Building Integration System (BIS) version 4.7 Release notes

Document history.

Version	Description
1	2019-11-29 initial version
2	2019-12-02 Modified note on AccessIPConfig and fingerprint readers

Table of contents

1 Installation Notes

1.1 Supported operating systems

The *BIS* system runs on these operating systems:

	BIS Login Server	**BIS Connection Servers**	**BIS Client**	**BIS VIE Client**
Windows 8.1 (32 bit) Professional or Enterprise	No	No	Yes [1]	Not recommended
Windows 8.1 (64 bit) Professional or Enterprise	Yes [1]	Yes [1]	Yes	Yes
Windows 10 (64 bit, Enterprise LTSB - Version 1607)	Yes	Yes	Yes	Yes
Windows 10 (64 bit, Pro)	No	No	Yes	Yes
Windows Server 2012 R2 SP1 (64bit) Standard or Datacenter [2]	Yes	Yes	Yes	No
Windows Server 2016 (64bit) Standard or Datacenter [2]	Yes	Yes	Yes	No

[1] Latest supported Windows version

[2] Not as domain controller

Notice

The version 4.6.2 was the last version to support Windows 7/Windows Server 2008R2 on a server and a client station. *BIS 4.7* is not supported on Windows 7 and Windows Server 2008 R2.

1.2 Server

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

Supporting Software on Windows and Windows Server Operating Systems	• IIS 8.5 for Windows 8.1 and Windows 2012 Server R2 • IIS 10 for Windows 10 and Windows 2016 Server **Notice!** • IIS is not necessary on *BIS* connection servers. • Internet Explorer 9, 10 or 11 in compatibility mode * • .NET for various operating systems: o On Windows 8.1 and Server 2012: .NET 3.51 and .NET 4.5.1 (includes .NET 4.0) o On Windows 10: .NET 3.51 and .NET 4.6.2 (includes .NET 4.0) o On Windows Server 2016: .NET 3.51, .NET 4.6.2 (includes .NET 4.0) **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 4 physical cores • 8 GB RAM (32 GB recommended) • 200 GB of free hard disk space (SSD recommended) • Graphics adapter with o 256 MB RAM, o a resolution of 1280x1024 o at least 32 k colors o 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: o On Windows 8.1 and Server 2012: .NET 3.51 (for Video Engine with DiBos),and .NET 4.5.1 (includes .NET 4.0) o On Windows 10: .NET 3.51 and .NET 4.6.2 (includes .NET 4.0) o On Windows Server 2016: .NET 3.51, .NET 4.6.2 (includes .NET 4.0)
Minimum hardware requirements	• Intel i5 processor (4 Core) or greater • 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 • 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 4.7: EN, DE, RU, ES, ZH-CN, ZH-TW, PL, TR, AR, HU, NL, FR

1.4 Updating BIS to version 4.7

Notice!

1. 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**.
2. If the existing *BIS* is already https enabled, make sure it is properly enabled by running the batchfile file from the installation media:
   `.\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 4.7* installation.
3. If the previous version of *BISProxyOPCDA* is already registered, unregister it before you register the new version. Replace the previous version of *BISProxyOPCDA* with the new version and register it with the one delivered with *BIS 4.7*. The configuration file must not be replaced.

The setup program identifies any currently installed version of *BIS*.

- 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.
- Before upgrading *BIS* to a newer version, make sure that all events are registered in the database.
- Make sure folder `MgtS\EventlogEntries` is empty.
- Before upgrading the *BIS* version, make sure to install SQL server 2008 R2 or any newer supported version. SQL server 2005 will not support this update.
- If the upgrade to *BIS 4.7* fails and the previous version is maintained, it is recommended starting the previous version manually.
- 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. If Windows updates are not turned off, the *BIS* installation might fail due to Windows update processes. Generally, it is recommended to install all Windows updates before the installation.

