



BOSCH

Building Integration System

en Installation Manual

Table of contents

1	Legal	4
1.1	Software License Agreement	4
1.1.1	Limited Warranty	4
1.1.2	Remedy	4
2	System Overview	5
2.1	About this manual	5
2.2	Intended audience	5
2.3	BIS single server systems	5
2.4	BIS multi-server systems	6
3	Planning information	9
3.1	System requirements for the BIS server	9
3.2	System requirements for BIS clients	10
3.3	Hardware for special server functions	11
3.4	An overview of the installation process	12
4	Performing a first-time installation	13
4.1	Setting up the network	13
4.1.1	Connecting server computers to the network	13
4.1.2	Installing prerequisite software Internet Information Services (IIS)	14
4.1.3	Setting up a remote SQL Server computer to host the BIS databases	16
4.2	Installing the BIS software on the BIS server	16
4.3	Firewall setup	20
4.4	Engine-specific post-installation information	20
5	Configuring DCOM and OPC servers	21
5.1	Technical background and introduction	21
6	Performing an upgrade installation	22
6.1	Prerequisites and assumptions	22
6.2	Running the BIS installation wizard on the BIS server	24
6.3	Possible further actions	25
7	Configuring BIS clients and optional tools	26
7.1	Configuring the web browsers for the clients	26
7.1.1	Settings for Internet Explorer (IE)	26
7.2	Firewall setup	27
7.3	Installing optional BIS tools	27
7.4	Installing third-party software alongside BIS	28
8	Licensing your BIS installation	29
9	Maintenance and Deinstallation	30
9.1	Maintenance	30
9.2	Backing up and restoring configurations	30
9.3	Deinstallation	30

1 Legal

1.1 Software License Agreement



Notice!

This software relates to security. Limit access to authorized individuals. This software contains provisions for setting security passwords. Establish appropriate security levels and set passwords before allowing operating personnel access to this software. Safeguard the original disk against unauthorized use. Additionally, Bosch Sicherheitssysteme GmbH control panels contain passwords to prevent unauthorized access. These passwords must also be set and their identity carefully safeguarded. You may not transfer this program or license to any other party without the express written approval of Bosch.

1.1.1 Limited Warranty

Bosch Sicherheitssysteme GmbH warrants that the program substantially conforms to the published specifications and documentation, provided that it is used on the computer hardware and with the operating system for which it was designed. Bosch also warrants that the magnetic media on which the program is distributed and the documentation are free of defects in materials and workmanship. No Bosch dealer, distributor, agent, or employee is authorized to make any modification or addition to this warranty, oral or written. Except as specifically provided above, Bosch makes no warranty or representation, either express or implied, with respect to this program or documentation, including their quality, performance, merchantability, or fitness for a particular purpose.

1.1.2 Remedy

Bosch will replace defective media or documentation, or correct substantial program errors at no charge, provided that you return the item with proof of purchase to Bosch within 90 days of the date of delivery. If Bosch is unable to replace defective media or documentation, or correct substantial program errors, Bosch will refund the license fee. These are your sole remedies for any breach of warranty.

Because programs are inherently complex and may not be completely free of errors, you are advised to verify your work. In no event is Bosch liable for direct, indirect, incidental, or consequential damages arising out of the use or inability to use the program or documentation, even if advised of the possibility of such damages. Specifically, Bosch is not responsible for any costs including, but not limited to, those incurred as a result of lost profits or revenue, loss of use of the computer programs or data, the cost of any substitute program, claims by third parties, or for other similar costs. Bosch does not represent that the licensed programs may not be compromised or circumvented. In no case shall Bosch's liability exceed the amount of the license.

Some states do not allow the exclusion or limitation of implied warranties, or limitation of liability for incidental or consequential damages, so the above limitation or exclusion might not apply to you.

Bosch Sicherheitssysteme GmbH retains all rights not expressly granted. Nothing in this license constitutes a waiver of Bosch's rights under the U.S. Copyright laws or any other Federal or state law.

If you have any questions concerning this license, write to Bosch Sicherheitssysteme GmbH, Postfach 1111, 85626 Grasbrunn, GERMANY.

2 System Overview

2.1 About this manual

This guide covers software and hardware installation, initial login and basic maintenance. After the software installation procedure has run you will also need to complete mandatory post-installation procedures. These procedures are displayed in a document window immediately after installation, and can also be found under <installation drive>:\MgtS\Platform\Mandatory post installation BIS.rtf

2.2 Intended audience

As the BIS installer, you should understand the following topics:

- Installing the Windows operating system and applications on a server
- Networking

2.3 BIS single server systems

Definition

A single server BIS system contains only one BIS login server (also known as the BIS server). It may run OPC servers itself, and it may contain zero or more Connection servers and Database server computers.

