From	Our Reference	Tel	Grasbrunn
	ESG2-PAS5		November 2020

Issue Mandatory post installation steps

Topic Building Integration System

Description

Contents

From	Our Reference	Tel	Grasbrunn
	ESG2-PAS5		November 2020

Report

Issue Mandatory post installation steps

Topic Building Integration System

1 Installation:

1. Install Building Integration System from the installation medium (using “Setup.exe”), including all necessary Third-Party-Components (Leadtools, …etc.).
2. Remove the installation medium (if applicable).
3. Answer **YES** when prompted to reboot the computer.

4. After this reboot the installation of Building Integration System or Microsoft Patches is done.
5. Afterwards please reboot the computer a second time.

6. Open this document again and proceed as indicated on the next page:
   `<installation root>\MgtS\Platform\Mandatory post installation BIS.pdf`
7. Proceed here after the second reboot:

2 Enhanced HTML pages (supplied by updates):

- This release contains improved templates for HTML pages. To avoid overwriting customized files they are not automatically copied to any existing configuration. Instead are stored under `<installation_root>\MgtS\Default_Configurations`.
  Use these enhanced pages in your existing configuration as desired.

3 Upgrading the configuration:

- After upgrading BIS, old configurations may need to be converted to a new internal format. To perform this conversion start the Configuration Browser and load the configuration. The loading process automatically converts the configuration to the current version.

4 Upgrading Access Engine devices:

- During an upgrade the Access Engine device configuration database is updated to reflect the most recent controller programs. At this time all MAC/AMC controllers are set offline by default, to prevent the new controller programs from being downloaded into the controllers simultaneously and causing widespread disruption.
- See the Access Engine configuration manual for details bring MAC/AMC devices back online separately, at the system administrator's discretion.

5 Upgrading Access Engine pictures:

- An upgrade installation, from BIS version 4.5 or earlier, copies all ID photos and signatures to the ACE database. To verify the success of the copy procedure, ensure that ID photos appear in the ACE personnel dialogs, and check the log file `\AC\Log\DBinstaller.log` for errors.
- After a successful upgrade the original graphic files need to be deleted manually from the folders: `MgtS\AccessEngine\CardholderImages_bak` and `CardholderImages_signBak`.

6 Upgrading Access Engine badge layouts and forms:

1. Due to the addition of a data field for Division, badge layouts and ACE forms must be updated manually after an upgrade.
2. In the Badge Designer program (Configuration Browser Menu: **Tools** > **Badge Designer**, open each layout and save it again. When prompted, select the desired Division for the layout.
   When you have done this, the old layouts can be deleted from the folder `MgtS\AccessEngine\AC\Layouts_bak` manually.
3. In the ACE forms dialog (Configuration Browser Menu: **Infrastructure** > **ACE forms**) use the drop-down list to select a Division for each form in the list.
   When you have done this, the old forms can be deleted from the folder `MgtS\AccessEngine\AC\Forms_bak` manually.

7 Preconditions:

1. BIS by default installs self-signed certificates for secure networking, but can also work with certificates signed by a Certificate Authority (CA).
   Search for `certificate` in the Installation Manual and verify that the procedures have been completed regarding the importing, installing of self-signed certificates and (if necessary) the updating of CA certificates.
2. After the installation, Building Integration System (Service „A1_BISStarter“) will try to start automatically. In case of an upgrade the last configuration used will be loaded. In case of a first installation no configuration is available and Building Integration System will indicate this with a warning signal. How to create a configuration will be described as follows.
3. Start BIS Manager GUI, log on as user "Administrator".
4. Select the ‘**License’** tab
5. Check if the activated licenses are listed. If not, activate the license via License manager. To start License Manager click the ‘**Start License Manager**’ button.
6. Choose the correct features and activate the license using the activation key obtained from the `https://activation.boschsecurity.com` website. Use the computer signature displayed and authorization number to obtain the activation key. Please refer to the BIS Installation Manual on the installation medium for more information.
7. In the license information box all the activated features must be shown. If not, your activation is not correct.
8. In the BIS-Manager "**Event log**" tab the event log size must be indicated. If not, the SQL Server is not properly installed.
9. In the BIS-Manager on tab "System start/stop": Start the Configuration program (BIS Configuration Browser).
10. In BIS Configuration Browser: In case of a first installation you can now create a new configuration. Please select a default configuration to use as a starting point for your own configuration. Logon with the user name “Administrator”. Answer the possible question about data conversion with “**Yes**”. The configuration will be opened.
11. In the configuration GUI, select the field „**Administration**“ and choose "**License**": push the Button "Read", to read the activated licenses. (An error occurs if there are no activated licenses or the features and/or multiplicity of the features do not match with the activated licenses.)
12. Check if all features are enabled correctly.

