Building Technologies

Building Integration System (BIS) version 5.0
RELEASE NOTES

2023-06

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

Version	Description
2	Building Integration System V 5.0 with CVE-2023-29241

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 32

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 2022 (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
The version 4.9.2 was the last version to support Windows 2016 server

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 2019 (64 bit, Standard, Datacenter) – Windows Server 2022 (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

5 32

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 2019 (64 bit, Standard, Datacenter) – Windows Server 2022 (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 5.0: Romanian added: The full list is now AR-EG, DE-DE, EN-US, ES-AR, FR-FR, HU-HU, NL-NL, PL-PL, PT-BR, RO-RO, RU-RU, TR-TR, ZH-CN, ZH-TW

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 112 or higher • Microsoft Edge, version 111 or higher • Mozilla Firefox, version 102 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 5.0

- 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 4.9.2, 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 of BIS 4.8 and later, 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.

- When upgrading from BIS 4.4 or older, please terminate the old ACE Card Personalization 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.
- After upgrading to BIS 5.0, the file `<BIS Install Drive>\MgtS\HTML-Login\Login.html` needs to be manually modified as below. The "ChangePassword" function expects 2 additional parameters, username and password, which will be used to connect to the BIS Server to retrieve the password policy from the BIS server.

  -Existing:
  ```
  onclick="document.all.LoginControl.ChangePassword();"
  ```

  -To be replaced by:
  ```
  onclick="document.all.LoginControl.ChangePassword(document.all.txtUserName.value,document.all.txtPassword.value);document.all.txtPassword.value='';document.all.txtPassword.focus();"
  ```

- Only for users of the Chrome browser
  After a BIS upgrade, if a certificate issue occurs in the Chrome browser, it may be due to root certificate creation. To solve it, create a new root certificate using the following procedure:.
  1. Open the computer certificate store:
  2. Press the Windows key + R to bring up the Run command, type `certlm.msc` and press Enter.
  3. Delete the BIS root certificate from the certificate store as follows:
     a. Go to Trusted Root Certificate Authorizations, select Certificates
     b. Select “Bosch Security System Internal CA - BISAMS” and delete this certificate
  4. Delete the BIS certificate from certificate store:
     a. Go to Personal, select Certificates
     b. Select “Bosch Security System Internal CA – BISAMS” and delete this certificate
  5. Run certificate tool located in <BISInstalledDrive>\MgtS\Certificates\BoschCertificateTool.exe
  6. Install the new certificate on all clients as described in BIS installation manual

- The setup program identifies any currently installed version of BIS.
  1. 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.

2. 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.
3. 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.
4. 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.
5. Windows updates must be paused during BIS installation, because they can interfere with it. Install all Windows updates before the installation.
6. 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 Post-installation steps for BIS 5.0 (CVE-2023-29241)

After installing BIS 5.0, update the Cybersecurity Guideline Document. For this purpose, a file named `BIS_5_0_21100_0_Patch1.zip` is available from the online product catalog and the download server, in the BIS 5.0 section.

Patch file details :
Name: `BIS_5_0_21100_0_Patch1.exe` (Product version : 5.0.21100.2)
Date modified 01.06.2023
SHA256:
`235E264CE3862D54E915E7461EA0752CC53B7D2CCB2E89340E85809116FB8766`

Update procedure

On the BIS server:
1. Extract `BIS_5_0_21100_0_Patch1.exe` from the downloaded ZIP file:
`BIS_5_0_21100_0_Patch1.zip`
2. Run `BIS_5_0_21100_0_Patch1.exe` as administrator

Notes:

- If you re-install BIS version 5.0, re-apply this patch also.
- Before updating to next BIS version, remove the Cybersecurity Guideline PDF file manually from <installation dive>: `\MgtS\Platform\`

1.7 Updating Access Engine (ACE) to 5.0

Updating dedicated ACE client computers

Before updating a dedicated ACE client machine to 5.0 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.

Alternatively the provisioning phase can be activated using the AMCs context menu 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.