Illustration

BIS installations vary enormously in size and complexity. The following illustrates a small and a complex BIS single-server installation.



Figure 2.1: A small single server BIS system

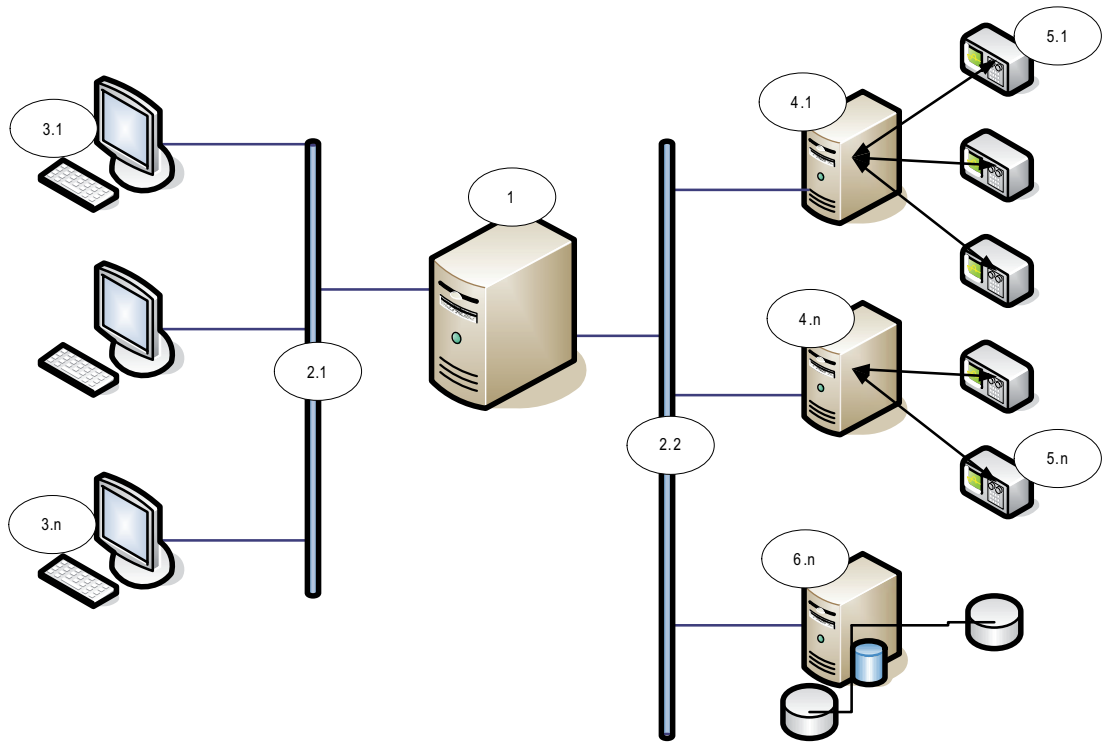


Figure 2.2: A complex single server BIS system

No.	Name	Function
1	BIS (Login) server	Runs the BIS application. The BIS server functions as an OPC client
2.1 to 2.n	Network(s)	Carries signals
3.1 to 3.n	BIS Client Workstation(s)	Runs the BIS user interface
4.1 to 4.n	Connection server(s)	Runs OPC server processes
5.1 to 5.n	OPC device(s)	Interacts with the outside world
6.1 to 6.n	Database server	Hosts BIS data for event log and engines

2.4 BIS multi-server systems

Definition

A multi-server BIS system is one in which two or more BIS single server systems share information. BIS multi-server systems can be organized as hierarchical or peer-to-peer networks.

Implementation overview

Participating BIS single-server systems can be providers of information, consumers of information, or both simultaneously.

