Building Integration System (BIS) version 4.8 Release notes

2020-11

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

Document history.

Version	Description
1	2020-10-16 initial version
2	2020-10-23 releasable
3	2020-11-05 miscellaneous additions; releasable.

Table of contents

1 Installation Notes

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

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 8.1 (64 bit) Professional or Enterprise	No	No	Yes	Yes
Windows 10 (64 bit, Enterprise LTSB - 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 [2]	Yes	Yes	Yes	No
Windows Server 2019 (64bit) Standard or Datacenter [2]	Yes	Yes	Yes	No

[1] Latest supported Windows version

[2] Not as domain controller

Notice

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 will be the last version to support Windows 8.1 on clients

1.2 Server

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

Supporting Software on Windows and Windows Server Operating Systems	• IIS 10 for Windows 10 and Windows 2016/2019 Server.
	• SQL Server 2012 SP2, SQL Server 2014 SP1, SQL Server 2016 SP2 and SQL Server 2017.
	
	Notice!
	• IIS is not necessary on *BIS* connection servers.
	• SQL server 2012 SP2 is not supported on Windows Server 2019.
	• Internet Explorer 9, 10 or 11 in compatibility mode *
	• .NET for various operating systems:
	  ○ On Windows 10: .NET (3.5 SP1, 4.0, 4.6.2 and 4.8), .NET Core 3.1
	  ○ On Windows Server 2016/2019: .NET (3.5 SP1, 4.0, 4.6.2 and 4.8), .NET Core 3.1
	
	Notice!
	• Latest drivers and OS updates are highly recommended.
	• If HTML5 is enabled in IE 11, then Video will not be displayed.

Minimum hardware requirements	Intel i5 processor with at least 6th Generation and a minimum of 4 physical cores
	• 8 GB RAM (32 GB recommended)
	• 200 GB of free hard disk space (SSD recommended)
	• Graphics adapter with
	  ○ 256 MB RAM,
	  ○ a resolution of 1280x1024
	  ○ at least 32 k colors
	  ○ OpenGL® 2.1 and DirectX® 11
	• 1 Gbit/s Ethernet card
	• A free USB port or network share for installation files

1.3 Client

These are the hardware and software requirements for a *BIS* client:

Supporting Software	• ASP.NET
	• Internet Explorer 9, 10 or 11 in compatibility mode *
	(**Notice!** The SEE client requires IE 9.0)
	• .NET for various operating systems:
	  ○ On Windows 10: .NET (3.5 SP1, 4.0, 4.6.2 and 4.8)
	  ○ On Windows Server 2016/2019: .NET (3.5 SP1, 4.0, 4.6.2 and 4.8)

Minimum hardware requirements	• Intel i5 processor with at least 6th Generation & min 4 physical cores • 8GB RAM • 20GB free hard disk space • Graphics adapter with 1280 x1024 resolution, 32k colors, 256MB dedicated memory with OpenGL 1.2 or later • 1 Gbit/s Ethernet card
Additional minimum requirements for VIE (Video Engine) clients	• No Windows Server operating systems • 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 4.8: EN, DE, RU, ES, ZH-CN, ZH-TW, PL, TR, AR, HU, NL, FR

1.4 Updating BIS to version 4.8

Notice!

1. Ensure that the BIS version from which you are upgrading is running properly. The upgrade procedure cannot repair defective installations.
2. 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**.
3. If you are about to update from BIS 4.6 with HTTPS enabled, make sure HTTPS is properly enabled by running the batch file from the installation media:
   <Installation Medium>\Tools\HttpsForBIS\DisplayCurrentHttpsStatus.bat
   If the status is disabled, then run the batch file:
   \Tools\HttpsForBIS\EnableHttps.bat to enable HTTPS before starting the BIS 4.8 installation.
4. If the previous version of *BISProxyOPCDA* is already installed, unregister the previous version of *BISProxyOPCDA*, replace it manually with the version delivered with BIS 4.8, 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**

5. If the Reporting service is installed on the remote SQL server machine, then it has to be properly configured with HTTPS, if not then the BIS upgrade will fail. See installation guide for instructions on setting up the database servers with their respective certificates.
6. During the BIS 4.8 upgrade, 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.

