Building Integration System (BIS) version 4.9.1
RELEASE NOTES

2021-12

This document is intended to familiarize you with your new BIS version as quickly as possible

Version	Description
1	2021-12-16 approved version

General note on documentation
Although every effort is made to keep translations as up-to-date as possible, late changes to the software may be documented only in English, and their translations available only after release of the product, or in the next version. In case of discrepancies, the English-language documentation should be regarded as more up-to-date.

Table of contents

1 Installation Notes

3 29

BIS installations with computer names longer than 15 characters are not supported. Keep the computer names to 15 characters or fewer.

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 10 (64 bit, Enterprise LTSB/LTSC - Version 1809, Build 17763)	Yes	Yes	Yes	Yes
Windows 10 (64 bit, Pro Version Windows 10 (64 bit, Pro Version 20H2 Build 19042.1348 or 21H1 19043.1348)	No	No	Yes	Yes
Windows Server 2016 (64bit) Standard or Datacenter *	Yes	Yes	Yes	No
Windows Server 2019 (64bit) Standard or Datacenter *	Yes	Yes	Yes	No
* Not as domain controller				

End of support notices:
The version 4.7 was the last version to support:

- Windows Server 2012R2 on a server and a client station
- Windows 8.1 64 bit as a server
- Windows 8.1 32 bit as a client

The version 4.8 was the last version to support Windows 8.1 on clients

1.2 Server

These are the hardware and software requirements for a BIS server:

Supported operating systems (standalone or client/server mode). Installations of BIS on other operating systems may succeed, but are entirely without warranty.	– Windows Server 2016 (64 bit, Standard, Datacenter) – Windows Server 2019 (64 bit, Standard, Datacenter) – Windows 10 Enterprise LTSC (64-bit) – **Note:** The default database delivered with this BIS Version is SQL Server 2019 Express edition with advanced services
Other Software	**Always install the latest drivers and OS updates.** – IIS 10.0 for Windows 10, Windows Server 2016 and Windows Server 2019 **Note**: IIS is not necessary on BIS connection servers – Internet Explorer 9, 10 or 11 in compatibility mode – Chrome, Firefox, Edge (Chromium-based) for Smart Client – .NET: – On Windows 10, Windows Server 2016 and Windows Server 2019: .NET 3.51, .NET 4.8, .NET 5.0 and Core 3.1.7
Minimum hardware requirements	– Intel i7 processor generation 8 – 16 GB RAM (32 GB recommended) – 250 GB of free hard disk space – 300 MB/s hard disk transfer rate – 10 ms or less average hard disk response time – Graphics adapter with – 256 MB RAM, – a resolution of 1920x1080 – at least 32 k colors – OpenGL® 2.1 and DirectX® 11 – WebGL2-compatible (for example, Intel UHD Graphics 600 class or comparable), non-virtualized – 1 Gbit/s Ethernet card – A free USB port or network share for installation files

1.3 Operator Client

These are the hardware and software requirements for a BIS Operator Client:

Supported operating systems (standalone or client/server mode). Installations of BIS on other operating systems may succeed, but are entirely without warranty.	– Windows Server 2016 (64 bit, Standard, Datacenter) – Windows Server 2019 (64 bit, Standard, Datacenter) – Windows 10 (32 or 64 bit, Pro or Enterprise LTSC) – **Note:** with a Pro edition, updates must be deferred until 8 months after the release of the BIS version. For further information see the Microsoft technet page at `https://technet.microsoft.com/en-us/itpro/windows/manage/introduction-to-windows-10-servicing`

Other Software	– ASP.NET
	– Internet Explorer 9, 10 or 11 in compatibility mode (Note: The SEE client requires IE 9.0)
	– Chrome, Firefox, Edge (Chromium-based) for Smart Client
	– .NET:
	  – On Windows 10, Windows Server 2016 and Windows Server 2019: .NET 3.51, .NET 4.8, .NET 5.0 and Core 3.1.7
	  – **NOTE** .NET 4.8 needs to be installed manually on remote ACE clients. It can be found on the BIS installation media under `\3rd_party\dotNet\4.8`

Minimum hardware requirements	– Intel i5 (Gen 6 / Skylake or newer) or higher, multiple cores
	– 8 GB RAM (16 GB recommended)
	– 25 GB free hard disk space
	– Graphics adapter with
	  – 256 MB RAM
	  – a resolution of 1920x1080
	  – at least 32 k colors
	  – OpenGL® 2.1 and DirectX® 11
	  – WebGL2-compatible (for example, Intel UHD Graphics 600 class or comparable), non-virtualized
	– 100 Mbit/s Ethernet card

Additional minimum requirements for VIE (Video Engine) clients	– No Windows Server operating systems – Intel i5 processor with at least 6th Generation & min 4 physical cores – 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

Supported languages in BIS-ACE 4.9.1: EN-US, DE-DE, RU-RU, ES-AR, ZH-CN, ZH-TW, PL-PL, TR-TR, AR-EG, HU-HU, NL-NL, FR-FR, PT-BR

1.4 Smart Client

These are the hardware and software requirements for the browser-based BIS Smart Client:

Browser software	Either one of: • Google Chrome, version 90 or higher • Microsoft Edge, version 90 or higher • Mozilla Firefox, version 88 or higher
Minimum hardware requirements	• Intel i5 processor Generation 6 with at least 4 physical cores • 8GB RAM • Graphics adapter with 1920x1080 resolution, OpenGL® 2.1 or later • 1 Gbit/s Ethernet card

