Building Technologies

BOSCH

Building Integration System (BIS) Version 4.6.2
Release Notes

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

Inhalt

Building Technologies

1 Installation Notes

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 (Not recommended)	Yes (Not recommended)	Yes (Not recommended)	Not recommended
Windows 7 SP1 (64 bit) Professional or Enterprise	Yes (Not recommended)	Yes (Not recommended)	Yes (Not recommended)	Not recommended
	Windows7 is only supported for updates to version 4.6.2 Note that BIS version 4.6.2 will be the last version to support Windows 7 on BIS client, BIS Login & Connection server			
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 4.6.2 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				

Note:
BIS Version 4.6.2 will be the last version to support Windows 7 on server and client.

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 4.6.2 (includes .NET 4.0) o On Windows Server 2016: .NET 3.51, .NET 4.6.2 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:
	    ○ 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 4.6.2 (includes .NET 4.0)
	
	    ○ On Windows Server 2016: .NET 3.51, .NET 4.6.2 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 4.6.2

NOTICE: On some machines the update procedure may cause your hardware ID to change. Demo mode will be activated automatically. In such cases please create a support ticket and include the new and old hardware IDs. Support will transfer your licenses to the new hardware ID as soon as possible.
To obtain your new hardware ID, open the Licenses tab in the BIS Manager, and open the license manager.

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 the database. Check folder `MgtS\EventlogEntries` and subfolders for content. You may delete additional content if not required.
- Upgrade from a previous BIS version with SQL server 2005 will not work. Upgrade to SQL server 2008 R2 or later before upgrading BIS
- If upgrade to 4.6.2 fails and rolls back to the previous version, we recommend that the rolled back version be started manually.
- From BIS V4.6.2 onward the "Mandatory post installation BIS" document will be delivered in PDF format, hence it is required to install a PDF viewer to view the BIS related documents.
- Windows updates must be turned off during BIS installation, if not turned off then BIS installation might be failed due to Windows update process.

1.5 Security advice: BIS Version 4.6.2.

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. Make careful, secure note of the password for later use.

1.6 Supported languages

BIS 4.6.2 is a minor release for the following languages:
- EN-US: English
- DE: German
- NL: Dutch
- PL: Polish
- PT-BR: Portuguese (Brazilian)
- TR: Turkish
- ZH-CN: Simplified Chinese

2   New features in version 4.6.2

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   SQL 2016 support

When installing this version of BIS, it by default supports SQL version 2016 SP2. For upgrading existing BIS, the SQL 2016 will not be upgraded and it has to be upgraded separately.

Note:

- Report print does not work, it is a known issue in SQL 2016 SP2 and hence a cumulative update need to be executed manually in order to solve this print issue. https://support.microsoft.com/en-sg/help/4505830/cumulative-update-8-for-sql-server-2016-sp2

- SQL 2016 can only be installed on windows 10, 2012 or 2016 or later versions.

2.2 Access Engine (ACE)

2.2.1 ACE API

Applications using the API from BISACE V4.6.0 or V4.6.1 are largely compatible with BISACE V4.6.2 servers. An exception is the new return value datetime for certain member variables. See `ACE API.pdf` for details.

NOTICE: API V4.6.2 is NOT compatible with BIS Version 4.6.1 and earlier.

The API provides general multithreading but be sure to consult the documentation.

Updates and modifications to the API are documented in detail in the files, `ACE API.pdf` and `ACE API Database-*.pdf`.

2.2.2 Tool to migrate single server ACE to a hierarchical system

An existing ACE single server system can be converted to a hierarchical system server. If an ACE server is added to a hierarchical system it is possible to move 2..n MACs from upper levels to the newly added ACE server.

Limitation:
- The first MAC of the upper server levels cannot be moved.

2.2.3 Improvements on W2 fingerprint reader integration

- Bugfixes in connection management between ACE and W2 reader
- Improved "Template on Device" handling, management the update and upload on fingerprint templates. Increased the time to download new cardholder data on the W2 reader.
- Bugfix for 37 bit HID cards using Bosch coded cards, if enrolment is performed on a W2 reader.
- Stability fixes in handling the application services for fingerprint management.
- Improved management of CPU load in mode "Template on Device"
- Improved real time synchronization between ACE and W2 reader.
- In case of "Template on Device", cards are accepted if their validity dates lie in the future.
- Faster connection times to execute fingerprint verification on W2 devices

Notes:
To scan W2 fingerprint readers successfully, make sure that the "Access IP Config" tool runs in the same subnet as the fingerprint reader.

If W2 reader is operating in "Template on device" mode, and the AMC connected to the reader is offline, an authorized card is accepted for access, even if the fingerprint cannot be checked

when the AMC is offline.
If this behavior is not desired, prevent the AMC from granting access when offline.
In case of "Template on device", no message is sent from the W2 reader in case of:

- User wrong card
- User wrong finger
- Duress Finger

2.2.4 Support new ADS‑AMC2‑2W one door controller (China market only)

The AMC2 -2W controller supports two Wiegand reader ports and extension modules, and is available for the China market.