13. Select "Server structure": Answer the possible question about applying the changes with “**Yes**”. Type in the name of the computer by pressing the button “**Modify**”.
14. Apply the changes again by pressing the button “**Apply**”.
15. Close the BIS Configuration Browser.

8 Start the Building Integration System:

1. Log onto the operating system as user "Administrator".
2. After a reboot, Building Integration System will start automatically with the last used configuration.
3. How to start a configuration manually will be described as follows.
    a. Start the BIS Manager GUI, and log on as "Administrator".
    b. Manager / Folder "Load / Save configuration":
    c. Select the configuration directory by clicking the button "…".
    d. Start the server software by clicking "Load" and answer the questions with “Yes”. It will be automatically switched to the Folder "System start/stop".
    e. The LED on the lower left side must indicate green, and the username of the currently logged on user must appear in the list box. If not, the Proxy manager is installed incorrectly, or DCOM, or an OPC server is not ready to connect.

4. Start Internet Explorer, and change following settings (these settings must be available also for the windows user who later starts the BIS Client):

Important:
- The download and the installation of the BIS client needs **Administrator** rights to work correctly.
- The BIS server certificate must be downloaded and installed on the BIS client machine.

5. Logon with a user with administrator rights and start the Internet Explorer.
[For Windows 10, Windows Server 2016 and Windows Server 2019 launch the Internet Explorer using the context menu and select “**Run as administrator**”]
    a. For all supported Internet Explorer versions (9 + 10 + 11 [partial support]):
    (Only the 32-Bit Versions of Internet Explorer are supported)
    b. The level of the security settings of the trusted sites shall be set to “Medium”.
    c. add: https://<login-server-name>/, do not use https://localhost, since the certificate is issued to login-server-name, starting with https://localhost will malfunction
    d. Change startup page to https://<login-server-name>/
    e. Based on the Default-Level “Medium” setting, please change the following settings:

        – In the “ActiveX controls and plugins” section, set:
            1. “**Allow Scriptlets**” to **Enable**
            2. “**Binary and script behaviours**” to **Enable**
            3. “**Download signed ActiveX controls**” to **Enable**
            4. **Only for Video Engine:**
            “**Download unsigned ActiveX controls**” to **Enable**
            5. “**Initialize and script ActiveX controls not marked as safe for scripting**” to **Enable**

- In the “**Miscellaneous**” section, make the following settings:
  1. “**Access data sources across domains**” to **Enable**
  2. “**Allow scripting of Microsoft web browser control**” to **Enable**
  3. “**Allow web pages to use restricted protocols for active content**” to **Enable**
  4. **“Display mixed content”** to **Enable**
  5. “**Launching applications and unsafe files**” to **Enable**
  6. “**Pop-up blocker** “to **Disable**
  7. “**Phishing Filter**” to **Disable** (formerly known as the Smartscreen filter)

6. In the “**User Authentication**” section, set:
   - “**Logon**” to “**Automatic logon with current username and password**”

Based on the Default-Level “**High**” setting, please change the following settings, additionally to the settings mentioned above:

- In the “ActiveX controls and plugins” section, set:
  – “**Run ActiveX controls and plug-ins**” to **Enable**

- In the “Miscellaneous” section, set:
  – “**Submit nonencrypted form data**” to **Enable**

- In the “Scripting” section, set:
  – “**Active Scripting**” **Enable**

A full listing of all IE 9 + 10 + 11 (partial support) settings can be seen on the BIS installation medium under \Documents\BIS platform\IE-Settings.xls.