1.5 Updating BIS to version 4.9.1

- Ensure that the BIS version from which you are upgrading is running properly. The upgrade procedure cannot repair defective installations.
- For BIS versions below 4.7 only: 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 fast as possible.
- To obtain your new hardware ID, open the **Licenses** tab in the BIS *Manager*, then open the **License manager**.
- If a version of *BISProxyOPCDA* below 4.9 is already installed, unregister that version of *BISProxyOPCDA*, replace it manually with the new version delivered with BIS 4.9.1, and register it.
  The configuration files need **not** be replaced. These are
  `BisProxyOPCDA.config.crp`
  - `ProxyDA.exe.config`
  - `RemoteSitesConnector.DetectorTypes.xml`
  - And are located in `<installation drive>\Mgts\Connections\BISProxyOPCDA\`
  - For full instructions, see the following help file on the installation media `AddOns\BISProxyOPCDA\BIS_Proxy_OPC-DA_Server.chm` > **`Installing the OPC Server`**
- During the upgrade BIS 4.8 onwards, the *A1_BISStarter* service is disabled to avoid starting the BIS services during upgrade process. This service will be enabled and marked to run automatically upon successful completion of the upgrade. If the upgrade is canceled or aborted, then a rollback is performed and this service will remain

disabled. To run BIS on a rolled-back installation, set the service manually to run in **Automatic (Delay start)** mode. 7 29

- When upgrading from BIS 4.4 or older, please terminate the old ACE Card Personalisation service (CP) before starting setup. Right click the CP system tray icon and select the bottom option “End program”. Alternatively, kill SfmApp-4.exe in task manager.

The setup program identifies any currently installed version of BIS.

- Before updating, make sure folder `MgtS\EventlogEntries` is empty.
  - If the log entries are not required, delete them to empty the folder.
  - If the log entries are required, start the old version of BIS, and wait until the folder becomes empty, that is, the buffered log entries are imported into the database.
- If the setup program detects a version older than or equal to BIS 3.0, the upgrade process will be aborted. The setup program will ask you for permission to remove the older version and install the new version. The existing customer configurations will be maintained.
- If the setup program identifies an installed version of BIS 4.0 or higher, the update will proceed as normal. All customer-specific files and configurations will be maintained.
- SQL Server 2008 and older will not work with BIS 4.8 onwards. Before upgrading the BIS version, make sure you upgrade to at least SQL Server 2012 R2 or another supported version.
- Windows updates must be paused during BIS installation, because they can interfere with it. Install all Windows updates before the installation.
- The BIS 4.8 onwards installation media contain a new version of the PRAESIDEO OPC server. We recommend that you use this version.

1.6 Updating Access Engine (ACE) to 4.9.1

Updating dedicated ACE client computers

Before updating a dedicated ACE client machine to 4.9.1, delete the following folder with all its contents: `%programfiles(x86)%\AccessEngine\`

Reinstating AMCs after an ACE update

Before putting AMCs online after an update, ensure the AMC is physically connected to the network and that the device communication password (DCP) has been set.

The automatic provisioning phase of firmware to the AMCs lasts 15 minutes from the time of saving the changes made in the device editor. AMCs that are not reachable within these 15 minutes will not be receive the firmware update.

To restart the provisioning phase,

1. Clear the **Enable** check box and save the configuration, then
2. Select the **Enable** check box and save again.

8 29

Alternatively the provisioning phase can be activated using the AMCs context menu:
For AMS: Command in the MAP View: **Send TLS key**
For BIS: Command in the Device tree: **Allow sending of the secure key to the AMC**
Follow this procedure also whenever you have cleared the DCP using the AMCIPConfig tool or cleared the key via AMC's LCD display button.

1.7 Updating Service References in WCF applications

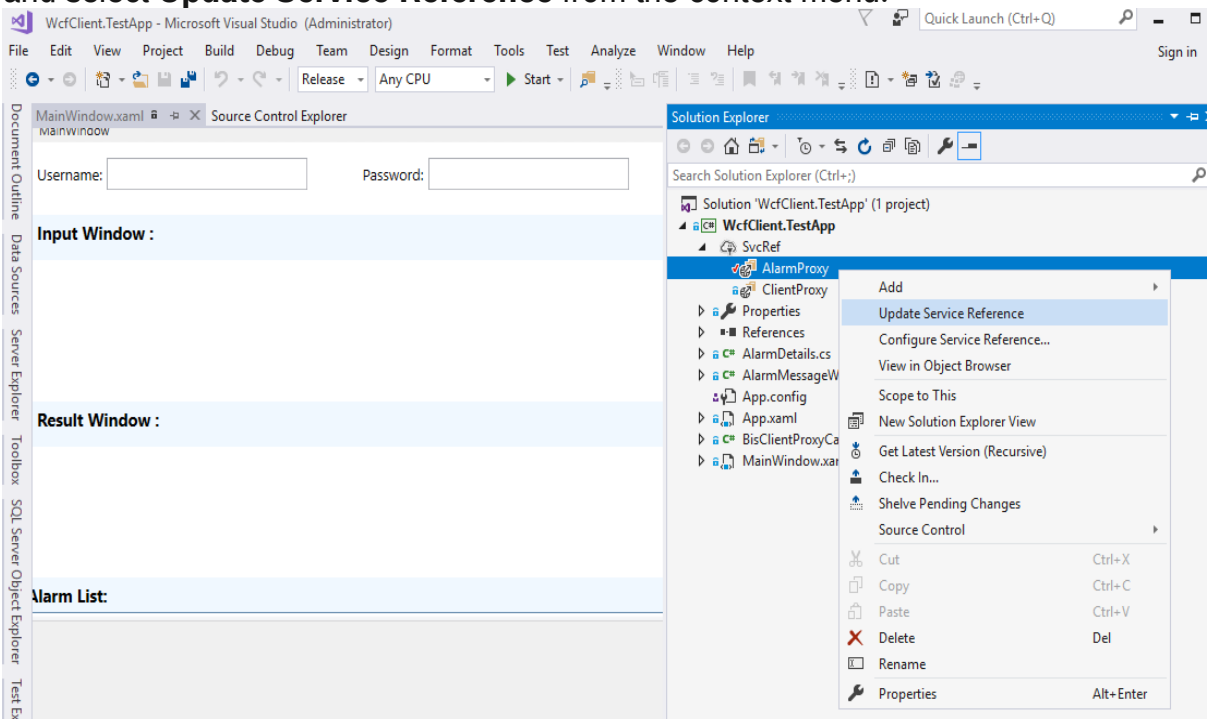
Introduction
WCF (Windows Communication Foundation) client applications that were created based on an earlier version of the BIS WCF service will not work with a BIS version of 4.8 and above due to changes in the service **BISClientProxyWCFService**.