1.5 Updating Service References in WCF applications

Introduction

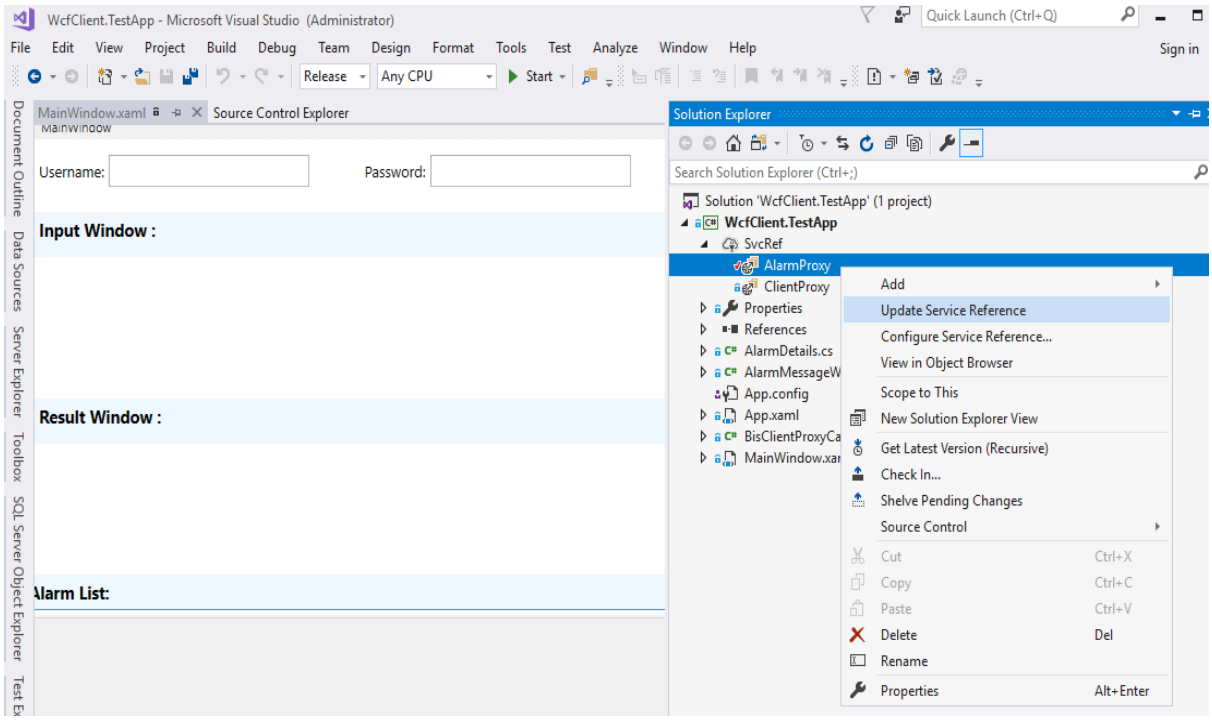
WCF (Windows Communication Foundation) client applications that were created based on an earlier version of the BIS WCF service will not work under BIS 4.7 due to changes in the Service **BISClientProxyWCFService**.

Remedy

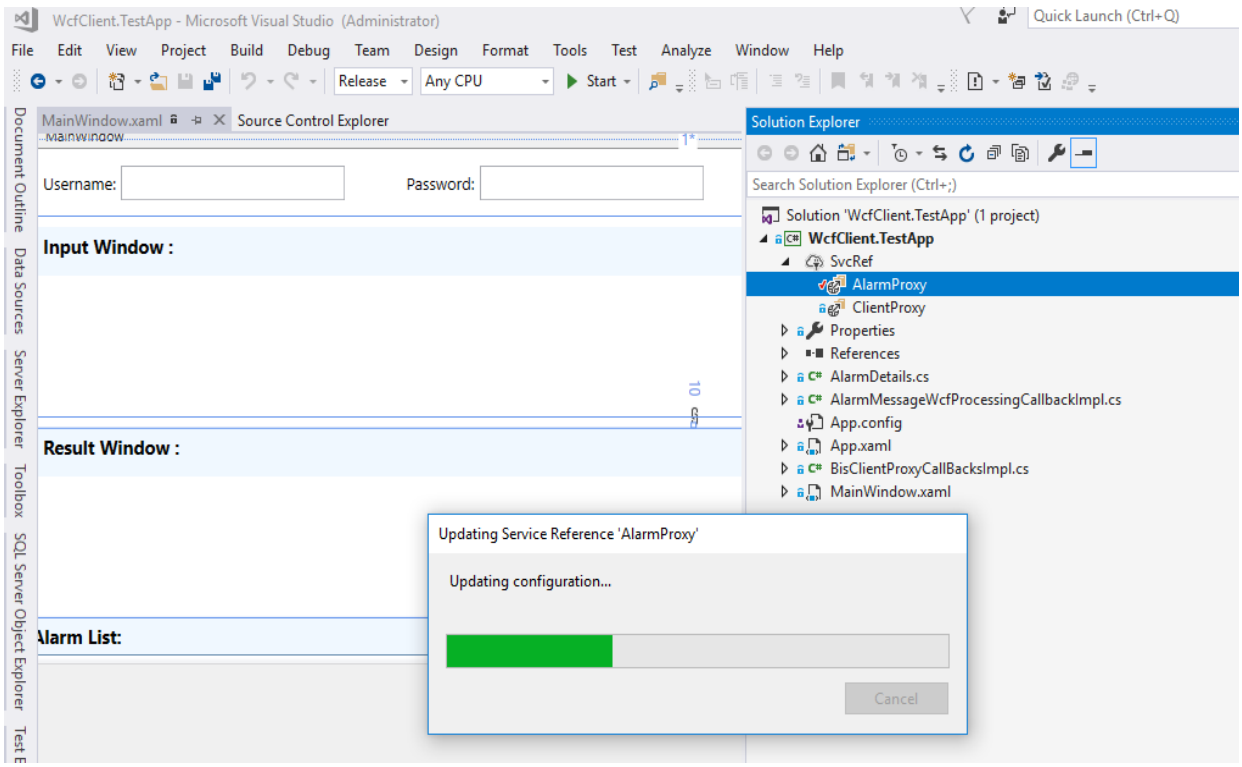
After upgrading to BIS 4.7, update the service references in the code of the client application.