1.8 Updating Service References in WCF applications

Introduction

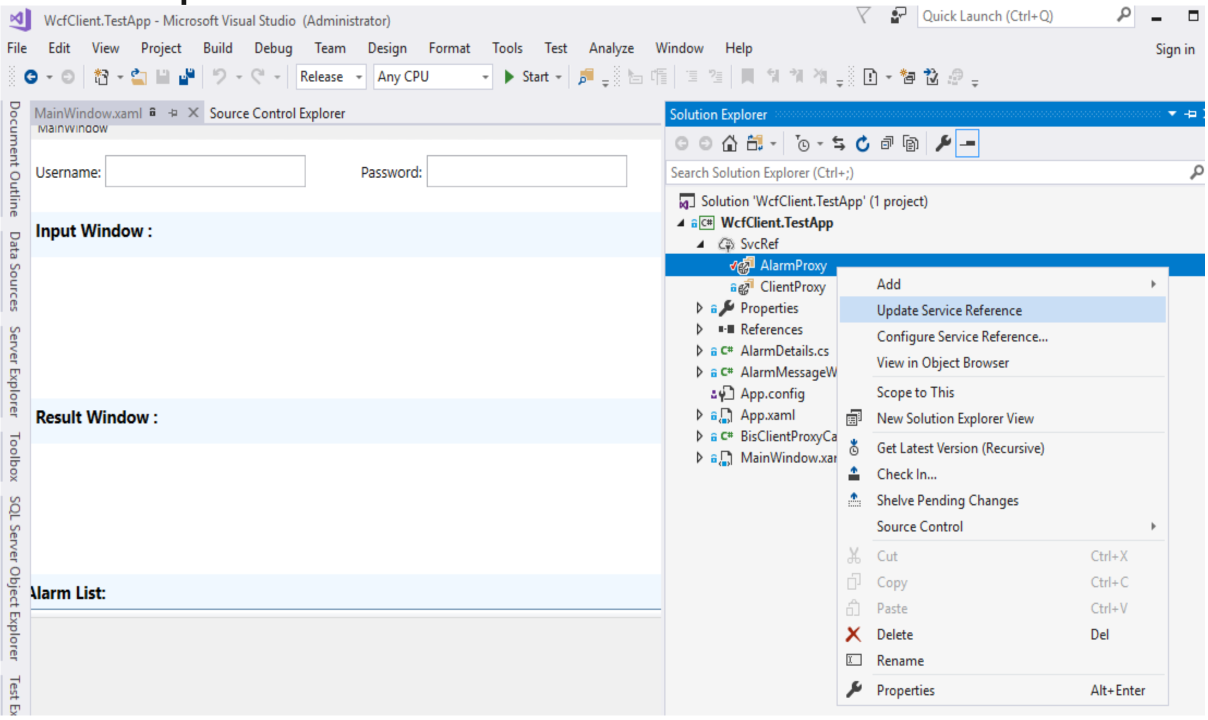
WCF (Windows Communication Foundation) client applications that were created based on an earlier version of the BIS WCF service will not work with a BIS version of 4.8 and above due to changes in the service **BISClientProxyWCFService**.

Remedy: After upgrading from a version below 4.8 to BIS 5.0, 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.

1.9 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 system locale, so it must be set manually:

- Regional Settings / Administration / Language for non-Unicode programs / Change system locale: select an Arabic language.
- Alternatively, run the *Set-WinSystemLocale* cmdlet with Administrator permissions. For example, **Set-WinSystemLocale "ar-SA"** sets the 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.

1.10 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.

1.11 Certificates require synchronized system clocks

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

1.12 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 from version 5.0

The limitations cited in this document are the maximum values that were tested by the time of publication of BIS 5.0 They do not necessarily reflect the absolute maxima for the system.

2.1 Platform

12 32

2.1.1 BIS Smart Client

2.1.1.1 Device Tree view

This release adds a new tree view tab to the Device Widget that presents devices based on logical device hierarchy and lets operators interact with all configured devices, even when they are not placed on a location. This complements the existing location-based tree view.

2.1.1.2 Working with sub-devices

In this release, Smart Client enables operators to work with sub-devices, i.e., “detector” and “sensor” levels below device groups. Operators can access these from the improved Device Widget.

2.1.1.3 Support for command parameters

Up to BIS 4.9.2, Smart Client only supported executing parameter-less commands or commands with fully predefined parameters. BIS 5.0 enables operators to execute the full set of available commands for all devices and will prompt the operator for input where needed. This works everywhere where the Smart Client has device commands, i.e., Device Widget, Map Widget, and action plans.

2.1.1.4 Extended support for Address Lists

Smart Client in BIS 5.0 improves the handling of Address Lists by presenting all fast commands, standard device commands, and states for devices in a list.

2.1.1.5 Password change from Smart Client

Logged-in operators now have the option to change their BIS password from the user menu in Smart Client. Changing the BIS password from Smart Client affects all BIS applications including the classic Windows Desktop client and ACE applications, and enforces the newly configurable password complexity rules in BIS 5.0 as do other parts of the BIS platform.
In summary, the Smart Client now has the same password-changing capability as the classic client.

