Building Technologies

BOSCH

Building Integration System (BIS) version 4.9 Release Notes

2021-07

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

Version	Description
1	2021-04-27 Initial version
2	2021-05-31 Updated with Smart Client features and its limitations
3	2021-06-10/11 Review of all contents
4	2021-06-30/-07-06 Further additions

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
1.1 Supported operating systems 3
1.2 Server 4
1.3 Operator Client 4
1.4 Smart Client 6
1.5 Updating BIS to version 4.9 6
1.6 Updating Service References in WCF applications 7
1.7 Settings required for Arabic installations 8
1.8 Advice for security of personal data 9
1.9 Certificates require synchronized system clocks 9
2 New features in version 4.9 10
2.1 Platform 10
2.1.1 BIS Smart Client 10
2.1.2 SQL Server 2019 support 12
2.1.3 Setup Enhancement 13
2.1.4 New Certificate Tool 13
2.1.5 ChangePasswordTool Enhancement 14

2.1.6 Fully Qualified Domain Name (FQDN) Support........................14
2.1.7 Access Reporting service using Domain Account Support.......14
2.1.8 Configuration Collector enhancement.....................................15
2.1.9 Security Improvements..15
2.1.10 Improvements to default documents......................................16
2.2 Access Engine (ACE)..17
2.2.1 Visitor Management...17
2.2.2 Occupancy Monitor...17
2.2.3 "IDEMIA Universal BioBridge" Integration................................18
2.2.4 Mode override...19
2.2.5 Extended filters...19
2.2.6 PegaSys and LEGIC advant cards..19
2.2.7 Temporary cards for intrusion systems....................................19
2.2.8 New report layout...19
2.2.9 Key Management Tool for LECTUS select and MIFARE DESFire 20
2.2.10 AMC Bootloader...20
2.2.11 IP Configuration Tool..20
2.3 Video Engine...20
3 Resolved issues in BIS version 4.9.......................................21
3.1 Platform...21
3.2 Access Engine (ACE)...22
4 Known limitations in BIS version 4.9.....................................22
4.1 Platform...22
4.2 Access Engine..25
5 Compatibility updates...30

1 Installation Notes

3 30

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 1909 Build 18363 or Version 2004 Build 19041)	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 LTSB (64 bit) – 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 i5 processor with at least 4 physical cores – 8 GB RAM (32 GB recommended) – 200 GB of 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 – 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) 5 30 – Windows Server 2019 (64 bit, Standard, Datacenter) – Windows 10 (32 or 64 bit, Pro or Enterprise LTSB) – 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
Minimum hardware requirements	– Intel i5 (Gen 6 / Skylake or newer) or higher, multiple cores – 8 GB RAM (16 GB recommended) – 20 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 or higher – For camera sequencing, virtual matrix or Multiview add 4GB RAM – Latest video drivers are highly recommended. Use the Windows dxdiag tool to make sure drivers are no more than 1 year old

Supported languages in 4.9: 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 with at least 6th Generation & min 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

- 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 the previous version of *BISProxyOPCDA* is already installed, unregister the previous version of *BISProxyOPCDA*, replace it manually with the new version delivered with BIS 4.8/4.9, 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 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 Personalisation service (CP) before starting setup. Right click the CP system tray icon and select the bottom option “End program”. Alternatively just 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 an older than or equal version 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 Service References in WCF applications