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 SystemLocale 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.

2 New features in version 4.7

Notice!
The limitations cited in this document are the maximum values that have been tested by the time of publication of BIS 4.7. They do not necessarily reflect the absolute maxima for the system.

2.1 Platform

2.1.1 BIS Web Client (BWC)

2.1.1.1 Operational information

- BWC stands for *BIS Web Client*

- BWC client supports the following browsers in Android: Chrome, Firefox and Edge
  Limitation:
  Edge does not support push notification in Android.

- BWC client supports the following browsers in IOS: Safari, Chrome, Firefox and Edge
  Limitation:
  - Shortcut icon is not automatically created.
  - Push notification is not supported.

- BWC client supports the following browsers in Windows: Chrome, Firefox and Edge
  Limitation:
  Windows 8.1 does not support push notification.

- To access BWC client use the following URL:
  `https://<hostname>/bwc`

- The following operations are possible from the BWC client:
  - Login
  - Logout
  - View list of alarms
  - Accept alarm without action plan or miscellaneous document
  - Delete alarm
  - Enable/Disable of disable push notification
  - View information about the current session

- Each logged in session is valid for token duration (default 30 minutes). If the logged in client is inactive for 30 minutes, that session will be automatically logged out.

- The logged in session is extended for 24 hours upon active working. After this time, a new login will be required.

- The two settings above could be changed using the configuration files:
  "*BIS* Installed drive": `\MgtS\SmartClient\BISIdService\appsettings.json`
  `AccessTokenLifetime`: 1800 [30 minutes in seconds - is the default value and this value can be changed]
  `AbsoluteRefreshTokenLifetime`: 86400 [24 hours in seconds - is the default value and this value can be changed]
  The maximum supported value is 1 week for both settings.
  After changing these two values, reset the *BIS IdService* in the application pool from the *Internet Information Service*. If a BWC session is already logged in, make sure to close the session and login again.

- The BWC client can logout even if no alarm is accepted.

- The BWC client accepted alarm status will remain accepted until a logout action is made.

  The session can be manually logged out, or it can logout due to timeout.

Notice!
These operations are not supported by the BWC client:
- Dual operator login
- Logout for client based authorization
- WOBA support (Workstation based authorization)
- IP filtering (Mobile clients are running as 127.0.0.1)

2.1.1.2 BWC – limitations

- The *BIS* manager displays 127.0.0.1 for all browsers that have been logged in through mobile or desktop.
- The information about the BWC session and the token are stored in local cookies. If the cookies are cleared, a new login is necessary. The session that is currently logged in will automatically logout, depending on the configuration that has been set for the token timeout duration.
- Up to 5 tabs are supported in one browser for the same *BIS* server. Opening more than 5 tabs may lead to system malfunction.
- A single login server can open multiple browsers. Each browser will establish a new session within the same *BIS* login server.
- If the alarm is displayed in BWC, and this alarm has an action plan or miscellaneous plan assigned, its not possible to accept this alarm. It is necessary to handle this event in BIS client (native client).
- Any browser refresh from a BWC page will redirect to the alarm list page.

2.1.1.3 BWC-Push notification

The Push notification is a short notification message sent to the logged in client device. The Push notification informs about any new alarm, in case the logged in client is not actively looking into the system.