Remedy: After upgrading from a version below 4.8 to BIS 4.9.1, update the service references in the code of the client application.

Procedure

1. Ensure that the Service **BISClientProxyWCFService.exe** is running.
2. Open the WCF client application In Visual studio.
3. In the **Solution Explorer**, under **Service References**, there will be two entries **AlarmMessagesProxyServiceReference** and **ClientProxyServiceReference**. Right-click each of these in turn

and select **Update Service Reference** from the context menu.



In each case a progress bar is displayed while the reference is updated from its original location, and the service client is regenerated to reflect any changes in the metadata.

4. After updating both references, rebuild the executable of the client application.

1.8 Settings required for Arabic installations

Access Engine requires the Windows System Locale to be set to Arabic. Otherwise the Access Engine reports an error, and some dialog controls will show invalid characters instead of Arabic characters.

In case the operating system is not originally Arabic, installing an Arabic language pack will not update the SystemLocale, 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 SystemLocale to Arabic (Saudi Arabia).
- Make sure that the Windows Gregorian calendar is configured and used.
- Make sure that the SQL server collation is set to **Arabic_CI_AS** otherwise login with Arabic characters is not possible.

1.9 Advice for security of personal data

In accordance with international and national data protection laws, companies are obliged to delete from their electronic media all personal data when it is no longer required.
You are hereby advised that access controllers and readers may contain such personal information, and that you are consequently obliged to use and dispose of them as electronic media in the sense of these data protection laws.

1.10 Certificates require synchronized system clocks

Certificates are only valid if the clocks of participating computers are synchronized. Use an NTP service to ensure this.

1.11 Monitor your hard-disk space.

Check your server's hard-disk space on a regular basis, and ensure that 20GB is available at all times.

2 New features in version 4.9.1

Notice!
The limitations cited in this document are the maximum values that have been tested by the time of publication of BIS 4.9.1 They do not necessarily reflect the absolute maxima for the system.

2.1 Platform

2.1.1 Edge browser

The BIS Client now supports the Edge web browser (Chromium based) in addition to the existing IE Browser. Do not deinstall the IE browser.

In order to use the Edge browser for the BIS Client:

1. Download and install edge browser (https://www.microsoft.com/en-us/edge).
2. Download "<Name_of_BIS_Server>.zip" from BISServer using URL http://<Name_of_BIS_Server>/<Name_of_BIS_Server>.zip
3. Unzip the archive and, from the extracted files, run "InstallBISClient.bat" with administrator privileges.

This BAT file does the following:

- Install BIS Server certificate,
- Configure browser security settings & trusted sites,
- Configure Edge to run in IE mode,
- Update the site list and
- Create a BIS Client shortcut on the desktop.

11 29

2.1.2 OPC UA write-item support

BIS is now able to write directly on OPC UA items using a custom command. This works even when the OPC server provides no method to change its value.
This custom command will be available for all OPC UA item data types which have write access.

Limitations:
This write functionality is limited to the standard data types supported by BIS:

OPCUA DataType	BIS Detector Type	DataType String
Boolean	RW_Boolean	"Boolean"
String	RW_String	"String"
DateTime(*)	RW_DatTime	"Date Time"
Int8	RW_Byte	"Byte"
Int16	RW_Int16	"Short"
Integer (Int16)	RW_Integer	"Short"
Number (Int16)	RW_Number	"Short"
Int32 / Int64	RW_Int32	"Int"
Float	RW_Float	"Float"
Double	RW_Double	"Double"
Uint8	RW_BYTE	"Unsigned Byte"
UInt16	RW_Uint16	"Unsigned Short"
Uinteger (Uint16)	RW_UInteger	"Unsigned Short"
UInt32 / Uint64	RW_Uint32	"Unsigned Int"

(*)Date only. The „time" part is not processed.

No other data types are supported.
If you nevertheless attempt to write to non-supported data types, then:

- Some nodes with write-access, will send a "Bad Node Error" to the `OPCUAClientLib.log` file.
- Other nodes with write access will not throw any error, and will revert to their default value, e.g. a node of type "DateTime".

2.1.3 BIS Smart Client

12 29

Since version 4.9 BIS includes BIS Smart Client: a modern, browser-based client. No special license is needed for the Smart Client.
The Smart Client supports the display of floor-plan layers based on alarm states.
Major features in this release include:

- New device tree widget that enables the operator to:
  - List devices in a given location from the location tree
  - Execute commands for devices from the context menu, and device-specific fast commands from the list of devices
- Automatic display on alarm layers in the map widget, based on the occurrence of matching alarms in a location.
- Numerous functional bug fixes, stability and performance improvements.