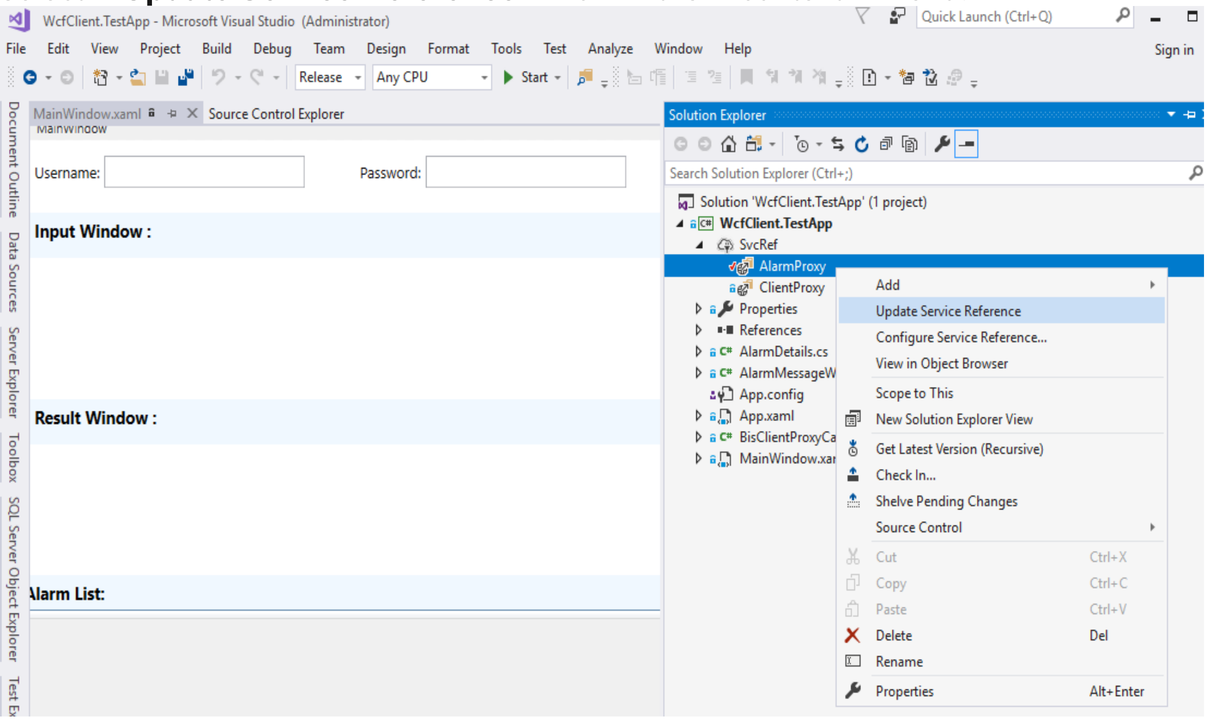
Introduction

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 below 4.8 due to changes in the service **BISClientProxyWCFService**.

Remedy: After upgrading from a version below 4.8 to BIS 4.9, 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.

1.7 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.

1.8 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.

1.9 Certificates require synchronized system clocks

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

2 New features in version 4.9

Notice!
The limitations cited in this document are the maximum values that have been tested by the time of publication of BIS 4.9 They do not necessarily reflect the absolute maxima for the system.

2.1 Platform

2.1.1 BIS Smart Client

BIS 4.9 includes BIS Smart Client, a modern, browser-based client that helps you stay on top of security operations at all times. No special license is needed for the Smart Client.

2.1.1.1 Major features in this release include:

- Configure flexible workspaces and dashboards comprised of widgets, which are reusable, modular user interface components
- Login from Smart Client using BIS credentials or Active Directory operator
- Workstation based authorization and IP filtering is supported
- Review and handle alarm messages from the alarm widget
- Use basic action plans to provide additional information and instructions based on alarm type and location
- View maps of your building, view devices and alarm states, and interact with devices on the map through commands

2.1.1.2 Limitations in version 4.9

- 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 or configuration backup or configuration collector will not back up the configurations related to workspaces/dashboards
- Default locations (Location tree root node, 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 at required places, and link detectors to the hyperlinks in the floor plan]

- 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 dialog]
- Displaying layers based on alarm states is not supported in Smart Client
- 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 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 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 file 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.
- After performing a repair installation or adding/removing features to/from BIS, Smart Client may no longer be able to connect to its SQL Server instance. As a consequence, you will be able to log into Smart Client, but Smart Client will no longer be able to load workspaces and dashboards. [Workaround: reset the password for the Smart Client database user using the "BIS Change Password Tool", under `<installation drive>:\MgtS\Tools\ChangePassword`].

2.1.1.3 Manual backup of workspaces and dashboards

12 30

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 needed. Note that this will remove any workspaces and dashboards that may have been created in the meantime.
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 restore parameters as needed.
6. Click "OK" to restore the "SmartClient.Shell" database from backup
7. Using IIS Manager, start the Smart Client application again by starting its application pool.

2.1.2 SQL Server 2019 support

2.1.2.1 Operational information

- For new installations of BIS 4.9 SQL Server 2019 Express edition will be installed if you are not using your own purchased version.

