Release Notes

Grasbrunn
2017-04-26

Building Integration System (BIS) Version 4.4

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

Table of Contents:

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	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
(*) 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 10.0 for Windows 10 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) Latest drivers and OS updates are highly recommended.
Minimum hardware requirements	• Intel i5 processor or higher. Intel Core 2 Duo 2.66 GHz (Dual Core) or greater • **4** GB RAM (**8** GB recommended) • **80**GB of free hard disk space • VGA graphics adapter with 256 MB RAM, a resolution of 1280 x 1024 and at least 32k colors • 100 Mbit/s Ethernet card (PCI) • 1 free USB port or network share for installation

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 and Server 2008: .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)
Minimum hardware requirements	• Intel i5 or higher, Intel Core 2 Duo 2.66 GHz (Dual Core) or greater • **4**GB RAM (**8** GB recommended) • **20**GB free hard disk space • Graphics adapter with 1280 x1024 resolution, 32k colors, 256MB dedicated memory with OpenGL 1.2 or later • 100 Mbit/s Ethernet card

Additional minimum requirements for VIE (Video Engine) clients	• No Windows Server operating systems • No Windows 10 • 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 4.4

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

2 New features in version 4.4

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 Arabic language support

This installation will support BIS installations in Arabic language on all the supported Operating System.

Additional settings:
Few additional settings are required to display the proper date and time

1. Date and time format should be in English
   Open “Control panel”, under “Clock, Language and Region” select “Change date, time, or number formats”
   In “Format” select English (English of any country should be fine) and click Ok
2. Arabic language should be set as default language
   Open “Control panel”, under “Clock, Language and Region” select “Add a language”
   Select “Add a language” button, select “Arabic” and click open
   In it select “Arabic (Egypt)” and click add button
   Arabic (Egypt) will be added to the supported language list, move it to the top most position to make it as a preferred language

Limitation:
Arabic: event log - Warning message not displaying correctly (160651)
If BIS is installed on Arabic Operating system or BIS installed on English operating system with Arabic as default language then warning message “Maximum number of result rows exceeded” will not display properly if more than 10,000 records are present in the event log database

Arabic: Praesideo30 PA translation of description is missing
Description information about the Praesideo30 PA OPC server will be in English and is not translated to Arabic

2.1.2 Layer visibility based on states

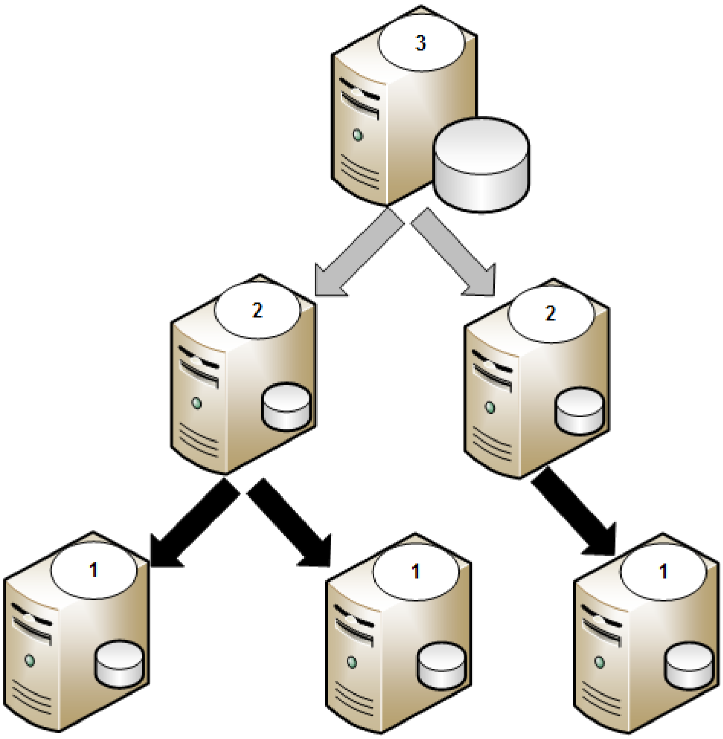
Up to and including BIS version 4.3, the visibility of graphic layers in floor plans was determined by alarm events only. With this new feature it will be possible to make the layer visible based on device states instead.
A set of batch files is provided from version 4.4 and later to enable this “LayerOnStates” feature. Once it is enabled the user can configure which layer should be visible when a chosen device changes its states. When the feature is enabled the states take priority, and layer visibility will be based only on states, even when there is an alarm.
A separate batch file is provided to disable this feature. If the feature is disabled, then layer visibility will be based on alarm events and not on states