2.1.3.1 Limitations in BIS Smart Client version 4.9.1

- Smart Client login will not work if the Client authentication method is set to "**Windows verifies authentication**". Use only "**BIS verifies authentication**".
- Changes done in the Smart Client configuration, for example: Adding/modifying/deleting workspaces and dashboards are not recorded in the audit trail.
- BIS database backup, configuration backup and configuration collector will not back up configurations related to workspaces and dashboards
- Default locations (Location tree root nodes, Devices, Operators, Detectors without location and New detectors) are not displayed. Only locations that are created manually are displayed in the location tree. [Workaround: Create new locations in the location tree, and link detectors to those locations]
- Dual-operator-login is not supported: Smart client will not prompt for the second operator to authorize the first. It uses only the first operator's authorization.
- It is possible to log off from Smart Client even if the operator logged in is not authorized to terminate the client, as set in BIS configuration > **Authorization** > **Allowed to terminate client**
- It is possible to access the fast command from Smart Client, even when the operator logged in is not authorized to use it, as set in BIS configuration > **Authorization** > **Authorized for fast access command**. [Workaround: Authorize the controls individually on the same configuration-browser dialog]
- Smart client has its own action plan format with the extension '`.sc.xml`'

It supports only static content with default style and Action buttons without authorization. No other items are supported

13 29

- Smart client does not support BIS “Miscellaneous documents”
- Smart client has no print command [Workaround: use the browser print command].
- Smart client will not support commands with dynamic or empty parameters. [Workaround: Copy and adapt commands that are already defined in the configuration]
- When you select multiple devices from a location, Smart Client will display only the commands supported by all the selected devices.
- When associating a floor plan with a location in the BIS Configuration Browser (via **Locations > Tree structure > Graphic file**), BIS will automatically copy the chosen DWF file to the “`Documents\Floor plans`” folder of your configuration if the file is not already at that location. However, it will not copy any corresponding DXF files automatically. In this case, you will need to place the DXF file in the “`Documents\Floor plans`” folder manually.
- In line with best security practices, we advise not to allow operators to share BIS user accounts. For example, doing so would enable an operator to view action plans that have been accepted by another operator using the same account.
- #360088: Using BIS Configuration Browser, you can place detectors directly at a location via the Detector directly at location tab in the **Detector placement** view.
  If you place address lists directly at a location in this manner, they will be available in the device widget, but you will not be able to execute any commands against the list.
  [Workaround]: Do not place address lists at a location, place individual detectors from that list instead.

2.1.3.2 Manual backup of workspaces and dashboards

As stated above, user-created workspaces and dashboard layouts are not covered by the BIS integrated backup/restore tools. If you intend to create a significant number of workspaces and/or dashboards, you can back those up and restore them manually using SQL Server Management Studio.

To create a backup of workspaces and dashboard layouts:

1. Launch SQL Server Management Studio and connect to the SQL Server instance for BIS (named “BIS” by default).
2. Under the “Databases” node, locate the “SmartClient.Shell” database
3. Right-click the “SmartClient.Shell” database item, and choose **Tasks > Back Up…** from the context menu.

4. Configure backup parameters as suits your needs, then click “OK” to commence the backup.

To restore a backup of workspaces and dashboard layouts:

1. Using IIS Manager, ensure the Smart Client application is stopped. If needed, stop its application pool (**Server root > Application Pools > Smart Client Shell AppPool**).
2. Launch SQL Server Management Studio and connect to the SQL Server instance for BIS
3. Under the “**Databases**” node, ensure there is no “SmartClient.Shell” database. Delete it if necessary. Note that this will remove any workspaces and dashboards that may have been created since the last backup.
4. Right-click the “**Databases**” node and choose “**Restore Database…**” from the context menu
5. Locate the backup you created earlier (e.g., by specifying the backup file under “**Source**” > “**Device**”), and configure the restore parameters as needed.
6. Click “**OK**” to restore the “SmartClient.Shell” database from the backup
7. Using IIS Manager, start the Smart Client application again by starting its application pool. See step 1.

2.1.3.3 Password for the Smart Client database user

If you changed the password for the Smart Client database user in BIS 4.9, then Smart Client may no longer be able to connect to its SQL Server instance after performing the upgrade from BIS 4.9 to BIS 4.9.1. As a consequence, you will be able to log into the Smart Client, but it will no longer be able to load workspaces and dashboards. This is due to a bug in the "BIS Change Password Tool" in BIS 4.9, which has been fixed in BIS 4.9.1.

To restore database connectivity in such a case, reset the password for the Smart Client database user using the "BIS Change Password Tool" from the BIS 4.9.1 program folder, located under:
<installation drive>:`\MgtS\Tools\ChangePassword`

2.1.4 SQL Server 2019 support

2.1.4.1 Operational information

- For new installations of BIS 4.9.1, SQL Server 2019 Express edition will be installed, if you are not using your own purchased version.

2.1.4.2 Limitations

- If the SQL Server Reporting Services (SSRS) and the BIS database SQL Server are not to run on the same machine, then Reporting

Services and the BIS database SQL Server require purchased, licensed versions of the respective products. 15 29

2.1.5 Setup Enhancements

Substantial enhancements have been made. Make sure that you follow the new instructions in the Installation Manual.

2.1.6 New Certificate Tool

This tool was introduced with BIS 4.9. It replaces the older BWC config tool and the even older certificate tool from ACE.
Use only those tools that are delivered in the same BIS Version. Always follow the instructions in the current Installation Manual and the manual of the Bosch Certificate tool, which is located in the same folder.
The following is a summary for your information.