2.1.2.2 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.

2.1.3 Setup Enhancement

Always follow the instructions in the Installation Manual. The following is a summary for your information.

- BISRemoteSQLServerSetup\Install.exe is required only for remote SQL Server Reporting Services (SSRS) machine. For remote SQL Server alone, this tool is not required.

- Instead of manually creating MgtS-Service account, MgtS – Sharing folder, enable TCP/IP and enable Force Encryption flag for SQL connection, a new tool *BISAccessRights.exe* is located at "_Install\AddOns\BIS\RemoteSQL\BISRightsSetup\" folder. This tool is required for remote SQL Server machine.

- Manual RSConfig.exe setup is **not** required for local SSRS, it is required for remote SSRS only. **Note**: This additional configuration is required from SQL Server 2017 onwards.

2.1.4 New Certificate Tool

This tool replaces the old BWC config tool and the older certificate tool from ACE.

Use only those tools that are delivered in the same BIS Version. Always follow the instructions in the Installation Manual.

The following is a summary for your information.

2.1.4.1 General information

- This tool will now create a single root certificate for BIS, ACE, ID-Service, SSRS and OPCUA instead of multiple certificates.
- New Certificate Tool is located on the BIS server machine after installation (<installation drive>:\MgtS\Certificates). The documentation for this tool 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.
- The BIS Client download certificate file name has been changed from MyCert.cer into "[SERVERNAME].CER"
- This tool has a separate configuration file for Remote SSRS certificate binding located at <Installation

media>\AddOns\BIS\RemoteSQL\Certificate. This is only for remote SQL Servers.

  - Do not execute the tool from this location for the BIS login server. If needed, always execute the tool from the (<installation drive>:\MgtS\Certificates folder.

2.1.4.2 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.

2.1.5 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.
  Note: See limitation for #340702 BIS Platform
- A new SQL user **smartclient** has been added for the SmartClient Shell DB.

2.1.6 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\Certficates*" 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.

2.1.7 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.

2.1.7.1 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.

2.1.8 Configuration Collector enhancement

You can now set the Configuration collector to collect log files for a defined period in the past.

"Last '14' days" is the default value. Enter 0 to collect all log files. The maximum value that you can enter is 99 days.

Limitations:

- The occasional remote SQL Server message: "The system cannot find the file specified" can be safely ignored. Press OK to continue.

2.1.9 Security Improvements

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

- BIS 4.9 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, using the Change Password Tool located in the installation folder `MgtS\Tools\ChangePassword\`.For passwords that you changed in previous versions, using the Change Password Tool, it is not necessary to change the passwords again.

2.1.9.2 Removed Critical information from webpage header

- The BIS web server no longer transmits security-relevant HTTP header information to the BIS client.

2.1.9.3 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.

2.1.10 Improvements to default documents

Changes in folder `C:\MgtS\Default_Configurations`
Deleted outdated action plans for Access Engine Default Configuration and added a new action plan.
Added `AP_AcccessExamplePlan.htm` to folder `\AccessEngine\ACE_Default_Configuration\Documents\Action plans\`
Moved "`AP_SecureVideoVerification.htm`" from `\Common\Documents\Action plans` to `\ACE_Default_Configuration\Documents\Action plans\`

2.2 Access Engine (ACE)

2.2.1 Visitor Management

BIS 4.9 supports the new Visitor Management application. The Visitor Management server setup must be executed on the same computer as the BIS login server. The BIS license to use the Visitor Management must be activated.

Data changed in Visitor Management are transferred directly to the access control system. Data changed on the access control system are synchronized every 5-10 minutes with the Visitor Management system.

The backup and restore of the BIS system includes the Visitor Management data.
The Visitor Management now supports all application languages.
The Visitor Management setup can be found in `AddOns\ACE\VisitorManagement` and must be installed on the BIS login server after installing BIS and ACE.

If you are using the Firefox browser, consult the English language online help or PDF manual for instructions on certificate handling in Firefox.

Limitations:

- Released for SQL Server 2019 only.
- If you restore a backup including Visitor Management on a second machine, run the Visitor Management repair setup after the restore. Ignore the error message from BIS restore.