2.2 Access Engine (ACE)

2.2.1 Centralized cardholder management

Overview and benefits
In large multi-server systems it may be beneficial to allow lower level ACE servers some degree of autonomy in the creation of cardholders and devices. They can then continue to create cardholder and device data if connection to the top-level server, that is the server with the main database, is temporarily lost.
When the connection is reestablished, cardholder data that was created at lower levels is normally merged with the cardholder data from the top-level server.
Device data temporarily created at lower levels in the hierarchy is normally overwritten by data from the top-level server.
Devices on level 1 can be configured on a level 2 BIS server. Authorizations can also configured on the level 2 server for all level 1 server assigned to this.

The following diagram illustrates a simple ACE server hierarchy. Gray arrows represent replication of cardholder data, and black arrows represent replication of cardholder and device data.



Limitations of the current version

- The hierarchy must be completely within the BIS Common Division
- Time models can only be used in one of the following ways in an ACE hierarchy:
  1. All time models for the hierarchy (a maximum of 255) must be configured on the top-level server (L3). No time models may be defined at any other levels.
     NOTE: If it is necessary to delete a time model from L3, it must first be deleted from all L2 servers. A time model can only be deleted from L3 if it is not present at L2.
     --OR--
  2. No ACE time models are permitted at all on the top level, and each mid-level server (L2) uses its own (locally defined) time models independently.
- The servers at the lowest level (L1) are intended to work as emergency backup servers with replicated data only. Any cardholder and device data that you create on an L1 server, for example during a network outage, will be overwritten by the next replication cycle, at the latest when a broken connection to the mid-level (L2) server is re-established.
- BIS operator data is not replicated. Therefore the management of BIS operators, including their authorizations, must be carried out separately on each BIS server.
- A BIS/ACE server must contain no person or device data while it is being registered in the server hierarchy
- The servers in the hierarchy must all be of exactly the same BIS version and language. During a BIS update all data transfer is stopped until the version numbers are the same.
- Extended ACE functionality, such as key cabinets (Deister or Kemas), parking-lot management and “PegaSys” Offline Doors have not yet been tested thoroughly in a server hierarchy.
- New states for devices as MAC states, replicator etc are only translated in English and German language.

2.2.2 Redundant Main Access Controller (MAC)

Overview and benefits

A redundant main access controller (MAC) that is a synchronized twin of an existing MAC, and takes over management of its data if the first MAC fails.

MACs may be twinned with redundant MACs (RMACs) to provide failover capability, and hence more resilient access control. In this case the access control data are replicated automatically between the two.

RMACs can be configured in single BIS systems and also on hierarchical systems. In the case of hierarchical systems, RMACS assigned to bottom level (level 1) MAC servers can be configured at level 2. This provides a failover if contact to the level 1 system is lost.

Upgrade without downtime
In larger installations with MAC and RMAC, system can be upgraded without disconnecting AMCs from a MAC. While BIS and MAC are beung updated, the RMAC can control and manage the AMCs. Once the BIS and MAC are upgraded, the RMAC transfers control back to the MAC and RMAC becomes ready for its own upgrade.

2.2.3 Kemas key cabinet integration

Prerequisites

- A Kemas key cabinet is ready for use and its IP address is known. The Kemas key cabinet system supports readers that can read and write Bosch standard card encoding.

Functionality

- The system prevents personnel from leaving the premises before returning their keys to the assigned compartment in the Kemas key cabinet .
- The system creates an alarm with the state Access denied (key) if a person attempts to leave the premises and the key has not been returned.
- The system creates an alarm with the state Access denied (offline) if a person attempts to leave the premises while the connection to the Kemas key cabinet is interrupted.
- The system creates an alarm with the state Key cabinet offline if connection to the Kemas key cabinet is interrupted.

Limitations
The current version supports only one key cabinet per ACE system

2.2.4 A new DMS / MAC sync functionality

Functionality
A new sync functionality can solve most problems between DMS and MAC, so a cold start of a MAC is not needed in most situations. All access functions on AMC/MAC side will be done independently without outage.

The MACCommander tool and the AEOPC will provide functions to start this new sync type, too. It can be used for example if hardware defects require a synchronization of the MAC database.