- The Push notification will turn on automatically for every new login session, even if the Push notification has been turned off in a previous session.
- The Push notification can be turned off in the settings. The settings are reset every new login session.
- When the Push notification is turned on, the BWC client will receive notifications for the following scenarios:
  - For every new alarm generated after the current login
  - *BIS* service is stopped
  - WCF service is stopped
  - 90% before the timeout of the current token
  - After automatic logout due to timeout of current token

- The Push notification does not support incognito or private mode.
- The Push notification requires internet connection.
- The Push notification expires 30 minutes after the notification message is sent.
- Microsoft Edge is not recommended for push notifications, since it does not display the notification message.

Notice! Push notification reliability

Due to the infrastructure involved in the Push notification, these limitations apply:

- There is no guarantee that the Push notification message will be delivered to the client device. The Firefox browser tends to be more reliable than Google Chrome.
- The Push notification time may be inconsistent, as it depends on the internet connectivity.
- If multiple notifications are simultaneously generated in one server, not all the notifications will be received by the client devices.

2.1.1.4 BWC-Shortcut

When accessing the page, a prompt to create a shortcut icon for the BWC website will be displayed. After selecting the prompt, the shortcut icon will be added to the home screen.

- Chrome: A prompt will be displayed at the bottom of the page. If the prompt is closed without adding, then it will not be prompted again until the site settings are reset.
- Edge: A prompt will be displayed at the bottom of the page. This prompt will be displayed for every time a site is visited using Edge, but when the shortcut is created using Chrome, then prompt will no longer appear in Edge.
- Firefox: For the self-signed certificate, it is not possible to add shortcut icon, while using CA provided certificate, an icon to add shortcut will appear next to the site address.

2.1.2 Security improvements

2.1.2.1 HTTPS by default

- The communication from *BIS* client to the *BIS* server is HTTPS.
- The *BIS* server creates a self-signed certificate for communication.

In case a self-signed certificate is used:

- Every *BIS* client needs to download the self-signed certificate from the server and install it on its local machine or device.
- Download the certificate on a client device as follows:

1. On the client device, open the URL of the certificate in a browser.
– For example, if your *BIS* server is called `MYBISSERVER`, the URL will be `http://[Hostname]/MYCERT.CER`

Notice!
The certificate must be downloaded via HTTP. Clear all the history before accessing via HTTP. In case the site is already accessed by HTTPS, then it will not be possible to download the certificate.

2. Save the certificate file in the local storage on the client device.

- Install the certificate on the client workstation as follows:

1. Double click and open the downloaded certificate `MYCERT.CER`
2. Click **Install Certificate** in the **General** tab.
3. Select **Local machine** as store location and click **Next.**
4. Select **Place all certificates in the following store** and click **Browse.**
5. Select **Trusted Root Certification Authorities** and click **Ok.**
6. Click **Next** and click **Finish** to complete the installation of the certificate.

- Install the certificate on a client mobile as follows:

1. On the mobile device open the device **Settings** and enter the word `certificate` to search for the certificates installation menu.
2. Select **Install certificate from storage** (or similarly named menu item, depending on your operating system).
3. Select the imported certificate and install it.
4. Some devices will automatically install the certificate.

Notice!
The certificates are created as a hostname. Logging in while using `https://localhost` or `https://[Host_IP]` will cause issues in the certificate. It is recommended to login using the hostname `https://[hostname]`

Certificate handling:
In order to use of HTTPS and for certificate handling a working DNS is necessary. In case a problem occurs, always check the DNS resolution first.

Self-signed certificate:

- *BIS* 4.7 will create a self-signed certificate for a new installation or an upgrade from a previous *BIS* version which was not HTTPS enabled.
- Self-signed certificates are created with 30 years until expiry date.
- If the previous version of *BIS* is configured for HTTPS using a certificate, the new version of *BIS* will upgrade with its own self-signed certificate.

Limitations:

- Firefox cannot display the **Add to home screen** icon.
- Firefox always displays a warning icon due to the self-signed certificate.

CA signed certificate:
After the *BIS 4.7* installation, in case you need to update the CA signed certificate, proceed as follows:

1. The *Internet Information Services SSL* must be updated with a CA certificate.
2. The new CA certificate thumbprint must be updated to *BISIdservice* configuration file as follows:
   a) Type `certmgr.msc` on Windows *Run* command.
   b) Select the issued CA certificate and open it.
   c) Select the **Details** tab and the **Thumbprint** field.
   d) Copy the thumbprint value (no special characters should be before or after the thumbprint value).
   e) Open the *BIS* installed drive`\MgtS\SmartClient\BISIdService\appsettings.json`
   f) Replace the existing thumbprint value with newly copied thumbprint value.