2.2.2 Occupancy Monitor

BIS 4.9 supports the Occupancy Monitor where the current populations of configured areas (including parking areas) are displayed. For areas the count reflects persons, for parking areas it reflects vehicles.

The Occupancy Monitor setup is found in `AddOns\ACE\OccupancyMonitor` and must be installed on the BIS login server after installing BIS and ACE.

Limitations:

- Released for SQL Server 2019 only.

- Occupancy Monitor does not distinguish between divisions. The areas of all divisions are shown

2.2.3 "IDEMIA Universal BioBridge" Integration

Introduction

– **IDEMIA** (formerly **Morpho**) is a multinational company specializing in security and identity solutions and an IPP partner of Bosch BT

– **MorphoManager** is a biometric access control application from IDEMIA.

– **BioBridge** is the interface software connecting **MorphoManager** with Bosch access control system.

Consult the White Paper for instructions on configuration

Limitations:

- **IDEMIA software supports up to 100.000 cards only**
- **IDEMIA software does not support divisions**
- **Use IDEMIA software on Windows 10 only, because older operating systems are not supported by BIS ACE.**
- **Duress finger functionality is currently not supported with IDEMIA devices.**
- **Only one IDEMIA system per BIS ACE is supported.**

Notice:

The deletion of biometry data must be configured on the IDEMIA side. Use IDEMIA readers only in accordance with the data-protection laws of your country. We recommend that you set a deletion cycle of 2 days.

If multiple cards are assigned to one cardholder in the access system, only the oldest of the valid access cards of a cardholder is synchronized with the IDEMIA system. This is because the IDEMIA system is restricted to one card per cardholder,

If you restore in BIS a backup of a system where IDEMIA was used, go to BIS Config browser > **Tools** > **ACE IDEMIA database configuration**; there delete and recreate the IDEMIA database.

Since BIS 4.9 the cardholder ID photos can be transferred for enrollment to the IDEMIA system. The quality of the cardholder pictures in the ACE may be insufficient for accurate face recognition by IDEMIA. The more secure variant is to enroll picture templates on the IDEMIA devices themselves. But if no high security face-recognition is needed, the transfer of ACE photos can be activated in the tool **ACE IDEMIA database configuration**.

2.2.4 Mode override

New reader\door command "Restore configuration" is provided. The BIS alarm operators can use the new command if they have the necessary permission in BIS.
The ACE Device Editor shows on the reader or door page if a configuration override is in progress. The “Restore configuration” command restores the reader or door configuration to the last saved settings done in the configuration browser.

ACE API
The “RestoreConfiguration” command is available in the ACE API, and behaves in the same way as in the user interface.
The new ACE API is backwards compatible with older BIS versions according to the feature sets of those versions.

2.2.5 Extended filters

The ACE dialogs “Group of persons” and “Group authorizations” have been enhanced. They now contain a maximum of 5 selectable additional fields for filtering and finding persons by custom fields.

2.2.6 PegaSys and LEGIC advant cards

In PegaSys systems where LEGIC advant cards are used, the Dialog Manager can now create missing LEGIC segments, provided that the IAM cards are available and your enrollment reader supports the writing of segments.

2.2.7 Temporary cards for intrusion systems

Temporary cards are now supported for intrusion panels.
If a card was assigned to intrusion system and afterwards replaced by a temporary card the temporary card is send to the intrusion system. If the original card is reinstated, then the temporary card will be removed from the panel, and replaced by the original card.
Prerequisite: The temporary card must have the same encoding as the original card.

2.2.8 New report layout

The reports dialog **Personal cards** contains an additional layout where cardholders are grouped by companies.

2.2.9 Key Management Tool for LECTUS select and MIFARE DESFire

This tool allows to customize the following access parameters of MIFARE DESFire credentials:

- The application ID
- The DESFire file number
- The file read key.

Since these parameters contain security relevant information, they are stored in a password-secured, encrypted file. This file, called the parameter file, can be then imported into the access control system through the Device Editor, and used to configure readers.