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 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. Before upgrading the *BIS* version, make sure you install SQL server 2012 R2 or another supported version.
- The *Mandatory post installation* BIS document is delivered in PDF format from *BIS 4.6.2* onwards. Install the PDF viewer to view the *BIS* related documents.
- Windows updates must be turned off during *BIS* installation, because they can interfere with it. Generally, it is recommended to install all Windows updates before the installation.
- The BIS 4.8 installation media contain a new version of PRAESIDEO OPC server. We recommend that you use this version.
- If you have modified the file `<BIS installation drive>:\MgtS\ConfigurationBrowser\BoschST.BIS.ConfigurationBrowser.exe.config` since the last installation, then the upgrade installation will not overwrite it to work with OPC UA.
  In this case, perform the following changes h manually:

  Add the two elements below after the `<Configuration>` tag in the `.config` file:

```
<configSections>
  <section name="Bis.Opc.Ua.Client" type=
"Softing.Opc.Ua.Sdk.ApplicationConfigurationSection,Softing.Opc.Ua.Sdk.Co
re"/>
</configSections>

<Bis.Opc.Ua.Client>
  <ConfigurationLocation
xmlns="http://opcfoundation.org/UA/SDK/Configuration.xsd">
    <FilePath>BisOpcUaClient.Config.xml</FilePath>
  </ConfigurationLocation>
</Bis.Opc.Ua.Client>
```

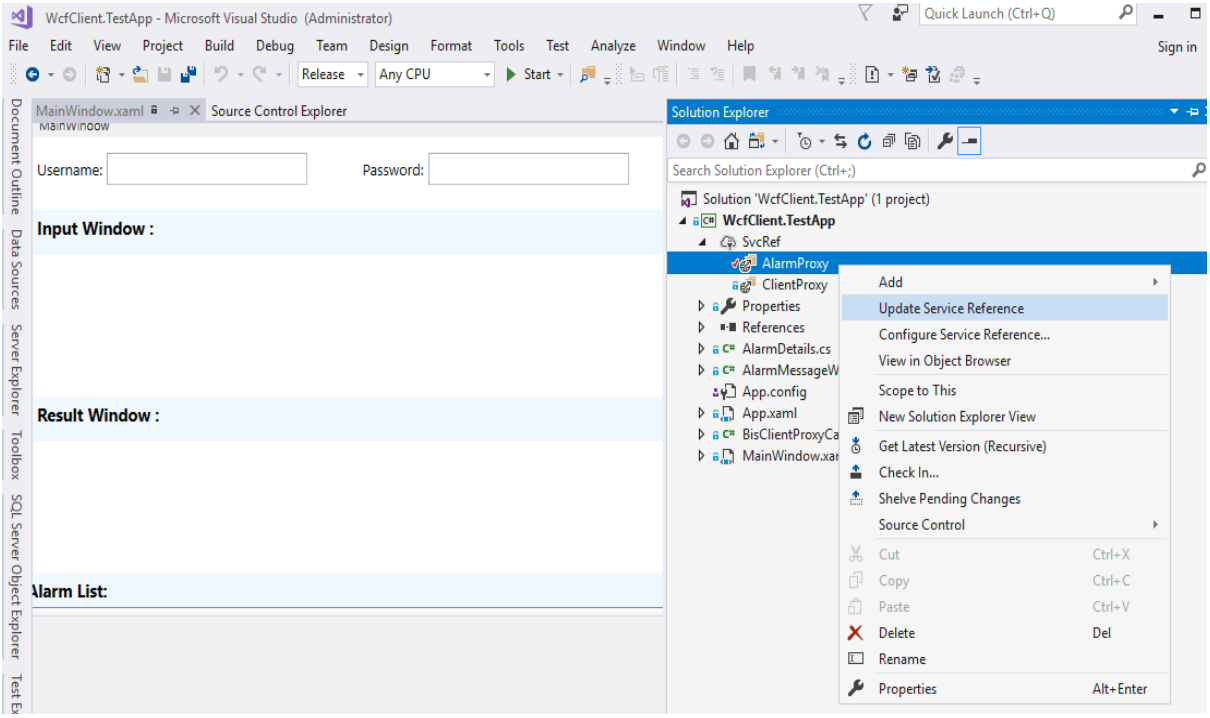
1.5 Updating Service References in WCF applications

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

Remedy: After upgrading to BIS 4.8, 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.