3. Open the *Internet Information Service* and restart the application pool *BIS IdService Application Pool* to complete the changes.
   - Step 2 could be performed by using the tool `BIS_4.7\Tools\BWCConfigTool\BWCConfigTool.exe`

2.1.2.2 Default password removed for MgtS-Service and SA user accounts

While installing *BIS*, the installer has to provide a password for the *MgtS-Service* account.
While installing *BIS*, the installer has to provide a password for the *SA SQL user* account.

Notice!
If necessary, change the *MGTS-SSRS-Viewer* user password after the installation. Change your password with the *SetPasswordTool,* which can be found in the `MgtS\Tools` folder.
All passwords need to meet the security settings and the security policy of the computer/domain, otherwise the installation will fail.

2.2 Access Engine (ACE)

2.2.1 ACE API (SDK)

Applications using API from *BISACE V4.6.2* are compatible with *BISACE V4.7* servers.

Notice!
Applications compiled with *API V4.6.2* or *V4.7* are not compatible with previous the *BIS* V4.6.1 and earlier.

All changes to the API are documented in detail in the files `ACE API.pdf` and `ACE API Database- xxx.pdf`
Please check if your application has been affected by the changes in the API.

2.2.2 OTIS Elevator integration

The OTIS Compass system is supported by the ACE. The MAC provides an interface to communicate with the OTIS Compass system.

According to the OTIS installation guide, it is necessary to add an additional network card to the access system server to support multicast communication.

To be sure that your system works fine, install BIS/ACE with deactivated second network card. Afterwards, activate the second network card for OTIS. The communication to OTIS system is not encrypted. We recommend to configure the Windows firewall:

`DDSInterface.exe` from MAC must communicate over the second network card only.

The full OTIS system is supported with up to 8 DES (Elevator groups) including redundancy and with 2 DER (Redirector groups). For every DES/DER up to 240 DET (Terminals) can be configured with 255 floors (front&rear). Furthermore, every floor can be configured for public access with\without a time model.

If **PIN only** is activated for a DET, the cardholder can use its PIN for authentication. A DET can be configured to work in one of 4 operational modes. Depending on the operational mode, the way of card usage and the home floor selection changes.

Cardholders can get a home floor assigned with up to 8 additional OTIS options. To support these options, the UI controls must be configured manually in the **custom fields** dialog. Make sure that 3 controls are needed for home floor selection (DES group, floor number, front/rear selection).

1. 0x01 Standard (cannot be combined with Disability)
2. 0x02 Disability (cannot be combined with Standard)
3. 0x04 VIP
4. 0x08 Vertigo
5. 0x10 Split Group Operation.
6. 0x20 CIM override.
7. 0x40 (currently not supported)
8. 0x80 (currently not supported)

Option 1 (standard) and 2 (handicapped) are never sent together to OTIS. If both are set in the dialog, only option 2 is supported and the DETs are communicating to the cardholder.

The BIS interface contains 3 new device families: DDS (Otis DDS), MRE (Otis DES/DER), PANEL (Otis DET). For these new ACE families, the state mapping must be configured in the BIS manually so that the BIS can show if the OTIS system is online or not.

Limitations:

- One OTIS Compass system per MAC.
- A MAC authorization can contain floors from one OTIS DES elevator group only.
- Prox and iClass card types are supported. Other card types have not been tested yet.
- The audit log of a DET can be activated for debugging, but is only visible in ACE logbook and debug log files.
- There is no cardholder area change in the ACE if an OTIS terminal is used.
- The AccessIpConfig tool can only browse fingerprint readers (ARD-FPBEW2-*) within a single IP segment. Therefore do not connect fingerprint readers to a secondary network adapter.

Notice!

ACE API supports cardholder OTIS options and home floor. See API description for details.

Recommendations for a secure OTIS System configuration:

Follow the OTIS configuration guide for connection to the MAC.
In case the MAC is not only used for the OTIS System, but also used for the access system connection, the following points have to be considered:

- Separate Network Interface

  OTIS requires a static IP address on the MAC site. This IP address is provided by the MAC. The network interface on the MAC server has to be configured accordingly. That means, a separate network interface for OTIS has to be installed and configured. It has to be ensured that the subnet of this OTIS interface is separated from the subnet of the access system, so that traffic from one subnet cannot be routed to the other subnet. This recommendation is mandatory to block multicast messages from OTIS network and to protect the access system from possible network attacks.