2.2.10 AMC Bootloader

With BIS 4.9 the bootloader has been updated to version 00.61 v01.47.00 LCM
AMCs will be updated automatically by BIS 4.9
If you wish to update AMCs manually using the Bosch.AMCIPConfig-Tool:
If the AMC has Bootloader V00.49 and later, you can update directly to V00.61v01.47.00
For all older bootloaders, first update to V00.49

2.2.11 IP Configuration Tool

With BIS 4.9 the IP Configuration Tool has been split:

- To configure AMCs use `BOSCH.AMCIPConfig.exe`
- To configure BioEntry W2 finger print readers use `BioConfig.exe`

2.3 Video Engine

No updates in *BIS 4.9* compared to *BIS 4.8*

Notice!
The *Video Engine* will still run under HTTP mode, and no special configuration is required. However, for security reasons we recommend that you configure all cameras with HTTPS, not HTTP.

3 Resolved issues in BIS version 4.9

21 30

3.1 Platform

The following list of issues has been fixed for BIS 4.9

#251619: BWC Client now correctly shows the description of a detector, not the line state

#320455: With OPC UA it is now possible to configure after renaming the OPC server machine.

#322699: THEN control does not work when copied from address trigger to timer trigger using Ctrl+C / Ctrl+V. This is now fixed.

#317284: Changes to ACE ID photos are now promptly reflected in BIS action plans.

#332417: Password policy now accepts ascending and descending sequences of 3 characters, but not more than 3 characters.

#321529: The Configuration Collector can now handle ZIP files of 15GB and above. Additionally it collects data from only the last 14 days by default (adjustable).

#313664: The Configuration Collector now collects log files from the Importer-Exporter tool.

#241358: BisClientSDK: Sample application has been enhanced. It now shows BIS addresses belonging to alarm messages.

3.2 Access Engine (ACE)

#281023: API SDK 4.9 is compatible with BIS 4.7 and 4.8, and can now save ID photos larger than 8kB.

#313596 BIS 4.8 – ACE services cannot connect to database
In rare cases after an upgrade or a fresh installation, BIS-ACE video verification or intrusion services would fail to work, due to an internal authentication error. This issue is now corrected.

#224650: Parallel working in the device configuration and the BIS client is now possible, thanks to the mode override feature.

#335631: In the Device Editor it is no longer possible to change a reader type to a type that is incompatible with the firmware of its AMC.

#277453: Using a camera under Windows 2019 server
Microsoft no longer supports web cams on server operating systems.

#246461: All Card types are now correctly activated after updating the BIS ACE version.

#334507: If a card is replaced by "Replace card" button, and its predecessor was registered with the intrusion system, then the new card still needs to be registered with the intrusion system.
It is no longer necessary to register the new card on the **Intrusion** dialog tab.

4 Known limitations in BIS version 4.9

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`*

#340945
If version higher than "Microsoft .NET 5.0.5" is already installed, then the BIS installation will fail.
Workaround: Check for and manually uninstall all versions of "Microsoft .NET" higher than 5.0.5. Then continue with the BIS installation, which will install the required version of Microsoft .NET 5.0.5 Windows Server Hosting and Runtime.

Report print
If you have not updated from SQL server 2016, 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

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

#178991:
No warning is displayed during setup if there is insufficient space for the 4GB audit trail database.
Workaround: Please refer to installation manual for prerequisite free disk space.

#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.

#248766:
BIS + remote SQL Server Reporting Services (SSRS) issue

Local user account “Mgts-SSRS-Viewer” is needed for the Reporting Services, this must be a local service account. It is not possible to use the domain account for viewing the report from BIS.
Workaround: See remedy and limitation in section 2.1.7 Access Reporting service using Domain Account Support

#**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.

#**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**.

#**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.

#340702:
After new installations where the Reporting Services is installed on BIS server with its own DB and there is a remote SQL Server (i.e. Topology 2 in the installation manual) the ChangePassword tool sometimes fails to change the password for internal SQL server users **logbuch_query** and **logbuch_w**.

Workaround: Change the registry value of
`[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Security`

Systems\Platform\ReportingServicesDatabaseServerName] to <yourBISserverName>\BISReports

#340754: The Configuration Browser sometimes crashes when configuring OPC UA with certificate authentication.
Workaround: A patch is available from tech support.

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

BISACE 4.9 is the last version to support the RS-485 MAC to AMC host interface. This serial interface is deprecated because it is not secure.

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

#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.