1.6 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.

1.7 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.

2 New features in version 4.8

Notice!
The limitations cited in this document are the maximum values that have been tested by the time of publication of BIS 4.8. They do not necessarily reflect the absolute maxima for the system.

The authentication of Active Directory users is performed by the configured Active Directory server. Operators now omit the domain name when logging on, and use the format `\username`. Anything written before the backslash is ignored. Internal usernames are now displayed in this format also.

2.1 Platform

2.1.1 Windows Server 2019 support

2.1.1.1 Operational information

- BIS 4.8 able to install and run on Windows server 2019

2.1.1.2 Limitations

- The Admin Center, which offered as part of the Windows Server installation, is not compatible with BIS, because it blocks the IIS service and the HTTPS port. **Do not** install the Admin Center option when installing Windows Server. The HTTPS port 443 is also not released by the Admin Center uninstall process, so you must reinstall Windows Server completely if you accidentally install Admin Center.

2.1.2 SQL Server 2017 support

2.1.2.1 Operational information

- For new installations of BIS 4.8 SQL server 2017 express edition will be installed, if you are not using your own purchased version.

2.1.2.2 Limitations

- If the Reporting service and the BIS database SQL server are not to run on the same machine, then Reporting Service and the BIS database server require purchased, licensed versions of the respective products.

2.1.3 Security Improvement

2.1.3.1 Password handling for MgtS-SSRS-Viewer account

- BIS 4.8 installation no longer uses hard-coded passwords. For the Mgts-SSRS-Viewer account 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 for connecting the Reporting service.

Notice!

- It is recommended that you configure the Windows password policy not to conflict with the policy above.
- When upgrading from version BIS 4.6 or older, it will not create new random password, instead it uses the existing password. Hence it is recommended that you change the Mgts-SSRS-Viewer password after upgrading to BIS 4.8, using the ChangePassword-Tool located in the installation folder `MgtS\Tools\ChangePassword\`
- If the Reporting service is installed on the remote database server, then after BIS installation the MgtS-SSRS-Viewer, change the Mgts-SSRS-Viewer password after insatallation of BIS 4.8, using the ChangePassword-Tool located in the installation folder `MgtS\Tools\ChangePassword\`
  If not changed then Audit trail report and Event log report will not work. See the BIS installation manual for details.

2.1.3.2 Password Protection of BIS ConfigCollector.zip

- A password is now mandatory for the configuration collector
- Minimum length of password is 3 characters.
- With the provided password, the configuration collector generated zip files will be protected.
- Please supply this password to technical support if and when you submit a configuration collection to them. Use a separate, secure communications channel for this.

2.1.3.3 Improved User Account Management

- Upon login from BIS client, if the password is same as the username, then you will be forced to change the password.
- The new password must conform to the password strength policy decribed in the installation documentation.

Notice!

- The password policy is predefined and cannot be modified
- BIS client and BIS manager have the same users and passwords.
- The Configuration Browser has different users and passwords that are not affected by this password policy.

2.1.3.4 Secured retrieval of photos used by Action plan and Message details

- Message details and Action plan HTML pages now use a secure way of fetching the photos using the ACE API
- The following code snippet is used in Message details and Action plans to fetch the photo.
  GET call using API
  `https://<BISloginservername>:62904/api/CredentialHolders/<persson_id>/photo`
  With the request header below:
  `"Content-Type", "application/x-www-form-urlencoded"`
  `"Authorization", "Bearer "<accessToken>`
- Photo will be return in JSON format

- For details, compare the default example file in the installation folder:`\MgtS\default_configurations\common\documents\MessageDetails\MessageDetails.HTM`
  See the function: `fetchPhotoJSONFile`

Notice!

- In Upgrade installations, existing Message details pages and Action plans will not be migrated. Migrate these manually. If not, then photos will no longer be displayed.

2.1.3.5 Encrypted communication between BIS server and SQL server

- For new installations and upgrades, the “Force Encryption” option in SQL server will be set automatically. This encrypts the communication between the BIS login server and the SQL server service.
- For remote SQL server computers, follow the instructions in the BIS installation manual.

Notice!