Resynchronization between DMS and MAC

The new sync feature is implemented on both sides (DMS and MAC), which allows a manual resynchronization between DMS database and MAC database. The resync is achieved by means of a new command that will be sent by DMS to MAC. The command allows resync of both full databases and individual tables. After receiving the RESYNC command for one table, MAC will request the specified table from DMS, will update all known records and will delete from its table all records not received as a result of this request.

Limitations
The communication between DMS and MAC is slightly delayed while the sync is running.
- For Patches / Updates:
A cold start is not required if the patch or the update is compatible to the database and the shared memory of the installed version. In this case the new sync is sufficient.

2.2.5 Enhanced AMC security connection management

Functionality

- If an AMC is connected to a MAC, connection requests from other systems are rejected. Only when AMC–MAC connection is interrupoted for more than 90 sec can an AMC be connected to a different system.

2.2.6 Anti-passback timeout extensible to 24 hours (TFS170317)

Functionality

- Anti-passback timeout is now extensible from 120 minutes to 24 hours.

2.3 Video Engine

2.3.1 Video SDK 5.92.0068 Support

The VIE Multiview Bosch Video Cameo is now using Video SDK 5.92.0068

Following cameras have been tested with 5.92 SDK

DINION IP starlight 7000 (720p)
DINON IP 7000HD (1080p)
FLEXIDOME IP starlight 7000 VR
AUTODOME 800 HD (VG5-836)
AUTODOME IP 7000 HD
FLEXIDOME IP indoor 5000

FLEXIDOME IP panoramic (7000)
DINION 4000 Series
DINION 5000 Series
DINION IP ultra 8000
VIDEOJET decoder 7000
VIDEOJET decoder 8000

Limitation:

1. RTSP protocol will not work and it requires a workaround.
   Workaround: A separate batch file needs to be executed to replace the library C:\Program Files (x86)\Bosch\VideoSDK5\bin\Bosch.VideoSDK5.RTSP\RTSP_VDP.dll of 5.92 version with the older version 5.71 library. This batch file is available from technical support.
2. The DIVAR IP 5000 requires that you switch on RCP+ protocol manually (debug page)

3 Resolved issues in BIS version 4.4

3.1 Platform

Detectors not changing color
The color of the detector is updated properly based on the current state, even after selecting unauthorized locations.

Problems with printing layer
Automatic printing will work as normal, issue was due to a HOOPS control not being properly cleared.

Template jobs intolerant of empty cells.
Import of template jobs works as normal, even íf the job template spreadsheet contains empty cells.

Event log remains half full even after importing an event-log backup
Backup with data removal deletes all events from the current event log. Structural information related to the events is nevertheless retained, so that the system can continue to use it.
During backup a popup dialog asks whether the saved data should be removed from the current event log.
– Click **No** to save event data to a file in the specified directory.
– Click **Yes** to save the event data as above, but additionally to remove the saved events from the current event log plus **(new)** attributes and other surplus information.

Alert is missing if virtual detector list exceeds the 10K limit
While creating address list, if the selected addresses in the address list exceeds the supported 10,000 limit then it throws a warning message

Prevent the import of parameter changes from a corrupted configuration.crp
Henceforth only a valid configuration files can be loaded into the BIS system

BISRemoteSQLServerSetup can run repair if SA is not default
BISRemoteSQLServerSetup now provides an option to get the password for the SA account as it does during installation. If the user has changed the default password, they can enter the new password to execute the repair process.

Imrovement to handling of numerical strings in ths BIS Configuration Browser
Virtual device addresses that contain only digits are now correctly handled as strings, and can be renamed without corrupting the configuration.

3.2 Access Engine (ACE)

Withdrawal of an authorization was not executed on AMC level
The problem has been resolved whereby some authorizations withdrawn in the ACE client were not withdrawn at AMC level.

ACE division names in non-Latin scripts
The problem has been resolved whereby the names of ACE divisions in certain non-Latin scripts were not properly displayed in ACE.

Messages for person and card related changes are no more written to BIS logbook
The problem has been resolved whereby ACE messages related to changes in persons or cards were not being properly recorded in the event log.

BIS ACE API 4.2 - GetAllLockoutIds
The problem has been resolved whereby the API function `GetAllLockoutIds()` would return 0 locked users, even when the dialogs indicated locked users.