  In case the access system has to be installed on the server with these two interfaces existing, make sure that the access system uses the correct network interface. This can be done by deactivation of the OTIS interface prior to the access system installation.

- Dedicated MAC on a separate Server

  In case the access system controls critical infrastructure, the MAC should be protected against DoS and DDoS attacks executed towards the OTIS network interface. In this case, it is recommended to install a dedicated MAC for OTIS connection only on a separate server.

- Windows Firewall Exceptions

  The connections in the Windows Firewall can be configured in a process based way to allow communication through Windows Firewall. Allow only the `DDSInterface` executable to communicate with the OTIS subnet.

- Separate card holder PIN for OTIS access

  Card holder with access to high security areas using *PIN Only* (PIN associated to virtual card), should not use the same PIN for OTIS access, because the network messages in the OTIS network are not encrypted and can be easily intercepted. In this case, an extra card holder for OTIS access should be configured.

2.2.3 Threat Level Management

ACE introduces the feature *Threat Level Management*. The goal of threat level management is to respond effectively to an emergency or foreseen situation by making an instant change to the behavior of entrances throughout the affected area.

- Lockout: Only first responders with high security levels can enter.
- Lockdown: All doors are locked. Both entering and exiting are denied to all credentials below a configured security level.
- Evacuation: All exit doors are unlocked.

Typical low threat levels can be configured as follows:

- Sport events: Doors to sport areas are unlocked, all other areas are secured.
- Parents evening: Only selected classrooms and main entrances are accessible.

Up to 15 different threat levels can be defined in the system. Authorized persons can trigger a threat alert with a momentary action. Examples: through the UI of the operator, through a hardware signal (e.g. push button), or by presenting a special alert card at any reader.
Threat levels can be set for each MAC independently. When a threat level is deactivated, entrances revert to their original states and behaviors.

The random screening can be configured in security profiles and assigned to cardholders. The random screening values can be configured in TLM reader profiles. The random screening values are used on activation of a threat level. The random screening rate of the cardholder is adjusted on thread level.

Notice!

- The *BIS* alarm operator has always the control over the doors and readers. Even if the door is blocked by an alarm, the operator can send an **Unblock** command to override the current state of the device.
- To activate the TLM configuration for a complete threat level in the MAC, use the **Activate** selection box on the right side of the threat level name. As long as the flag is not active, the MAC will not switch to the threat.

Limitation:
The configuration of the TLM should not be done while an alarm is active. The manual ACE commands should not be used while configuring TLM.

2.2.4 New Import-Export tool

The new ImportExport tool including documentation is available in the ACE\AddOns directory. Cardholder data can be imported\exported (including LDAP as source of an import). The old ImportExport tool in the BIS/ACE is deprecated and will be removed in future BIS/ACE versions.

2.2.5 Updated support of USB CANON camera

The *CANON SDK* used to enroll cardholder pictures is updated. The ACE now uses the *CANON EDSDK V13.11.0*.

Here is the official compatibility list of *CANON* cameras supported by EDSDK V13.11.0:

- EOS M200
- EOS 90D
- EOS M6 Mark II
- PowerShot G5 X Mark II
- PowerShot G7 X Mark III
- EOS 250D
- EOS RP
- PowerShot SX70 HS
- EOS R
- EOS M50
- EOS 2000D
- EOS 4000D
- EOS M100 [1]
- EOS 6D Mark II
- EOS 200D
- EOS 77D
- EOS 800D
- EOS M6 [1]
- EOS M5 [1]
- EOS 5D Mark IV
- EOS-1D X Mark II
- EOS 80D
- EOS 1300D
- EOS M10 [1]
- EOS 5DS
- EOS 5DS R
- EOS 760D
- EOS 750D
- EOS 7D Mark II

Please note that only the *EDSDK* will be updated in the future (Terms & Conditions agreement applies).

[1] Remote shooting functions are not supported.

2.3 Video Engine

No updates in *BIS 4.7* compared to *BIS 4.6.2*.

Notice!
The *Video Engine* will still run under HTTP mode and no special configuration is required. However, it is recommended to configure the camera in HTTPS instead of HTTP.

3 Resolved issues in BIS version 4.7

3.1 Platform

#214292: Live/replay camera with CPP 3 and newer/VIE
Document updated with more details about *BIS* user for *Video Engine*.
`Live user` is for live view.
`User/user` is for recordings/playback.
`srv admin` is never used for playback or livestream.