2.1.1.6 Improved map rendering

BIS 5.0 adds support for additional DWG/DXF geometry types, increasing the performance and the display of maps.

2.1.1.7 Bug fixes

- Security improvements in the .NET Core

- Alarms can now be sorted in any direction
- Operators can now see action plans for alarms accepted at a different workstation
- Fixed: Occasional crash in Map Widget when selecting alarms with a location.
- 90+ additional minor bugs and performance issues addressed

2.1.1.8 Limitations in BIS Smart Client version 5.0

- The 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
- 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
- Smart client does not support BIS "Miscellaneous documents"
- Smart client has no print command [Workaround: use the browser print command].
- 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.

- Using the BIS Configuration Browser, you can place detectors directly at a location via the Detector directly at location tab in the **Detector placement** view.
  In the Smart Client, if you have placed 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]: In the Configuration Browser, do not place address lists at a location, place individual detectors from that list instead.

2.1.1.9 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.

2.1.1.10 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 4.9.2. 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 was 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 4.9.2 program folder, located under:
<installation drive>:`\MgtS\Tools\ChangePassword`

2.1.2 More concurrent operator clients

The previous limit of 80 concurrent operator clients has been raised to 120. This limit refers to one sum of all clients, both “classic” and “smart”.

2.1.3 OPC UA library update

Version V5.70 of OPC UA C++ SDKs integrated

The new version V5.70 of our **OPC UA C++ SDK** now provides a set of additional functionalities:

New features:

- PKIStoreConfiguration paths can be initialized via base path
- PKI store option to allow partial chains
- Store rejected certificate chain as separate files
- Update to OpenSSL 1.1.1m

Bug fixes:

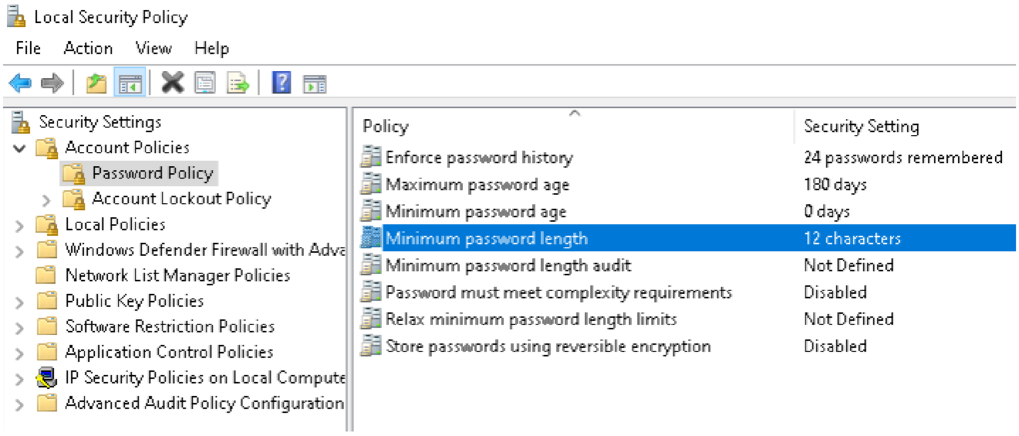
- Application: create SelfSignedCertificate now stores private key in password protected PEM format
- Significant improvement in OPC UA server connectivity from BIS

2.1.4 Support Windows Server 2022

Support of Microsoft Windows Server 2022 as BIS Login Server, BIS Connection Server and BIS Client

2.1.5 Password policy enhancements

The length of the BIS login password is now synched with the Windows password policy.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	24 passwords remembered
Maximum password age	180 days
Minimum password age	0 days
Minimum password length	12 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Disabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

- - In BIS 5.0 only the length of the password is customizable. Instead of using predefined password length, the password length is retrieved from the Windows password policy, which is configured using the Windows **Local Security Policy > Account Policies > Password Policy**
  - On the BIS Login server:
    - If the minimum password length is configured as 0 to 3 characters, then due to other non-modifiable BIS password policy as below, BIS uses at least 4 characters for new password
    - At least 1 uppercase letter
    - At least 1 lowercase letter
    - At least 1 decimal digit
    - At least 1 of the following special characters
    - `` `!@#$%^&*()_+?>/<;:-., ``
    - NO upward or downward sequence of more than 3 alphanumeric characters (case insensitive), e.g. aBcd, 2345, ZyXw
  - If the minimum password length is configured to more than 50 characters, then BIS nevertheless uses a maximum of 50 characters for new password
- The **Change Password** dialog will display the configured password length during change password process.
- The changes above are applicable to both the BIS Classic Client and BIS Smart Client.