- SQL server, by default, uses the Microsoft-generated certificate. For more secure communication it is recommended that you use a CA-signed certificate, please refer to the link below:
  https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-ver15

2.2 Access Engine (ACE)

2.2.1 Intrusion panel Integration

Cardholder synchronization with B/G panels

BIS 4.8 supports the synchronization of cardholder data between Access System and B/G panels via the RPS (Remote Programming Software) tool. The supported version for BIS/ACE 4.8 is RPS-API v2.1.25920. The contact for requesting the RPS-API tool is: `Integrated.Solutions@us.bosch.com`.

The items synchronized are:

- name
- user group
- passcode
- access card
- key fob
- remote access authorization
- language
- authorization profile
- authorization level
- reports

Limitations:

- Multiple intrusion panels can belong to one Access Intrusion authorization profile.
- Only one Access Intrusion authorization profile can be assigned per card (person).
- If 37-bit cards, e.g iClass HID 37 bit cards are used both for arming intrusion panels and for access control in Access system, then the facility code must not be larger than 32767. If these cards are used only for access control only, then the limitation does not apply.
- Temporary cards cannot be used for intrusion panels.

2.2.2 "IDEMIA Universal BioBridge" Integration

Introduction

– **IDEMIA** (formerly **Morpho**) is a multinational company specializing in security and identity solutions.
– **MorphoManager** is a biometric access control application from the IDEMIA Company. The application works with biometric devices to capture fingerprints and other biometric data. The biometric information is associated with cardholder data in a database. When cardholders present themselves at an IDEMIA biometric access reader, and their biometric data matches a card number in the database, the reader sends the associated card data to the local access controller, such as an AMC2 device, which then makes the decision to grant or deny access.
– **BioBridge** is the interface software connecting **MorphoManager** with other access control systems.

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.
- IDEMIA duress finger functionality is currently not supported.
- 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:
Because the IDEMIA system is restricted to one card per cardholder, only the oldest of the valid access cards of a cardholder is synchronized with the IDEMIA system.

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.

2.2.3 Validation for 3rd party reader like face stations and number plate recognition

The API-SDK and the AMC are enhanced to support access validation requests from 3rd party systems.
See the Access Engine configuration help for details.

Notice
The precompiled sample application provided in the API-SDK directory can be used to try out the new 3rdParty validation request: `\AddOns\ACE\API\C++API\bin\ClientACEInterfaceCS.exe`

2.2.5 AMC / MAC mass configuration

All AMC's of an MAC can be activated\deactivate with one configuration command in the device editor of the access system.

It is now possible to copy an AMC configuration with all sub devices, like readers, to another MAC or the same MAC. The complete device configuration is copied except for parameters like names and IP-addresses, which must be adjusted afterwards.

Notice
Be aware that the copy function of an AMC does not copy any dependent authorization definitions.

2.2.6 AMC broadcasts its presence on networks

In order to be monitored within a network infrastructure, the AMC broadcasts gratuitous ARP packets.
This protocol informs the network switch of the MAC address of the AMC at a connected switch port, so that the switch knows that it should transmit packets sent to that MAC address on that specific switch port.

The AMC will broadcast its presence on the network under the following conditions:

- The AMC is connected to a switch.
- The AMC is powered up.
- The AMC detects a new network link (e.g. because the switch rebooted or the cable was replaced).
- When no data has been exchanged over the network link for more than 30 seconds.

2.2.7 Alarm message support for OSDP reader manipulation

Security enhancement on ACE in cases where an OSDP reader using the V2 secure protocol is physically replaced.
The operator receives an alarm message (if so configured), and must confirm it to accept communication with the new reader.

Notice: Some readers, e.g. LECTUS Secure SE, store the security key internally. These readers require a factory reset in order to accept a new security key.

2.2.8 PegaSys systems

Different card sectors

MIFARE Desfire cards with different PegaSys AIDs and customer keys are supported. The PegaSys facility card V7 is required and Normbau firmware versions greater than V4.4.10.

In addition, further license SAM (Secure Access Modules) cards are needed to create PegaSys AIDs (application identifiers) and files.

Interflex

For the Interflex dialog readers a customer key can be defined to read the Bosch access card. The AID cannot be changed for the Bosch card number. To change that Bosch read key, the firmware of all access readers must be changed manually too. This firmware is not part of the access software described here.