#230354: Lose of floor plans and hyperlink symbols after some days
In *Windows 10* clients, the downloaded files are deleted automatically by the operating system with the new *Storage sense* feature.
To avoid the automatic deletion of the files, the following registry settings are recommended:

```
ClientDeploy
{BISInstallationMedia]:\MgtS\ClientDeploy\Tools\IE_InternetSettings_Zone2_TrustedSites_BIS.reg
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\StorageSense]
"AllowStorageSenseGlobal"=dword:00000000
```

#244675: *BIS 4.5* Action Plan video verification issue
The sample action plan for video verification (`AP_VideoVerificationACE_DBUser_VSDK.htm`) and its help document (`UserImage.html`) are delivered with the default **Action Plan** folder.

#245944: *BIS 4.6.1* detector types and conversion to *BIS 4.6.2*
The detector ID `MldTypID_1` is used by the **Forced Door Alarm** detector type. Removal of the detector ID `MldTypID_1` is removing the first created detector. These changes have been rolled back to solve the issue. All the manually created detectors will be deleted from now on.

#245893: Twincat Beckhoff OPC Converting from 4.6.1 to 4.6.2 gives an error in German Language
Is related to #245944 and solved now.

3.2 Access Engine (ACE)

#244795: Change Reader to **Keyboard reader** did not work as expected in all cases. This is now solved.

#243154: In case the **KeyKabinet** change requires more time than the maximum time set until timeout, all the `DlgMgr` clients will be deleted. The SQL statement has been optimized.

#246049: The *Signotec* signature pad only allows cancellation. A new *Signopad* driver has been included.

#242390: Palm vein software malfunction when removing or switching off one palm vein reader is solved.

#243742: The BIS logbook can always be opened from the ACE person dialog. This issue is now solved.

#150025: Incorrect display of the PegaSys duration time is corrected.

#249265: Patch for the Temporary Cards feature
After installing *BIS 4.7* with ACE, installers who intend to provide the **Temporary cards** feature in Access Engine must execute the file `Patch_4_7_TempCards.exe` with Administrator privileges on the ACE server computer. A separate ZIP file, containing the patch, is available for download from the official Bosch Product Catalog or the Bosch Download Store.

API (SDK):
#235780: API Unknown exception Overrun in `DmtArray::GetElement`

#235772: API Unknown exception Column `CLIENTID` does not exist.

#235770: API Unknown exception received while getting values from table columns.

#243210: API transaction fails on Open door permanent command. API incompatibility: API 4.6.2 commands are not compatible with previous *BIS* versions.

4 Known limitations in BIS version 4.7

4.1 Platform

SQL 2016 support
BIS V4.7 supports SQL 2016 SP2 by default. While upgrading an existing *BIS* version, the SQL 2016 will not upgrade simultaneously. The SQL 2016 has to be upgraded separately.

Report print does not work. A cumulative update needs to be executed manually in order to solve the **Report print** issue.
https://support.microsoft.com/en-sg/help/4505830/cumulative-update-8-for-sql-server-2016-sp2

#235434: If *VC++ 2017* or a higher version is already installed, the *BIS* installation will fail.
Workaround: It is necessary to manually uninstall the higher version and proceed with the *BIS* installation, which will install the required version of *VC++*.

#199188: If HTTPS is enabled for audit trail and an upgrade (modify/repair) is done, the service does not start after the upgrade.
Workaround: Disable HTTPS before upgrading or do not enable HTTPS until after the upgrade. Batch files for enabling and disabling HTTPS can be found on the BIS installation medium: `\Tools\HttpsForBIS\`

#188581: The *A1_BISAudit TrailWatcher* service blocks the update of BIS-ACE.
Workaround: Stop the task `AuditTrailFilewatcherservice.exe` in the **Task manager** before the upgrade.

#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. Please check for free space before the installation.

#169416: .NET 4.6 is not supported. Use .NET 4.6.2 instead
If additional software is installed on the *BIS* server, and that software includes *.NET 4.6*, then remove *.NET 4.6* and upgrade to *.NET 4.6.2*.

#126930: Operating System shows message "D3DRM is missing"
If displayed, the message *D3DRM is missing* can be ignored.

#225890: Installer/Licensing/BIS manager does not check the profile type before continuing
If the logged in session is 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.
Do not install or configure *BIS* if running with a temporary profile.

#217043: BIS 4.5 backup error
The *BIS* server could not backup/delete records with 10 GB or larger from the event log database. It is recommended to manage backup/delete before reaching 10 GB.

#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.

4.2 Access Engine (ACE)

#243264: License counters are not directly valid
Sometimes the license counter is valid only after restarting the computer.

