of the cardholder's other cards for a limited period, or until unblocked manually. *Temporary cards are therefore unsuitable for use as visitor cards.*

Limitations:

- Do not use automatic reactivation of the original card with fingerprint readers or PegaSys offline doors.
- Currently the API can only be used to read temporary-card data, not to write or modify it.
- Data for 'temporary cards' is less detailed in ACE reports than in the cards dialog (#215890).

2.2.8 Inactivity limits for authorizations

The authorization dialog contains an additional field **Inactivity limit**.
This is a timed period of between 14 and 365 days. If an assignee of this authorization fails to use it within the defined period, then they will lose it. Each time the assignee uses the authorization, the timer restarts from zero.
Notes:

- This feature is not available for visitors.
- A combination of authorizations with inactivity limit and bound profiles (where authorizations are fix set to a personal type of persons) is not possible. The configuration of such combinations is prohibited and cannot be saved in the ACE dialogs.

2.2.9 Enabling random screening from BIS client

The BIS client provides two new commands for ACE card readers:

- **Random screening on**
- **Random screening off**

A prerequisite is that random screening has already been fully configured in the device editor for the readers concerned.

2.2.10 Editing an area count from the ACE dialogs

The ACE dialog under **Systems** >**Areas** allows suitably authorized operators to set a limit to the number of persons allowed in an area.

2.2.11 Deister Key Cabinet and multiple access cards

If Deister key cabinets are licensed, **and** if persons can have multiple access cards in your configuration, then the **KeyCabinet** option is initially assigned

to the first card of type **access card** in a person's card list (**Personnel data > Cards**).
Use the same **Cards** dialog to assign the **KeyCabinet** option to a different access card if desired.
If a person has only one card, then the **KeyCabinet** option is assigned to this.

2.2.12 Additional customizable HTML tab page in Cards dialog

An HTML page can be displayed in a separate tab in the ACE **Cards** dialog. This HTML page can display cardholder data that is retrieved by SQL statements from the ACE database.

In order to view this HTML tab an operator requires a special authorization in the Cards dialog.
The html page for display (a local file or one from an external web server) must be created and configured before in the registry of the ACE server.
For more details, see the white paper, "How to configure the HTML display".

Security advice:
Ensure that any HTML pages you write for this tab conform to established security standards, in order to avoid exposing your system to attack.

2.2.13 DOP states recovered after power failure

A DOP (= digital output) can recover its previously configured state (on/off) even after a power failure.

- A cold start of the MAC will not change the configured DOP.
- After an AMC cold start (or power failure) the DOP state is reset directly after re-initialization (or power up).

2.2.14 ACE API

Applications using API from BISACE V4.6 are compatible with BISACE 4.6.1.
Changes to the API are documented in detail in the files, `ACE API.docx` and `ACE API Database- xxx.pdf`.

2.2.15 W2 fingerprint reader - new mode: Finger or card

The W2 fingerprint reader has a new mode: **Finger or card**. If so configured, fingerprint patterns are downloaded to the reader, and the cardholder can use either their card or their finger for access.
Note that at least one card must be assigned to the cardholder in order for them to use **Finger or card**.

2.2.16 MAC demotion in hierarchy

In hierarchical systems the additional MACs can be demoted from higher to lower system levels.

Limitation:

- MACs that govern parking lots or elevators cannot be demoted in this way (#217057).

3 Resolved issues in BIS version 4.6.1

3.1 Platform

#186441 CFS: BVIP OPC scanning of devices not correct
The BVIP scanning tool now correctly scans unknown device types and add them to the supported type list upon selecting the unknown device.

#186442 CFS: BVIP OPC not detecting camera type Flexidome 5000 MP correctly
The BVIP scanning tool now correctly scans unknown device types and add them to the supported type list upon selecting the unknown device.

#197348 CFS: Configuration corrupted if OPC sends characters which are reserved in XML
Device and detector type inputs are validated when retrieved from the OPC server. If any XML-reserved characters (e.g. “<” or “>”) are present in the input, then those entries are not imported into BIS and an error is logged.

#209828 CFS: configuration browser stopped sometimes when copying triggers
It is now possible to copy and paste triggers of all the types.

#209990 CFS: New detectors are missing
If any events or state changes are received from a device, and that device is not present in configuration, then that device will now be added automatically.

#205916 CFS: Configuration Browser address numbering
The maximum address number in BIS is 2147418112, hence from LSN it will no longer be possible to create a higher address than this. If an existing configuration contains an unsupported address, then it can be deleted in the Configuration Browser.

#216286 CFS: Logging folder on different drive
All BIS logging will be done in `C:\S3K_Logging\` folder irrespective of the BIS installation path.

3.2 Access Engine (ACE)

#182835 CFS: AMC - "Battery OK /NOT OK" not shown correctly
AMC Battery OK /NOT OK states are now shown correctly.

#186461 CFS: Authorization names are now unique
Issue resolved whereby authorizations with identical name were defined on different MACs.

#192199 CFS: Wrong export to reserved fields 2, 3
If the ID of a reserved field is larger than 1 its contents are no longer copied to fields 2 to 3.