Note: Alternate to the manual changes of IE settings, the built in registry settings could be used, which could be downloaded from the BIS server machine
https://<login-server-name>/ClientDeploy/Tools.aspx
Download the file, IE_InternetSettings_Zone2_TrustedSites_BIS.zip , unzip and run the IE_InternetSettings_Zone2_TrustedSites_BIS.reg file, which will make the necessary registry settings required for BIS client automatically.

1. Close Internet Explorer
2. Open Internet Explorer again. A connection to https://<login-server-name>/ is generated automatically.
3. Some components get installed now. No errors should appear. Details of a failed installation are written to a log file: **C:\S3K_Logging\Iexplore\Iexplore.log**
4. At the lower right side, "Trusted Sites" is displayed in Internet Explorer.
5. The login dialog appears.
6. Log on as user "Administrator". If the username is the same as the password, the “**Change password**” dialog will appear. Change the password in accordance with your local rules for strong passwords. If the username is not the same as the password then the BIS GUI starts as normal.
7. Start a log file query (button "EventLog"); The EventLog page appears after a view seconds. The

search results of the default filter (all messages of the last 2 hours) are shown. If not, the IIS is not installed correctly.

8. Log off from the client.
9. Close the BIS Client.
10. BIS-Manager / Folder "System start/stop": Stop server.
11. BIS-Manager / Folder "Error protocol": No error should appear in the list box, except a missing watchdog card, if not installed or after a new installation that a configuration is not present.

9 Notices:

- After the initial installation, the server software **does <u>start</u>** automatically after starting the operating system. **We recommend to leave the startup type on "automatic"!**
- If you want to install the NetLimiter on the client computer, you have to enter the URL <**https://<login-server-name>/ClientDeploy/Tools.aspx**> into Internet Explorer. Download the NetLimiter and start the installation. (The NetLimiter is able to limit the network bandwidth used for the communication between the server and the client. For more information, refer to the Installation manual.)
- With this version a new default page will be deployed, where all Engines are available.
- If you installed more than one products (Engines) and for your existing configuration you want to use the UI of another product, you have to do the following steps:
  - Load your configuration in the BIS Configuration Browser
  - Select "Operators" / Use profile – Manage… / select file / select the path **<installation root>\MgtS\Default-Configurations** / select the BIS product / select the **<Template>** and the sub-directory **Documents** / select the UI file.

  Notice: A copy of the selected file will be stored as part of your configuration.

10 Bringing OPC servers on remote server computers into operation (DCOM settings):

See document `DCOM Configuration.rtf` on the installation medium.

10.1 Realization of the sharing and security model for local accounts:

The communication between Login Server and Remote Server is not possible under Windows Server Windows 10/Windows Server 2016/Windows Server 2019, if the "Sharing and security model for local accounts" is set to "**Guests only - ....**"

During Installation this will be set to "**Classic - ...**" on the affected operating systems.

To revoke this setting.

1. Click: **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Local Policies** > **Security Options** > "**Network access: Sharing and security model for local accounts**"

2. Select "**Guests only - .....**"

Migration of the Event Log databases during upgrades from BIS Versions 1.4.8 or higher (2.*.* or 3.*.* or 4.*.*):

The Event Log database of your previous BIS version must be migrated for use in the newly installed BIS version.

The table below shows which migrations are performed automatically during the installation, and which must be done manually:

FROM BIS version→	**BIS 1.4.8**	**BIS 2.***	**BIS 3.***	**BIS 4.*.***
TO current database version	Manual (Make a backup before starting the upgrade!)	Automatic	Automatic	Automatic

Note that the BIS installation process does not make or restore backups. The making and restoring of backups is always a manual process, performed using BIS Manager > Tab: **Event Log** > **DB Migration**.

For further information about the migration of the databases refer to the BIS and ACE configuration manuals.

11 Certificate for Access Engine workstations

The Access Engine (ACE) by default installs self-signed certificates for secure networking.

Features like video-verification and intrusion configuration dialogs of the access dialogs will require it.

Therefore, on workstations where ACE is running, install the root certificate named

"`Access management system internal CA.cer`"

You will find the certificate on the BIS server after installation, in the directory:

`<Install_Drive>:\Mgts\Certificates\`

--- end of document ---