Setting Show LastAccess
The last access timestamp is shown by default in the dialog manger in the **Cards** menu.
A registry setting is available to prevent this if so desired for data security reasons.

API card collect dates function correctly
The problem has been resolved whereby the card collection dates set by API were not functioning properly.

ACE API improved stability for long query results (longer than 255 characters)
The ACE API now robustly handles query results longer than 255 characters.

Analog value messages fixed for the DIP door model
The line states **Short Circuit** and **Broken** have been added to the detector type DIP/DOP.

Deletion of entries in table SaCard CLU has been improved
Deletions from the table `saCards`, are now performed cleanly.

Improvements to Logifier
The logifier handles high access event traffic more robustly.

Language improvement for PIN or card reader in PL version
The Polish translation of the PIN or Card feature has been corrected

Support of duration of 1 day for visitor access profile
If duration of validity is set to 1 day then the visitor badge stays valid until the end of the day.

Restoral of ACE database now supports the computer name “BIS”

Note that Instance name and computer name should never be identical (see Installation Manual)

Deister key cabinet: Flex II 6U can be selected as an option
The Deister model Flex II 6U can be selected in the Configuration Browser.

The import of Pegasys Offline Doors is no longer supported.

API command => ACEPerson.AUTHUNTIL supports dates beyond 2038
The AuthUntil field works for dates beyond 2038 . However, entering dates prior to 1.1.2000 in the AuthFrom field causes access to be denied.

Improved logging of changes to Employees data
If changes are done to the *Employee* (adding and deleting cards, adding and deleting athorizations etc.) the BIS event log is updated correctly.

API connection to the event log
If using more than one AccessEngine instances connecting to one or more BIS ACE servers, the event log now updates correctly.

Person types (Persclass) not displayed correctly
If changes are mode on person types, the person types displayed correctly, and not in the state undefined.

Stability improvements for connections to external SQL servers
The stability of transactions to remoteSQL servers has been improved.

Improvement if value of random screening is set to 100%
Random screening can be set to 100%, without any interruption to the user.

Stability improvements to the "Card in use" feature in MAC

Changing a locked profile for a person class derived from “Employee”
The person *Administrator* is member of the person class **Employee** but does not take part in access control. The person count is no longer adversely affected by changes to it.

Improved handling of visitors’ authorizations and profiles
The **Visitor** dialog will correctly assign an authorization that was configured in the **Person Class** dialog to a new visitor.

4 Known limitations in BIS version 4.4

4.1 Platform

.Net 4.6 is not supported

In case that 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.

Post installation document

Since BIS version 4.2, the post installation document is only available in English for all the language installation

Untranslated strings

Following strings are available only in English and German language, in other languages they are not translated, will be translated in BIS version 4.5, some of them are state strings and some are display strings

1	Autostart
2	Card not yet valid
3	Coldstart of MAC
4	Connected
5	Disk nearly full
6	Duration
7	Duration in minutes
8	External Data
9	Global access sequence monitoring on or off
10	Global access sequence monitoring on/off
11	MAC coldstart
12	MAC initialized
13	MAC is Master
14	MAC is Slave
15	MAC not initialized
16	MAC offline
17	MAC online
18	MAC switched to Master
19	MAC warmstart
20	Not visible
21	PROCESS
22	Process kill failed
23	Process start failed
24	Process stop failed

25	RMAC
26	Ready
27	Replication disabled
28	Started
29	Stopped
30	Synchronization finished
31	Synchronizing
32	Version mismatch
33	Visible
34	Waiting for connection
35	warmstart of MAC
36	Address list contains more than supported addresses %1
37	(Supported: %d, Contains %d)

4.2 Access Engine (ACE)

Import authorizations

To avoid issues after importing authorizations, attend to the following:

- The “valid from” date of an AMC controller must be later than 01.01.2001 00:00. If an older date is used the MAC will reset it to 01.01.2001 00:00
- PegaSys cards are encoded with a “valid to” date on or before 31.12.2047 00:00, and the “valid to” date of the AMC controller must be the same.
- A date + time value must now include the hour and minute, for example in the format: dd.mm.yyyy **HH:MM.**
  Note that if you have old import descriptions using “valid from” and ”valid to” fields without HH:MM, then you need to edit them manually to include HH:MM.

Multiple lockouts' dlg missing

ACE dialog "Multiple lockouts" is missing in ACE user profiles, workstation profiles, and dialog manager.
If required, please contact ACE support for a special license file to support this dialog.