ODBC drivers

To use the PegaSys configuration tool on workstations:

- Install SQL Server 2017 ODBC drivers (32 and 64 bit)
  `\3rd_Party\ODBCDriver17SQLServer`
- Copy the registry entry
  `\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Micos\SPS\DEFAULT\Global\DB_CONNECTION`
  from the BIS login server to the ACE client workstation.
  Repeat this step whenever someone changes the BSUSER password in the ACE ChangePassword tool.

2.2.9 Enhancements on filtering of reports: Multiselect of entrances

In the report “Authorizations per entrance” it is now possible to select up to 20 individual entrances.

2.2.10 Improved workflow management: "Activate Pegasys-Cards via ACE-API-SDK

The API-SDK was improved so

- Access cards can be defined as PegaSys compatible
- the PegaSys permissions can be assigned and removed

See ACE API documentation for details.

2.2.11 Updated version of Import-Export tool

The new Import-Export tool including documentation is available in the `\AddOns\ACE\ImportExport` directory. Person data can be imported and exported. The old Import-Export tool in the BIS ACE is deprecated, and may be removed in future BIS ACE versions.

Notice:

- No API-SDK license is needed any longer to use the new Importer-Exporter tool.

2.2.12 AECT tool introduced for BIS-ACE

New configuration files have been added for BIS and ACE environment checking.
Notice: When selecting the XML file, the error message "wrong XML format" can mean that the AECT tool is being executed from a non-writable medium. Make sure that you run the AECT tool only from a writable medium.

2.2.13 Windows Server 2019 (Removed Server 2012)

Windows Server 2019 is supported as server operating system. The older windows server 2012 is no longer supported anymore.

2.2.14 SQL Server 2017

The new SQL Server 2017 is used as default on installation. But the ODBC driver from SQL Server 2017 is installed on the server and used always independently of the actual SQL Server version.
The SQL Server 2017 encryption uses the highest TLS mode 1.2 provided by Microsoft.

2.2.15 Door model 14 enhancement

The door model 14 has been improved. Now the behavior can be configured to grant access and disarm the alarm system in one step. The possible device configurations are described in detail in the manual.

2.2.16 Timeout for automatic transfer to “Outside” area

For each MAC in the Device Editor, tab **Global access settings**, you can configure the timeout for setting the location of a cardholder to Outside. The control is called

Area dwell time of person expires after:
The default value is 24 (hours). A setting of 0 deactivates the timeout.

2.2.17 Performance improvements

Improved the communication speed from DMS to MAC to AMC.
Cold/Warm-starts are much faster than before. This becomes noticeable with large numbers of cardholders, provided your computer has resources available.
Best performance is possible with AMCs with 2GB CF cards.

Improved the communication speed from MAC to DMS. Multiple events are packed into one message, so server hardware with more CPU cores is now faster.

AMC finds cards faster on CF card and can decide faster. This becomes noticeable with large numbers of cardholders, for example at main entrances.

2.2.18 API-SDK enhancements

The provided API-SDK is compatible to AMS V3.0, BIS V4.7 and V4.8 and future BIS versions, given current functionality. Non-existent functions of older systems remain of course non-existent. For more details see “ACE API.pdf” documentation provided in `AddOns\ACE\API\help\` directory.
All commands to subsystems, such as MACs and AMCs, are executed faster, even for large imports of cardholders.

2.2.19 Performance of fingerprint verification

For every MAC a dedicated interface process is started for biometric verification requests. For bigger systems we therefore recommend using multiple MACs and distributing the fingerprint readers over the MACs.
Recommended: Max. 100 readers per MAC, if fingerprints are rarely used. If frequently used, 50 per MAC.

2.2.20 New monitoring tools for MAC and ACE

After installation there are 2 new applications available on the desktop: **MAC Control Console** (MAC) and **ACE Process Control** (DMS). Administrators can use these to verify the state of the internal processes.

Limitations:
The debug trace level of the new ‘netcore’ services found in ACE process control cannot be changed at runtime. Workaround: First change of the trace level in the Configuration Browser and then restart the processes in the **ACE process control** (DMS) application.

2.2.21 Using Certificates

Use the `\MgtSCertificate\AccessCertificateTool.exe` to generate certificates from your own root certificate, or to generate new certificates for RabittMQ,

Bosch.IntrusionAPI, Bosch.DialogManagerApi and Bosch.AMSApi. These certificates are used for example, for video verification and intrusion configuration.