2.1.6.1 Additional details

- This tool will now create a single root certificate for BIS, ACE, ID-Service, SSRS and OPCUA instead of multiple certificates.
- The Certificate Tool is located on the BIS server machine after installation in <installation drive>:`\MgtS\Certificates`). The documentation is located in the same folder.
- SSRS can be used in a BIS installation only via HTTPS. HTTP has been removed from BIS 4.9.
    - A preconfigured tool with a separate configuration file for Remote SSRS certificate binding, is located at: <Installation media>`\AddOns\BIS\RemoteSQL\Certificate`. This preconfigured tool is only for remote SQL Servers, therefore do not copy and execute the tool from the BIS login server.
    - Conversely, use only the BIS login server's own preconfigured tool on the BIS login server.

2.1.6.2 Limitations

- Upgrading from BIS4.8 or older versions
    - The tool will create a new self-signed certificate. If you wish to use your own CA certificates, you must configure these manually. See the Certificate Tool documentation for instructions.
    - The tool will not delete the old self-signed certificates created by BIS.
    - You must download the new certificate ("`[SERVERNAME].cer`") from the BIS login server to all your clients, after the upgrade.

2.1.7 ChangePasswordTool Enhancement

- Changing the DB user password for the SQL Server user **logbuch_w** will now update the SSRS password as well, even if the SSRS and SQL Servers are running on two different machines.

2.1.8 Fully Qualified Domain Name (FQDN) Support

- The Certificate Tool now supports alternate names.
- You can add alternate names to your certificates using the Certificate Tool located at „*<installation drive>:* `\MgtS\Certificates`“ on the BIS login server. See instructions located in the same folder.
- For the remote SSRS machine, use only the tool located at `<Installation media>\AddOns\BIS\RemoteSQL\Certificate` folder. See instructions located in the same folder.

2.1.9 Access Reporting service using Domain Account Support

By default, the BIS system uses the **Mgts-SSRS-Viewer** user account to access Reporting Services. Alternatively you can enable domain user accounts to authenticate the Reporting Services (SSRS). To do this, follow the instruction in the readme.pdf file located at <installation media>`\Tools\EnableSSRSDomainAuthentication`.

2.1.9.1 Limitations

This feature is not supported for remote Reporting Services (SSRS). That is, where the SSRS service is not running on the BIS Login Server.

2.1.10 Security Improvements

2.1.10.1 DCOM Security level improvement

Microsoft recently identified a vulnerability in DCOM communication. Microsoft proposes to fix this issue by enabling DCOM hardening delivered in a future security patch. See: https://support.microsoft.com/en-us/topic/kb5004442-manage-changes-for-windows-dcom-server-security-feature-bypass-cve-2021-26414-f1400b52-c141-43d2-941e-37ed901c769c)

In BIS versions before 4.9.1 this hardening may cause connections to a "BIS connection server" to fail.

To avoid this issue, in BIS 4.9.1 we have changed the system level DCOM Security of "DCOM Authenitication level" from "Connect" to "Packet Integrity" for both "BIS Login server" and "BIS Connection server".

2.1.10.2 New VSDK patch

BOSCH VSDK recently patched a vulnerability in one of its components. The updated component is included in BIS4.9.1

2.1.10.3 Password handling for logbuch_query, logbuch_w, db9000_query and db9000_w account

- Since version 4.9 the BIS installation no longer uses hard-coded passwords. For each of these BIS SQL Server user accounts it generates a new random password.
- The following password policy is enforced:
  - Minimum 12 characters length
  - 1 uppercase
  - 1 lower case
  - 1 decimal digit
  - 1 special character from the following set:
    `~!@#$%^&*_-+=|(){}[]:<>,.?/`
- The generated password will be stored in an encrypted file and will be used by the BIS backend services.

Note that an upgrade from version BIS 4.8 or older versions will not create new random password, instead it uses the existing hardcoded password. Hence it is recommended that you change these passwords after upgrading to BIS 4.9.1, using the ChangePassword tool located in the installation folder `MgtS\Tools\ChangePassword\`. It is not necessary to change passwords that you already changed using the ChangePassword tool.

2.1.10.4 Removed ServiceStatus from IIS deployment

- Due to security issues, from BIS 4.9 onwards the service health check web application ("ServiceStatus") is no longer installed by default as part of IIS, and will be removed by the installation procedure.
- If required, the tool is available at "<installation folder>`\MgtS\Tools\ServiceStatus`". In order to use this, copy the entire contents into "`C:\inetpub\wwwroot`".
- Open a Chromium-based browser at the URL "`https:\\[SERVERNAME]\dashboard.html`" to display the service status.

2.2 Access Engine (ACE)

2.2.1 Integration of OSS-SO offline locks

Offline locking systems of the OSS-SO standard are now supported by BIS-ACE. In this first version of OSS-SO integration ACE supports locks from Uhlmann&Zacher.
MIFARE DESfire EV1 cards are used.
For updating the authorizations (from 24h to several days) on MIFARE cards, LECTUS Select Readers are used.
Bosch offers a web-based configuration tool to map the Uhlmann&Zacher site configuration to an offline locking system within BIS-ACE.