2.3 Video Engine

2.3.1 Video SDK 6.32 Support
The VIE Video Cameo is now using Video SDK 6.32

3 Resolved issues in BIS version 4.6.2

3.1 Platform

#231628 CFS: OPC UA command - command is executed on different node when both the UA nodes have same detector type and command
Command now correctly identifies the node where it is configured.

#237771 CFS: OPC UA: Sometime Access with User and Password not possible
Valid username and password are sent to the OPC UA server for authentication.

#237772 CFS: OPC UA Creates a lot of Open processes if credentials fail
A new connection is created for every attempt and that connection is closed if validation fails.

#224256 CFS: After Backup with delete, the column Status is empty for the next message
The column "Status" value contains the correct value even after backup with the Delete option.

#215840 / #224277 CFS: Duplicate HW ID at BIS Licenses
The fix improves the computer signature algorithm.

#233935 CFS: Event log does not open
If the operator had no authorization to execute the "Show Report" command, then it would hang. Fixed with proper handling.

#227009 CFS: Multisselect for "show report" command in device tree does not work any more
Fixed Report for multiply-selected address.

#221775 CFS: OPC UA Cannot remove command from detector type
OPC UA server commands can now be assigned or removed from detector types without problem.

#220628 CFS: DaBisProxy disconnection from WCF interface
The OPC server BISClientProxyDA is a pure DA (data access), not AE (alarm and events). The fix prevents the system from registering a fault when AE fails to work with BISClientProxyDA. Thus the DA server continues to function as designed, without interruption.

#218935 BVIP scanning tool is not supported in French
The BVIP scanning tool will be supported in the French language.

#219205 BVIP configuration tool issue in Traditional Chinese

The BVIP Config-manager buttons: **Save Configuration**, **Help** and **Exit** are now properly visible.

3.2 Access Engine (ACE)

 # 220025 CFS: AMC - "Performance improvement to store card data on CF card
Improved performance to store some 37 bit cards on CF card.

 # 230339 CFS: Lectus Enroll and card search error fixed
Fixed an issue where a card was enrolled with 10 digits.

 # 233815 CFS: Deister Key cabinet : Address bus input field DEC/HEX mismatch
Fixed.

 # 235299 CFS: If AMC IO Extension go offline, no message in BIS
AMC IO states and tamper status are now displayed correctly.

 # 240356 CFS: Permit certain persons without hand vein check
In case of hand vein verification, dialog is enhanced to permit cardholder even without hand vein check.

 # 229451 CFS: BadgeDesigner does not use BISLoginService and checks user and password
Fixed login issue, to login on Badge Designer without password or password do not work correctly.

 # 227225 CFS: Changed configuration in Device editor is not always saved
Fixed.

 # 226412 CFS: Change Division Menu can only used one time
Bugfix, that multiple changes in Division dialog could be made without logging onto BIS server.

 # 221822 CFS: Upgrade BIS 3.0 to BIS 4.6.1 caused loss of custom field content
Fixed.

 # 217430 CFS: Field Persons=>Reserve field 10 is not migrated at upgrade
Fixed. Reserve field 10 is also migrated.

 # 216485 CFS: Connection issues at Deister Key Cabinet
Improved connection handling between BIS and Deister Key Cabinet.

 # 216485 CFS: Report issues fixed in case of restore database

After restoring the database on BIS 4.6, reports can be created correctly.

 # 212333 CFS: Upgrade - BIS 3.0 to BIS 4.6 (No cardholder photo in ACE DB)

Fixed issue, that cardholder photos are covered by update from BIS 3.0.

 # CFS: Local anti-passback improvements

 # 206430 CFS: Customized report do not work correctly

Reports now work correctly with customized fields.

 # 206430 CFS: Report Area Muster List is not area selectable

Fixed issue, that reports do not work correctly with customized fields.

 # 216030 CFS: The Attribute "Auslosungsfactor" is out of range

Fixed issue, that BIS client tries to activate additional check but the probability (Screening rate) is configured to 0%. In that case the additional check is activated without useful probability.

#231091 Instability of BioIdentify process where a person has more than eight cards

The W2 readers allow only a number of eight cards per person. When a person possesses more than 8 cards of the type supported by the W2 reader the BioIdentify process becomes unstable operate. Do not exceed 4 cards pers person.

3.2.1 OLS (PegaSys)

 # 223488/224155 CFS: AMC - "Stability improvement on LBUS reader and OLS (Pegasys)

Fixed a stability issue where LBUS readers are used to update Pegasys card information.

 # 225062 CFS: OLS (Pegasys) flags deleted under certain conditions

Fixed.

 # 170524 CFS: OLS authorisation doesn´t work

Already fixed issue (4.6.1) , that OLS authorization does not work in some situations.

 # 208294 CFS: OLS table entries will be created without option being set

Fixed.