2.3 Video Engine

No updates in *BIS 4.8* compared to *BIS 4.7*

Notice!
The *Video Engine* will still run under HTTP mode, and no special configuration is required. However, for security reasons we recommend configuring cameras with HTTPS instead of HTTP.

3 Resolved issues in BIS version 4.8

3.1 Platform

#249692 BIS EventLog database in BIS 4.x to 4.7 contains duplicate attribute entries.
This issue has now been fixed.

#251619 BWC Client does not show the description of a detector, in description field the line state is shown
This issue has now been fixed.

#257668 after enabling TLS 1.2 (Disable TLS 1.0 and 1.1) some BIS functions fail
.Net 4.0 does not use TLS 1.2 by default, it is expecting the registry setting to enable the TLS 1.2, thus causes the BIS function to fail. The code has been modified to enable the registry settings to allow TLS 1.2 by default.
Security advice: SSL 3.0, TLS 1.0 and TLS 1.1 are not disabled by default. If they are not required by other applications disable them.

#260008 BIS mobile client date/time format not configurable
The time and date formats for the mobile client's alarm list and alarm details are configurable in a separate configuration file. Time format could be set to either 12 or 24 hours and Date format could be set to either “dd/mm/yy” or “mm/dd/yy”. If invalid format or format itself not provided then 24 hours with “dd/mm/yy” format will be taken as default value.
The configuration below is now possible in the BWC configuration file:
`\MgtS\SmartClient\BWC\config.json`
"timeFormat_24hrs": true, => Valid values are `true` or `false`
"dateFormat": "dd/mm/yy" => Valid values are "`dd/mm/yy`" or "`mm/dd/yy`"

#263460: Action Plan does not show user image
This issue is solved in BIS 4.8 by using secure API call. See 2.1.3.4 Secured retrieval of photos used by Action plan and Message details

#217043: BIS 4.x backup error
Improved the event log database backup/delete record handling. It is now possible to support databases of up to 10GB.

#255196: BWCConfigTool improvements
The BWCConfigTool must now be run as Administrator.

#260665: BIS 4.7 Video Engine returns Access Denied error.
Enabling “Display mixed content” in the Internet Explorer settings is now done automatically by the `IE_InternetSettings_Zone2_TrustedSites_BIS.reg` file. See installation manual for BIS client installation.

#262238 – Certificates not updated by the BWC Config tool
This issue has now been fixed.

#265014: sometimes watermark shown inside Live video
The Video Engine license is written into a temporary file, which is not locked properly hence causes the watermark to display due to failure in reading license file. The issue is fixed. The file is now locked before writing and reading.

#188581: The *A1_BISAuditTrailWatcher* service blocks the update of BIS-ACE
If the A1_BISAuditTrailWatcher service is not started properly then this issue will occur. To avoid this, the service has to be properly configured to run in HTTPS mode.
The remedy is documented in
`\AddOns\Platform\NetworkSecurity\BIS_Data_Security.pdf`

#199188: If HTTPS is enabled for audit trail and an upgrade (modify/repair) is done, the service does not start after the upgrade
If HTTPS is properly configured for Audit trail, then this issue is not seen, refer the procedure in #188581 to enable the HTTPS for Audit trail.

Bug# 282385 Control panel silent uninstallation
There are two ways to uninstall BIS from the Windows Control Panel:
Windows Control Panel> All Control Panel Items >Programs and Features

- If you click **Modify** > **Remove,** then, upon completion, the process will display a list of the SW products that need to be uninstalled manually, because they may be required by other programs.

- If you select **Uninstall** directly, then a "silent" uninstall will be performed, and so the list will not appear. The list nevertheless exists, and consists of the following items.
    - Microsoft SQL Server <version> Express Edition
    - Microsoft .NET Framework
    - Lead tools

3.2 Access Engine (ACE)

#278128: ACSP Process does not reconnect to logifier on very rare occasions
This issue has been fixed.

#276162 and #276065: PXP Task AddFields with additional fields
This issue has been fixed. The PXP process now parses the `persid` field correctly.