Limitations:
One locking system (OSS-SO “site”) only
One card technology (MIFARE DESfire) only
A maximum of 10 update readers of type "LECTUS select"

The OSO card initialization of OSO file 1 and 2 is performed externally (for example by Uhlman&Zacher)

Files are 288 bytes in size, with up to:

- 3 time models
- 2 week models
- 2 time intervals
- 72 authorizations

The following Bosch and OSS-SO features are not supported:

- Divisions
- Hierarchical DMS systems
- ACE SDK
- Visitors
- Import/Export of OSO cardholders
- OSO battery or reader states
- OSO logbooks
- OSO blacklists
- OSO reports

2.2.2 Secure DTLS protocol for MAC/AMC communication

In ACE 4.9.1 and later, AMC controllers communicate with MACs via the secure DTLS protocol. For this, every AMC controller that is enabled requires

a device communication password (DCP). You can set DCPs for all AMCs in a top-down manner in the device editor. Alternatively you can set individual DCPs initially using the AMCIPconfig tool, and add the DCPs in the device editor afterwards.
See the ACE and/or AMCIPConfig manuals for detailed instructions.
See also Known limitations for **Access control hardware devices** (4.3 below).

3 Resolved issues in BIS version 4.9

3.1 Platform

The following issues have been resolved for BIS 4.9.1

Resolved issue #**158964**: Change Error message with error icon, if reload of BIS config fails.

Resolved issue #**178991**: Audit Trail, setup: There is no warning during setup when there is insufficient space (less than 15GB) available.

Resolved issue #**181056**: Setup: Pre-requisites window shows "Windows 10" on Windows Server 2016 PC

Resolved issue #**231734**: Inappropriate application icon of OPC compliance test tool BISOPCComplianceTest was replaced with proper icon

Resolved issue #**280266**: Setup does not check password complexity for SQL Database **sa** user.

Resolved issue #**283514**: In the configuration browser the Audit trail report gives a warning for the internet explorer if the server name not in the browser's trusted sites.

Resolved issue #**340754**: The configuration browser sometimes stops when configuring OPC UA with Certificate Authentication.

Resolved issue #**342465**: A BIS-created OPC UA certificate is not used by the BIS-UA Client, so IndraControl worked only with the "None" option in BIS 4.9

Resolved issue #**343158**: "CreateBISCertificate" popup message will appear when trying to install BIS ConnectionServer installation in BIS 4.9

Resolved issue #**343603**: Configuration Browser stops after a second scan of a DWF on certain Virtual Machines

Resolved issue #**353225**: Setup: The Mgts-Service password check gives irrelevant information

Resolved issue **#359011:** Using a user different from `sa` for Reporting services during setup

3.2 Access Engine (ACE)

The following issues have been resolved for ACE 4.9.1

Resolved issue **246461**: **Card types not correctly activated after update**
On AMS/ACE update the active card types are no longer overwritten.

Resolved issue **269523**: **MAC online/offline state is not shown correctly**

Resolved issue **270449**: **Temporary cards are not assigned to intrusion panels.**
Temporary cards will now be assigned to intrusion panels if the card type is supported and this card replaces the intrusion card.

Resolved issue **249850**: **Fingerprint W2 reader firmware stops reading cards if the reader is not used for long periods (>= 2 weeks).**
Only affects some card types in special configurations.
Provided firmware "bew2-oap_v1_1_5_bosch_20210419_170700_sign.bin" must be updated manually to avoid this error. It is located in the same folder as the BioIPConfig tool in the installation media.

Resolved issue **287009**: **ACE failed after setup when the server name contained the letters “APP”**
Server name can now contain the word "APP".

Resolved issue **326143**: **During the repair setup, the setup of the certificate tool fails**

Resolved issue **335631**: **It isn't possible to change a reader type to a reader type using another firmware at one AMC in the device editor.**
The reader type can now be switched to other protocols by removing the AMC firmware version and replacing with new one in device editor.

Resolved issue **#336792: Additional cipher suites**
RabbitMQ has now been updated to support additional secure cipher suites “ECDHE-RSA-AES256-GCM-SHA384” and “ECDHE-RSA-AES256-SHA384”. Thus cipher suites “AES256-SHA256” and “AES256-GCM-SHA384” can now be disabled in case of security concerns.

Resolved issue **340427. The OPC messages Disk nearly full and Disk full are not being sent to BIS**

Resolved issue **340743**: **ACE-Authorizations: no Otis elevator shown**

4 Known limitations in BIS version 4.9.1

4.1 Platform

In a hierarchical BIS system, the Consumer computer cannot accept or delete alarms containing Action Plans from the Provider computer.
Workaround: On the Consumer client computer install the certificate from the Provider computer.

If the .NET 5 hosting bundle is installed before IIS then the SmartClient login page is not displayed, and there are no BISIdServer logs in the S3K_Logging folder.
Workaround: Execute `dotnet-hosting-5.0.5-win.exe` to repair the installation. It is delivered with the BIS installation package, and can be found at *<BIS Installation media>\3rd_Party\dotNET\5.0*

Report print
If you have not updated your SQL server 2016 in recent years, then Report print may not work.
Workaround: A Microsoft cumulative update needs to be executed manually.
https://support.microsoft.com/en-sg/help/4505830/cumulative-update-8-for-sql-server-2016-sp2

#225890:
Installer/Licensing/BIS manager does not check the Windows profile type before continuing.
If the Windows login session is using a temporary profile, the current BIS installation cannot detect it. It continues the installation. The installation may need to be repeated when you are logged into Windows with the full profile.
Workaround: If Windows warns you that you are running with a temporary profile, then first repair Windows and log in with a full profile in order to install or configure BIS. Do not install or configure BIS if running with a temporary profile.

#243483: Configuration browser is able to scan OPC UA, but BIS cannot connect
Cause: OPC UA server enabled with IPv6 is supported by the Configuration browser but not supported by the BIS server.
Workaround: Disable IPv6 and use only IPv4.