#200042 CFS: Report: Area Muster List
Area handling has been improved for cases where an area is selected in report **Area Muster List**

#206023 CFS: Audit trail shows card numbers with 10 digits.
In Audit Trail menu on Access Engine, 10 digit card numbers starting with 22XXXXXXXXX are now supported.

#212333 CFS: Upgrade - BIS 3.0 to BIS 4.6 , cardholder photos
Cardholder photos are now correctly migrated when BIS is upgraded from BIS 3.0 to 4.6.1

#213216 CFS: Improved database restoral prevents problems when creating reports

#140540 CFS: Valid from and Valid until date on authorizations
Authorization handling corrected for cases where start and end dates of an authorization are set for different MACs.

#181468 CFS: PegaSys: visibility of time model names improved
After creation of PegaSys time models, names of time model entry are now visible in lists when the line is selected.

#195778 Local antipassback for offline AMC
AMCs now support antipassback correctly in cases where the AMC has been configured not to query the MAC, that is, where timeout is set to zero (ADDTIME=0)).

#207608 More than 9 MACs in one system
More than 9 MACs can now be connected to one system without problems.

#204197 Improved synchronization of logging time stamps
Synchronization between log time and access time has been improved for cases where the systems are offline.

#205518 Access to help file improved for badge designer
Help file access is improved for badge designer.

#206126 SimonsVoss integration: Improvements in the handling of line states
The handling of states has been improved, so that only the first reader in a door updates Access Engine.

#207504 Redundant MAC: Improvements in failover
Improved the reliability of the failover between MAC and RMAC. In rare cases the failover was not executed correctly.

#215362 Performance of logging improved
Unnecessary logging has been disabled by default, in order to improve performance in systems with many MACs
Note: if requested by technical support telegram logging can be reactivated for any MAC-<number> in the system parameter editor:
ACSP-<number> → EnableTLG. @value=true

#208294 CFS: SACARDs (locking system cards) created even without PegaSys option being set
PegaSys cards are no longer created unless the PegaSys option flag is selected.

#215837 CFS: OPC customer-specific attributes in reserved data fields
Customer-specific OPC attributes can now be written to customer-specific personnel data fields.

#205210 DlgMgrAX - failure to set AM/PM correctly for PegaSys
PegaSys now always receives the correct AM/PM value from ACE.

4 Known limitations in BIS version 4.6.1

4.1 Platform

#199188 If HTTPS is enabled for audit trail and an upgrade (modify/repair) is performed, the service does not start after the upgrade.
Workaround: Disable HTTPS before upgrade or do not enable HTTPS until after upgrade. Batch files for enabling and disabling HTTPS can be found on the BIS installation medium under: `\Tools\HttpsForBIS\`

#188581 A1_BISAudit TrailWatcher service blocks update of the BIS-ACE
Workaround: End the task of `AuditTrailFilewatcherservice.exe` in the task manager before the upgrade.

#181056 Prerequisites window shows "Windows 10" on Windows Server 2016 PC
Workaround: This message can safely be ignored.

#178991 There is no warning during setup if there is insufficient space for the 4GB audit trail database.

#169416 .NET 4.6 is not supported. Use .NET 4.6.2 instead
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.

#170194 Post installation document
From BIS version 4.2 onwards, the post installation document will be only available in English for all the language installations.

4.2 Access Engine (ACE)

#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 when an unauthorized card is used.

#199275 & #202554 Instability of the BIS client after enrolling a card in the ACE dialogs
This rare instability can happen only if no dialog reader is selected.
Workaround: Select a dialog reader before enrolling.

#199503 Instability of the BIS-Client when trying to record a fingerprint after the reader has lost its network connection
During fingerprint enrolment the enrolment do not disconnect the reader from the network.

#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 FP reader in the moment the finger is successfully read, is still audible.

#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.

#206988 SimonsVoss delete construction Whitelist
If a construction whitelist was used before integrating with ACE then the MAC is not always able to delete the construction whitelist.
Workaround: Delete the construction whitelist manually.

#216031: Reader state "Random screening" does not follow the settings in the Configuration Browser
The on/off states for “Random screening” and “Palm vein verification’ in the Configuration Browser are not shown in the BIS Client.

Guard tour and SimonsVoss readers
The guard tour may be configured using SimonsVoss readers but the card-registered messages are not sent, so these readers are currently not supported for guard tours.

SignoPad
If a SignoPad from company Sigma is used with Windows 10 the drivers must be installed.
See https://www.signotex.com/download/treiber/twain-wia-treiber/

DMS Master startup
If the ACE logifier files are increased beyond the 7 days default, and the system creates many events (see #215362) then the ACE core system may fail to start. The DMS master process now waits longer for the logifier process. In all other cases the start-up will be faster than before.

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

New enrolment reader firmware
The new firmware for the dialog reader 'Lectus Enroll 500' supports the reading of CSN\Bosch and MIFARE Classic\Desfire badges in one step. The ACE dialogs no longer support older firmware versions, but upgrade files and documentation are located in the `\ACE\AddOns\AdmittoFirmware` directory of the BIS setup medium.

PegaSys and temporary cards
If a 'temporary card' is created for a PegaSys card, the original card is blocked by ACE system, However the PegaSys permissions on the card are not deleted.

Workarounds: Reduce the validity period of PegaSys cards, or do not create temporary cards for PegaSys users.