3.2.2 ACE API

 # 232536 CFS: API using C# throwns exception, if Cards.Collectdate is used
Fixed.

 # 237203 CFS: API, login sometimes not accepted
Fixed.

4 Known limitations in BIS version 4.6.2

4.1 Platform

#235434 If VC++ 2017 higher version is already installed, then BIS installation will fail
Workaround: Need to manually uninstall the higher version and continue with BIS installation, which will install the required version of VC++

#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 Task manager before the upgrade.

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

#178991 No warning during setup if there is insufficient space for the 4GB audit trail database. Ensure that there are 200GB free before setup.

#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.

#126930 Operating System message D3DRM is missing
The message " D3DRM is missing" can be safely ignored.

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.

#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.

#216031: Reader state "Random screening" do not follow the settings in Configuration Browser

The enable\disable state for "Random screening" or "Palm vein verification' in the Configuration Browser is not shown in the BIS Client.

#194295 Access IPconfig Tool

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

#216031: Reports have truncated information in Traditional Chinese language

#242390 CFS: Palm Vein Malfunction

If you switch two or more hand vein readers off by disabling palm vein verification at reader configuration) then the HandVerify Process will disconnect ALL readers, but all readers flash blue.

Workaround: Stop the HandVerify process or restart system.

#241329/216026 The dialog Manager of the ACE does not correctly display the replacement card when they are expired

The Persons dialog displays the cards incorrectly, that is, the options for PegaSys and KeyCabinet are shown for the temporary card even after the validity period has elapsed.

#240773 Set Area dialog

The area of person is sometimes wrongly set when changing the parking area at the same time.

Workaround: Change the person's area back to the previous area afterwards.

#222502 If Computername exceeds 15 characters, then ACE becomes unstable
Workaround: Ensure that the computer name does not exceed 15 characters. See also Microsoft pages for NETBIOS naming conventions.

https://support.microsoft.com/en-gb/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and

#240857 AMC : Arming and Disarming an IDS (intrusion detection system) causes inconsistent AMC messages
Any extraneous card numbers attached to IDS arming/disarming events in the event log can be safely ignored.

#219598 Set/reset command changes status of relay hosted on an offline IO Extension board
Relay status representation in BIS GUI changes even if the extension board is disconnected. Monitor the I/O Board Online state to be sure that the status is valid.

#243264 License counts are not updated immediately
Immediately after changing the numbers of licensed divisions or cardholders, the new numbers are not always reflected accurately in the dialogs.
Workaround:
After making changes to the numbers of installed licenses always restart the computer.

#150025 Incorrect PegaSys duration time shown
If you switch between fixed duration values and default, the display may become inconsistent.

#224650 Parallel working in device configuration and command operator
Making device changes simultaneously in the device editor and the ACE client can lead to inconsistent displays.
Workaround:
Use the device editor if possible only outside of business hours, and close it as soon as changes are complete.

#243742 BIS logbook can be opened from person dialog always
An ACE operator who can execute the persons dialog is able to access the BIS logbook for the selected person independent of operators permission.

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/

Limited CANON camera support
The integrated canon SDK does not work with the operating system windows 10.

W2 fingerprint readers
For performance reasons we currently recommend no more than 100 W2 readers per system.
If network communication to the W2 fingerprint readers is lost, a complete resynch is started automatically. Depending on the amount of data, this may take some time.

As visitor credentials are typically recycled there is thus a danger that card and fingerprint data stored on the W2 device will be inconsistent during the resynch. We therefore recommend that visitor credentials be used ONLY with the "Template on Server" option.

W2 readers in "template on device" configuration
On very rare occasions after prolonged use, the card-reading (not the fingerprint-reading) interface of BioEntry W2 fingerprint readers has been observed to fail in "Fingerprint or Card" mode. The exact causes are still under investigation.
Workaround: Power-cycle the reader

4.2.1   SimonsVoss

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

#214318 SimonsVoss Whitelist enabled\disabled state
is not shown on MapView
Workaround: Use the SimonsVoss tools for verification.

#235565 SimonsVoss commands are not greyed out dependent on specific of SimonsVoss device states

All SimonsVoss commands are available if it is a reader type of type SimonsVoss.

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.

#202508 While deleting a cardholder assigned to a Simons Voss lock, the error message has limited information

While deleting a SimonsVoss lock, the error message simply says it iss assigned to a SmartIntego whitelist authorization, but not which cardholders are affected.

4.2.2 ACE API

#243210 API incompatibility: API 4.6.2 commands are not compatible on previous BIS Versions

If you connect to BIS versions like 4.6.1 and earlier the execution of commands where a door\reader mode is changed will lead to defect door\reader configuration. For a complete bug overview see API description.

#243210 API transaction fails

If Visitors are created where related IDs like ATTENDANTID or VISITEDPID are not correct given an error will be returned but leaving the existing vistor entry without the required changes in the database.

#218694 Visitor.IDTYPE property can be changed by API but is not shown in the visitor dialogs

Please only import valid IDTypes