Limitation:
The password length-check applies only to the password-change function.
It does not affect previously set passwords.

2.1.6 SQL Server 2019 support

2.1.6.1 Operational information

- For new installations of BIS 5.0, SQL Server 2019 Express edition will be installed, if you are not using your own purchased version.

2.1.6.2 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.

2.1.7 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.

2.1.7.1 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.

2.1.7.2 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.

2.1.8 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.
- If the key used by ChangePasswordTool is missing, then upon launching this tool will detect it and provides an option to generate a new key, after which all the user's password must be changed.

2.1.9 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.

2.1.10 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`.

2.1.10.1 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.

2.2 *Access Engine (ACE)*

Security updates

Update of Microsoft libraries.
Update of Wiegand AMC firmware file.

3 Resolved issues in BIS version 5.0

3.1 Platform & BIS Smart Client

#221003: The Configuration Collector has been enhanced to include the log files generated during installation, in the `%temp%` folder

#268122: Audit trail report now exports to Microsoft Word in Spanish and Romanian.

#340033: When the Configuration Collector, retrieving system information, times out or fails, a valid error message is now displayed.

#340465: The correct command is now executed, even if different detectors have same command name.

#370247: The BIS setup will abort if FIPS is enabled, or if the installing user does not have local Administrator rights. A valid error message is displayed.

#371587: If any encryption-related issue is encountered while using ChangePassword tool, then the tool itself provides instructions to generate a new encryption key, and use it for generating new passwords.

#371934: Document `BIS_Firewall_Configuration.pdf` is replaced with the more generic document `Cybersecurity_Guidebook_for_BIS_and_Access_Control_Systems.pdf`

#371956: If there are no detectors in a group, then the license count considers that group as one detector.

#373507: The BIS Client now able to use the auto-login function with Windows credentials, and can also open Access Engine dialogs

#381833: Optimized DWF file handling prevents crashes when loading very large files.

#382929: Older events will be cleaned up more efficiently by a background process (the Event-log manager) when the Event log is nearly full.

#384508: The Restore process now replaces the file `BisClientProxyWcfServer.exe.config` only when necessary. (An upgrade from version 4.7 will replace the file. For older BIS versions the installed `.config` file will not be replaced.

#386243: The description of the parameter **Delete alarm after timeout** has been updated in the BIS Configuration online help.

#387331: It is again possible to install a BIS Connection server, even if IIS is not installed on that machine.

# 387344: The description of LDAP login has been updated in the BIS Configuration online help.

# 391302: In multi-server BIS, the connection between a Provider and Consumer is now properly restored after a disconnection or network failure.

# 391332: The Configuration browser's **Association** screen has been expanded to view more associations at once.

#411148: When a firewall blocks any of the ports used by the BIS Classic Client connection after successful connection with BIS Server, then the BIS Classic Client will now log off immediately.

#412347: The BIS Client will no longer allow access to the BIS server via a URL containing `localhost` or a loopback IP address starting with `127`. Access is now allowed only by hostname. An error message is displayed.

3.2 Access Engine (ACE)

The following issues were resolved for ACE 5.0

This list Includes patches that were already released for BIS 4.9.1 and 4.9.2.

#329005 ACE SDK enhancements:. See separate SDK documentation in the AddOns folder.
#371946 Support has been added for older PegaSys time-model cards, used in MIFARE systems.
#371989 The AMC firmware has been updated to prevent the delays that were observed in rare cases.
#374846 Access Engine OPC area counters are now correctly shown in BIS.
#380152 The OSS-SO tab page in the Dialog Manager now only appears if the license is active.
#396041 The Device editor now allows the changing of reader types for door model 01b.
#400061 The IO-functions for AMC in the Device editor now work in all supported languages.
#405744 Certificate generation now works for Google Chrome also.
#412047 A person moved to division X is now only visible to operators of division X.

4 Known limitations in BIS version 5.0

23 32

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.

#**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.

#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.

#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.

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

#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.

#243753 Import-Export – Delete of cards failed.
If you start an import process of type “delete”, and it refers to cards that do not exist in the database, then the whole import process will fail.

#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.

#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.

#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**.