#336792: Cipher Suite

The Access System supports only the RSA-based cipher suite TLS_RSA_WITH_AES_256_CBC_SHA256
If this suite has been disabled by group policies or registry settings, please re-enable them. Otherwise ACE will not function.

#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.

#328222: Synchronization fails between DMS and MAC

If you try to swap two AMC names or IP addresses the MAC will not accept the change, because they are already used.
Workaround:

1. Change one of the names or IP addresses to a third and unique name or address.
2. Wait until the MAC accepts the first change, before completing the swap.

#281079: Remote MAC setup fails if the MAC process control is running

Workaround: Stop the service **Access Engine (MAC)** before using the setup.

#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 Sync 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 are continuously online.

#313246: Door Model 05 (Parking lot)

BIS-ACE 4.8 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.

#338501: Configuring the Intrusion RPS endpoint

The Configuration dialog for the (Intrusion) RPS-API cannot be opened in Dialog Manager on client workstations.
Workaround: Configure the RPS endpoint on the server.

#339314: Spurious messages in the error log

You can safely ignore messages of type

```
ACE|AE event with an empty source received
```

in the BIS error log:

#339728: Editing resistor values

In the Configuration Browser on the AMC tab "**Inputs**" the event check boxes "**Open, Close**" and "**line cut, short circuit**" are not selected by default. Therefore the resistor values are not editable.
Workaround: Enable the check boxes in order to set resistor values.
Note that if you clear the check boxes, the resistor parameters are immediately reset to their default values.

After updating a BIS 4.6.2 or earlier system, select the event check boxes.

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.

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.
If you require FQDNs, contact Technical Support for a workaround.

Multiple sequential logins to Importer-Exporter

If you log in to the Importer-Exporter Web Application (IMPEX) more times than you have client licenses, further client logins at the BIS Manager may be blocked for up to 35 minutes or until BIS system is restarted.
If all operator client licenses are already in use, then the internal IMPEX service may be prevented from authenticating itself at the BIS server, thus preventing the import or export of data.
Moreover no further logins will be possible at the following applications:

- BIS classic client
- BIS web client
- BIS smart client
- Visitor Management
- Occupancy Monitor
- Any third-party applications that use the ACE API or BIS API to log in.

Workarounds

- Avoid logging into web interface of the Importer-Exporter application multiple times sequentially.
- If the BIS Manager is running, close it to free an additional login.
- Restart service "`A1_BisClientproxyWcfServer`" in `services.msc` will clean up all login processes except those of the BIS Classic Client and the BIS Manager.

If these measures are not practicable in your case, contact technical support for specialized assistance.

#340427 The OPC messages **Disk nearly full** and **Disk full** are not being sent to BIS
These two OPC messages are not mapped correctly to the ACE DMS detector type in the default configuration, therefore they not being sent to BIS.

Workaround: Add the mappings manually as follows:

1. In the BIS Configuration Browser navigate to **Infrastructure** > **Detector types**
2. In the **Detector types** pane select **Access Engine** > **DMS**
3. On the **State mappings** tab, select **The reported states are mapped**.
4. Click **+** to add a mapping.
   The **Changes of the mapping of states** popup window appears.
5. In the popup window, select **Single value** and type (case sensitive) `7f000067` in its text box
6. In the **State** list, select `4301 Disk Full`
7. In the popup window, click **OK**
8. Click **+** to add another mapping.

9. In the popup window, select **Single value** and type (case sensitive) `7f000066` in its text box
10. In the **State** list, select `4301 Disk Nearly Full`
11. In the popup window, click **OK**

Optional The mapping for `4302 Disk Normal` is not an alarm, but can be added analogously, if desired:

- **Single value** (case sensitive) `7f000044`
- **State** `4302 Disk Normal`

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.

#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.

#340743: OTIS Compass integration
In this version BIS 4.9 access authorizations cannot be assigned to OTIS elevators. If you are using OTIS Compass integration please refrain from upgrading to BIS 4.9. An update of the OTIS Compass interface will be provided with the next BIS version.

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.

AMC with serial connection to the host system
Connecting AMCs to the host system via RS485 is approaching end-of-life. BIS 4.9 is the last release which will support the serial connection to AMCs. If you intend to update your system, and you are using serial AMC connection, then please contact support to get detailed information regarding updates and restrictions.