#276070: - additional field, check unique data
This issue has been fixed. If a data field is changed, uniqueness is now checked

273336: Wrong Result is displayed in report Persons PegaSys
This issue has been fixed. The report now returns the correct result, even if sorting the list of doors/doorgroups.

266505: Parking Area max. counter problem with subarea count "0"
This issue has been fixed. If the counter of a parking area is changed and one of the subareas is set to "null" (unlimited), then the total for the whole area is now also set to "null".

265833: Importer/Exporter: Custom fields support improved
Improved usage of custom fields by Importer/Exporter

255193: Unexpected 'Door opened unauthorized' with Door model 03 a
This issue has been fixed.

255169: Generating Threat Level Management report on Client
This issue has been fixed. The TLM Report is now available on the remote client PC.

255008: Improved MAC log
This issue has been fixed. The ID of the blacklist now shows the correct values.

252441: Reader parameters fixed in Russian language
Reader parameter setting is now fixed in the Russian language.

250624: BIS ACE ActionPlans and Misc Documents do no more work with Https
This issue has been fixed. See 2.1.3.4 Secured retrieval of photos used by Action plan and Message details

250004: Card Print dialog shows obsolete path
This issue has been fixed.

#218694: Visitors.IDTYPE property can be changed by API but is not shown in the visitor dialogs
This issue has been fixed. See ACE API documentation for details.

4 Known limitations in BIS version 4.8

4.1 Platform

Report print does not work if you use SQL server 2016.
Workaround: A 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 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, which might need to be repeated again after having the full profile.
Workaround: Do not install or configure *BIS* if running with a temporary profile. Windows notifies of this at logon.

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

#248766: BIS + Remote SQL Server Issue
Local user account “Mgts-SSRS-Viewer” is needed for the Reporting service, this must be a local service account. It is not possible to use the domain account for viewing the report from BIS.

#268122: Audit trail report failed to export to WORD – (only in 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: Threat Level Management commands not visible in BIS Client
In BIS client, when right clicking a MAC, the commands for Threat Level Management activation and deactivation are missing.
Workaround: Re-synchronize the Access Engine in the BIS Configuration Browser > **Connections** > **Connection servers**, right-click **Access Engine** and select **Synchronize**.

4.2 Access Engine (ACE)

#281023: API SDK 4.8 is compatible to BIS 4.7 except saving pictures bigger than 8kB.
Workaround: See 2.2.18 API-SDK enhancements

#246461: Cardtypes are not correctly activated after update and in dialog
Sporadic: card type definitions not active after upgrading BIS.
Workaround: Remove the card types from the configuration and save the changes. Re-define the card-types that you require and save the changes.

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

#277453: Using a camera under Windows 2019 server
Microsoft no longer supports web cams on server operating systems.
Workaround: If the DirectShow driver on Windows Server machine is installed, you need to install the Desktop Experience server feature on your server to obtain the components needed for the DirectShow decoding.

#199503: Instability of BIS Client when trying to enroll a fingerprint after a reader lost its network connection
Workaround: During fingerprint enrolment, do not disconnect the reader from the network.

#216031: BIS states "Random screening" or "Palm vein verification" do not reflect settings made in the Configuration Browser
The enable\disable state for *Random screening* or *Palm vein verification* in the Configuration Browser is not reflected in the *BIS* Client.
Workaround: Send 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.

#224650: Parallel working in device configuration and command operator
Changing the configuration with a command (e.g. **Open door unlimited**) from *BIS,* and parallel working in the device editor, can lead to error messages. Since the configuration has been changed, the device editor cannot be updated.
Workaround: If changes are being made in the Configuration Browser, all operators should log out.

#280246 When an AMC is going offline, it takes at least 12 seconds before it can activate or deactivate a Threat Level by pushbutton.
Workaround: If there is no immediate response from system, keep trying for at least 12 seconds.

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

Workaround: Run
<installation drive>:\MgtS\AccessEngine\AC\Bin\ChangePasswordTool.exe
to generate a new password. Then restart the system.

#313246 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.

BioEntry W2 Fingerprint Readers

#243864: Fingerprint reader BioEntry W2: Templates on device card mode:" do not work with unknown cards
Workaround: Do not enroll to unknown card types

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 fingerprint W2 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.
  Performance for templates on server has been improved. See 2.2.17 Performance improvements

General recommendations:
If possible, 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.

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.