#268122:
Audit trail report failed to export to Microsoft Word (Spanish).

It is not possible to export the audit trail report in Word format. The Event log report is not affected.
Workaround: For the Audit trail report, it is recommended to use another format, such as Excel or PDF.

#313830:
Superfluous certificate reminders upon closing the BIS Configuration Browser.
In rare cases, on fresh installations, when closing the BIS Configuration Browser, it prompts you to add the certificate to the trusted store.
Workaround: Click **Yes** – the popup window will not reappear, and the audit trail will continue to work as normal.

#337338:
BIS Client at Windows 10 OS fails to install .NET Framework 3.5 from https://<server-hostname>/ClientDeploy/Tools.aspx
Workaround: Open the Windows installation media. Open a command prompt as administrator, and type in the following command (**x:** represents the drive letter and path of the windows installation media)

```
DISM /Online /Enable-Feature /FeatureName:NetFx3 /All /LimitAccess /Source:x:\sources\sxs
```

Wait until the installation has completed.

#355988: Simultaneous commands to different detector types
If you select multiple detectors of different types in the BIS client and send the same command to all of them, then, if that command exists on more than one of the selected detector types, the command will be executed on only one of them.
Workaround: Avoid using the same command name on different detector types.

#358307:
The BIS time scheduler cannot be configured to remain switched off for an **Extra day** without time intervals.
Workaround: On the extra day, set Time1 to `00:00 00:00`

Running the BIS Client on virtual machines
On virtual machines, BIS clients that use HTML pages with floor plan graphics may experience problems such as a failure of the client to start after logging in, or a failure to close completely after logging out.
Cause: The BIS client needs dedicated graphic card memory to display graphics in HTML pages, and some virtual machines do not provide this.
Workaround: Disable floor plans in the HTML page viewed in the BIS client on the virtual machine.

4.2 Access Engine

As of Version 4.9.1, BIS-ACE no longer supports the RS-485 or RS232 MAC to AMC host interfaces.

#218631: The Importer/Exporter tool does not import or export Person records of type W (Guard).

#282775: If you configure Threat Level Management the commands may not appear in context menus in the BIS Client.
Workaround: In the BIS Configuration Browser, re-synchronize the Access Engine with BIS. Go to **Connections** > **Connection servers**, right-click **Access Engine** and select **Synchronize**.

#329012: BIS ACE setup does not work if 8.3 filenames are disabled
Despite an apparently successful setup, some ACE features (mainly intrusion) do not operate correctly if filename format 8.3 is disabled in Windows.
Workaround:
Before installing BIS, ensure that 8.3-format filenames are enabled. Start the command shell as Administrator, and run the command:

```
fsutil 8dot3name query
```

The result should be: 0
If not, execute the command

```
fsutil behavior set disable8dot3 0
```

#339261, 339262:
We recommend that each Visitor Management user (receptionist, administrator, or host) work under a personal Windows account, so that any browser data is stored independently.

#323446: Readers of type LECTUS select or LECTUS duo appear online but do not react to AMC communication
Disabling the secure OSDP channel checkbox in the device editor does not disable the secure channel on the reader; it will only cause the access control system to use unencrypted communication. The reader can still be polled and appears to be online, but it continues to reject any unencrypted communication.
Workaround: Either re-enable secure communication or reset the reader hardware to its factory default state, which allows unencrypted communication. To reset the reader please refer to the reader manual and reset the OSDP secure channel using the reader's DIP-Switches.

#342685:Microsoft print to PDF and Microsoft XPS document writer
Microsoft PDF print does not work from .NET dialogs on any operating system.
Workaround: use other PDF printer drivers, such as doPDF.

#361710 Operator login by reader
In the Dialog Configuration browser > **ACE Workstations** > tab:**Workstations** do not use the option **Login via reader**.

#336189: .NetCore 5.0
The BoschCertificateTool requires the .NetCore 5.0 package
On remote SQL Servers, install Microsofts .NetCore 5.0 package before using the BoschCertificateTool. On BIS login servers the .NetCore 5.0 package will be installed automatically by the setup.

#357145: Using wrong credentials with the ACE SDK
The ACE SDK repeatedly attempts to log in to the ACE BISLoginService if invalid credentials are used, even if the application that uses the SDK is closed.
Workaround: Avoid using ACE SDK with wrong credentials.

#248449: Group access for revolving doors
Group access for revolving doors is only supported if the whole group fits into one compartment of the turnstile.

#332685: Hierarchy: MAC Synchronization in Configuration browser
In a hierarchical system the MAC can be resynchronized by command in the Config browser. This removes all devices below MAC are removed and re-adds them to the BIS configuration.
WARNING: This action will also remove the devices from any “Address lists”, “Associations” and “Detector placements” where they are used.

#248582: Limitation on Random screening
Random screening timeout values below 5 minutes can be configured, but the check is only done every 3 minutes.
Workaround: Do not configure Random screening timeout below 5 minutes.

#216031: BIS states "Random screening" or "Palm vein verification" do not reflect settings made in the Configuration Browser
The enable/disable states for *Random screening* and *Palm vein verification* in the Configuration Browser are not correctly reflected in the BIS Client.
Workaround: Re-send the commands from the BIS client.

#219598: Displayed status of subsidiary devices when offline

When a device (e.g. AMC) is offline, the status of its subsidiary devices (e.g. extension boards) may not be displayed accurately.
Workaround: Make sure that the main devices (DMS and MAC) are continuously online.