#220025: AMC - "performance decrease when writing CSN on CF card"
If a lot of card numbers are identical in the last 4 positions, the message slow card will be displayed on an AMC. This can be observed when using CSN (which is not intended to be used for security reasons) as identification. If you run into this problem, please contact technical support. A final solution is being developed for the next release.

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

#216031: BIS states "Random screening" or "Palm vein verification" do not follow the settings in the Configuration Browser
The enable\disable state for **Random screening** or **Palm vein verification** in the **Configuration Browser** is not shown in the *BIS* Client. If the commands are sent from the *BIS* Client, everything works as expected.

#240773: Set Area dialog
The area of a person is sometimes wrongly set when changing the parking area at the same time.
Workaround: Change the area of the person back to the previous area afterwards.

#222502: If a computer name exceeds more than 15 characters, ACE may not be stable
Make sure that the computer name is shorter than 15 characters before the installation.

#240857: Arming and disarming IDS alarm causes inconsistent AMC messages
The number of the previously used card is randomly sent with the IDS activation/deactivation messages.
Sometimes the card number is attached to the message and sometimes it is not.

#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.

#218694: Visitors.IDTYPE property can be changed by API but is not shown in the visitor dialogs
Import only valid Idtype. Up to now only **passport**, **other** and **identity card** are valid.

#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:
Apply your changes again and save. Synchronize your work with the alarm operator.

#244424: The checkboxes used for activating/deactivating the authorizations for parking places do not work
Having two door model 5c entrances configured in two AMCs in the configuration browser or activating/deactivating the parking zone as part of an authorization will not work. Use the **Assign all entrances/Remove all entrances** buttons.

Simons Voss SmartIntego:

#202508: While deleting a cardholder assigned to a Simons Voss lock, the error message has limited information
While deleting a *Simons Voss* lock, the error message only informs about the *SmartIntego* whitelist authorization assignment, but not about the affected cardholders. Before deleting the lock, remove all the assigned authorizations.

#206393: Sequence monitoring mode 1 does not function correctly when a Simons Voss lock goes offline
In the *Access Sequence Monitoring* mode 1, monitoring should be deactivated when a lock goes offline. This deactivation is currently not functioning for *Simons Voss SmartIntego* devices.

#206241: Simons Voss Delete Whitelist action does not generate user feedback
If the whitelist is deleted from *Simons Voss* devices, the user does not receive confirmation that the command has been executed successfully.

#206988: Simons Voss delete construction whitelist
If a construction whitelist was used before integrating with ACE, the MAC is not always able to delete the construction whitelist.
Workaround: Delete the construction whitelist manually.

Guard tour and Simons Voss readers
A guard tour may be configured using *Simons Voss* readers, but the card registered messages are not sent. These readers are currently not supported for guard tours.

BioEntry W2 Fingerprint Reader

#194295: Access IPconfig Tool
The fingerprint reader scan does not work when multiple network cards or multiple network segments on the same network card are used on the computer.

#184154: Fingerprint reader Wiegand green LED is OFF after red LED is triggered by an AMC (for some card types)
In Wiegand mode, even if **set permanent open** is selected by the controller, when an unauthorized card is used, the green LED is not shown for the card types MIFARE Classic CSN, iClass, EM and Prox.

BioEntry W2 Fingerprint reader in "template on device" configuration
Occasionally, after prolonged use, the card-reading interface of BioEntry W2 has failed in **Finger or Card** mode. The exact causes are still under investigation.
Workaround: Power-cycle the reader. Additonally, there is a hotfix firmware available in the `AccessIpConfig` folder of the installation media.

#195988: Fingerprint reader BioEntry W2: Disable reader beep does not mute the sounder completely
Even when the beep for the reader is disabled in the configuration, the sound generated by the fingerprint reader is still audible, when the fingerprint is successfully read. This is part of the design of this reader and cannot be changed.

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 not more than 100 readers.

Notice!
If the network quality is not reliable, communication can be affected severely in all fingerprint W2 readers. In such cases, the synchronization is restarted and new cardholder updates are sent subsequently, depending on the amount of fingerprints and cardholders. The already transferred cardholders can use the readers independently, but new registrations/unregistrations are synchronized later.
We do not recommend to assign fingerprint templates of visitors and reused cards at W2 readers, because the fingerprint templates might not be up to date. The AMC2 controllers cannot verify if the provided reused card from the W2 reader is from a new visitor or an old visitor in the W2 reader. In secure environments, please use the **template on server** mode.