#313246: Door Model 05 (Parking lot)
BIS-ACE 4.9.2 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.

#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
```

#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.

#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 the MAC and re-adds them to the BIS configuration.

NOTICE: This action will also remove the devices from any "Address lists", "Associations" and "Detector placements" where they are used. This will require you to reconfigure all the elements above.

#336189: .NetCore 6.0

The BoschCertificateTool requires the .NetCore 6.0 package

On remote SQL Servers, install the Microsoft .NetCore 6.0 package before using the BoschCertificateTool. On BIS login servers the .NetCore 6.0 package will be installed automatically by the setup.

#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.

#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.

#354408 LECTUS select – after reenabling encrypted communication the last access is sent from the reader to the AMC

If LECTUS Select reader communication is encrypted, and you reset the reader device with the DIP switches, then the data of the last card that was presented to the reader is retained, and cannot be sent to the AMC.

As soon as encryption is reinstated, then the data of the last card will be sent to the AMC.

#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.

#357145: Using wrong credentials with the ACE SDK

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

#361710 Operator login by reader

In the Dialog Configuration browser > **ACE Workstations** > tab:**Workstations** do not use the option **Login via reader**.

#397466 Special day configuration reset to default on update

Any customization of the default special days (Easter, New Year, etc.) in an ACE or AMS configuration will be reset to factory defaults by an update installation. This does not affect special days that you have added manually.

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.

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).

#412698 Communication between AMCs and MAC is disabled if the Device Editor is in demo mode

If the demo mode is activated in Configuration Browser, and you switch afterwards to the Device Editor, the communication cannot be activated, even if you refresh the device tree.

Workaround: Restart the Configuration Browser after activation of demo mode.

#413408 After installing ACE

After a new installation of the BIS client with ACE, you must reboot the computer. If you do not do this, then the ACE Dialog Manager may close the BIS Client unexpectedly, without any error message.

In addition: on *first use* of the Access Engine Dialog Manager after an installation, always run the BIS Client as Administrator.

#414592 The Synchronize command on the MAC detector type

The **Synchronize** command on the MAC detector type may not work correctly if the SQL database is not available at the time the command is issued.
The impact is that data will be missing in the MAC and AMC.
Workaround: If you cannot guarantee that the SQL server is always reachable and stable, we recommend removing this command from the available BIS commands.

#416794 Configuration Browser – Spurious error message while navigating to ACE Licenses

If you select the ACE **Licenses** dialog, then the BIS error log file will receive the error message: `Failed to resolve current usage value for key 'MaxNoOfLocks'!`
This error can be safely ignored.

#416940 #416946 #416953 #416955 When moving persons or visitors to another division, always check and adjust their authorizations afterwards

If you change a person's division using the **Personnel data** > **Change division** dialog, or the API/SDK, verify that the person's authorizations are still valid after the move.
The **Personnel data** > **Cards** and the **Visitors** > **Visitor** dialog will automatically correct by re-adding authorizations from their authorization profiles, if any are lost in the move.

Workaround: Change some cardholder data in the **Personnel data** > **Cards** or **Visitors** > **Visitor** dialog, to re-synch the cardholder with his authorizations.

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.

#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.

Note on achieving EN 60839 access-control standards

EN 60839 is a family of European international standards for the hardware and software of intrusion detection and access control systems.
Measures to ensure compliance of your access control system with EN 60839 are described in the ACE Configuration online help. Two additional points did not make the editorial deadline for the online help, and are therefore listed here:

- The status of all entry points, primarily doors and windows, must be monitored; for example through electric contacts.
- Visitor Management does not support EN-60839 Class 4. Installations that include Visitor Management can attain a maximum of Class 3.

Visitor Management

#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.

#327038: Visitor Management – identical visitors not editable in BIS-ACE
If you try to create a visitor with same the same last name, first name and birthday as an existing visitor, 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`

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.

As of BIS 4.9.1 the bootloader was updated to version `00.62 v02.30.00 LCM` AMCs will be updated automatically by BIS 4.9.2.

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 and later, or AMS 4.0 and later, 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.

#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.

31 32

```
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
```

#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.

#339756

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

#411272

If the time setting on an AMC differs by more than 15 minutes from the time on its MAC, then communication between the MAC and the AMC will fail.

There are two independent workarounds

- Wait until the MAC sends the next time sync command. This can take up to 1 hour.
- Perform a Cold Start on the AMC

There are no side effects, except the AMC will be out of synchronization for a maximum of 1 hour.

5 Compatibility updates

32 32

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.