26 29

#313246: Door Model 05 (Parking lot)
BIS-ACE 4.9.1 cannot use door model 05 (Parking lot) for Threat Level management.
Workaround: Define an association in BIS to control the boom barriers of parking lots.

Initializing passwords of service user accounts for ACE-API-based applications
Before the service user accounts will work, their passwords need to be set in the BIS classic client or Smart Client.
This affects user accounts created in BIS Configuration Manager as service users for ACE-API applications, such as the Importer/Exporter, Visitor Management or third-party applications.

Workaround: Before installing the ACE-API application, start the classic or smart client, and log into the newly created user account. Set a password in accordance with your password policies.

FQDN (fully qualified domain name)
FQDNs are currently not supported by the ACE dialog manager.

#355988 Simultaneous commands to different detector types
If you select multiple detectors of different types in the BIS client and send the same command to all of them, then, if that command exists on more than one of the selected detector types, the command will be executed on only one of them.
Workaround: Avoid using the same command name on different detector types.
In ACE the **Restore Configuration** command is implemented on both doors and readers. To avoid this problem, create a copy of the command in the detector types configuration, and give it a different name, for example: **Restore Configuration (Doors)**, and remove the original command from that detector type (here doors).

BioEntry W2 Fingerprint Readers

#199503:
The BIS Client becomes unstable if you try to enroll a fingerprint after the fingerprint reader has lost its network connection

Workaround: During fingerprint enrolment, do not disconnect the reader from the network. 27 29

#220970:
Fingerprint readers that use PoE (Power over Ethernet) must not draw power from an AMC at the same time. This will damage the reader and void your warranty.

#243864:
Synchronization from ACE to fingerprint readers does not work for unknown card types
Workaround: Make sure that the card type and coding are set correctly when enrolling the cards. These must match the card type and coding of the fingerprint reader.

Limitations - fingerprint BioEntry W2 reader

- Approximately 5-10 minutes are needed to synchronize 25 readers with 1000 cardholders and their fingerprints.
- From a technical perspective, up to 200 W2 fingerprint readers are supported in the templates on device, or templates on server modes. To achieve best performance, we recommend the use of no more than 100 readers.

General recommendations for fingerprint readers
Avoid using fingerprint readers for groups of persons that require temporary authentication, such as visitors. If unavoidable, use the template on server mode for the best performance.

Visitor Management

#327038: Visitor Management – identical visitors not editable in BIS-ACE
If visitors are created with same last name, first name and birthday, then the Visitor dialog in BIS-ACE will show the error message that the visitor already exists.
Workaround: Disable the unique key check in the registry key
`\HKLM\SOFTWARE\WOW6432Node\Micos\SPS\DEFAULT\PersData\PkUnique`
Set `@value` to `00`

#282466: Visitor Management – Card reader not working if used by BIS-ACE and Visitor Management

If a LECTUS enroll 5000 MD reader is in use by the BIS-ACE Dialog Manager, it cannot be used by Visitor Management simultaneously.
Workaround: Stop the Dialog Manager before using enrolment in Visitor Management, or use a different type or a second enrollment reader in the Dialog Manager.

4.3 Access control hardware devices

With DTLS-Support AMC will no longer support RS485 or RS232 connections between Host (MAC) and AMC.
Disable or remove from your configuration all AMCs that are configured on COM ports. Until you do this the device editor cannot finalize the migration, that is, it cannot save the configuration.

DTLS allows only one connection to AMCs at a time

- The AMCIPConfig tool is no longer able to change AMC settings (IP address, Firmware, passwords) if the AMC is still connected to a MAC. Disable the MAC connection first.
- Conversely, the MAC is not able to connect to an AMC if it is still open in the AMCIPConfig tool. Close AMCIPConfig first.

With BIS 4.9.1 the bootloader has been updated to version `00.62 v02.30.00 LCM` AMCs will be updated automatically by BIS 4.9.1.
If you wish to update AMCs manually using the Bosch.AMCIPConfig-Tool:
If the AMC has Bootloader `V00.49` and earlier, you must first update to `V00.61v01.47.00`
And from there to `00.62 v02.30.00 LCM`

Firmware downgrades: If you wish to use an AMC that has been upgraded to BIS 4.9.1 or AMS 4.0 on an older access control system (ACE, AMS or APE) then an AMC firmware downgrade is necessary: Firmware versions `V00.62` must first be downgraded to `V00.61` before they can be downgraded to older versions.

#339756
Reader input/output signals for **LECTUS select** (LCTSL) cannot be configured in the device editor (Entrance node > **Terminals** tab).

#328222
When reassigning the names or IP-addresses of AMCs in the device editor, make sure that you never have two or more AMCs with the same name or IP-address simultaneously. If you want to swap the name or address of two AMCs, the recommended procedure is:

1. Reassign one of the AMCs involved to an unused dummy name or address, save it.
2. Reassign the other AMC to the intended name or address, save it.
3. Reassign the first AMC from the dummy name/address to its intended name/address.

29 29

#240264
For AMCs input/output signals only conditions of type "state" can be used for the FOLLOW_STATE function.
The following conditions are of type “event”, and cannot be used with the FOLLOW_STATE function.

```
11 - Door n forced open alarm
12 - Door n left open
13 - Reader shows access granted
14 - Reader shows access denied
23 - Messages to readers
24 - Messages to devices
25 - remote control Function set
```

5 Compatibility updates

BG900 reader protocol
Support for the BG900 reader protocol is approaching end-of-life, and is not guaranteed beyond the end of 2021.
Workaround: For reasons of availability and security, Bosch recommends replacing BG900 readers with readers from the current portfolio.