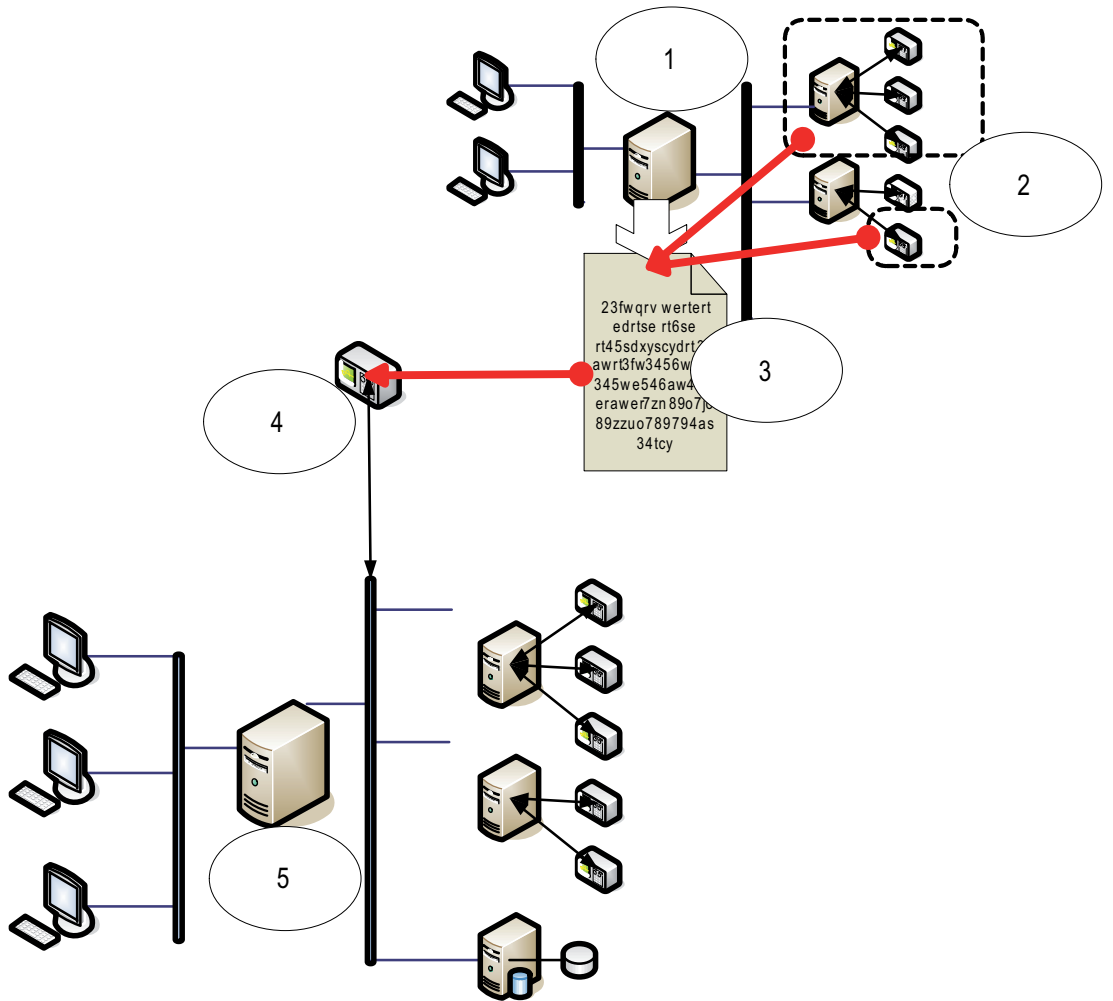
- The Provider server creates a configuration file that details exactly which information it should share with others.

- The Consumer server configures and browses the provider server as a remote OPC server.

Any or all of the information monitored by the provider can be passed to the consumer or consumers. Typically the information consists of OPC addresses, state-changes, commands and alarms.

Illustration

For simplicity, the following illustrates the interaction of one provider and one consumer server. The size and complexity of the multi-server BIS system is limited by the network traffic and the capacity of the consumer servers to process incoming data.



No.	Name	Function
1	The provider server	A kind of BIS server that provides information to other BIS single server systems
2	The subset of the addresses that the provider server should share	
3	The encrypted configuration file generated by the provider server	Describes the subset of information that the provider server should share

No.	Name	Function
4	An OPC server of type BIS Remote System	Acts as an interface between the provider server and the consumer server. It is configured on the consumer server using the encrypted configuration file, and then browsed like any other connection server.
5	The consumer server	This BIS server receives and processes information from its own devices, and those of connected provider servers

3 Planning information

3.1 System requirements for the BIS server

Servers	
Supported operating systems (standalone or client/server mode). Installations of BIS on other operating systems may succeed, but are entirely without warranty.	<ul style="list-style-type: none"> - Windows 7 SP1 (32 or 64 bit, Pro, Enterprise) - Windows Server 2008 R2 SP1 (64 bit, Standard, Datacenter) - Windows 8.1 (64 bit, Pro, Enterprise) - Windows Server 2012 R2 (64 bit, Standard, Datacenter) - Windows Server 2016 (64 bit, Standard, Datacenter) - Windows 10 Enterprise LTSB (64 bit) - Note: The default database delivered with this BIS Version is SQL Server 2016 SP2 Express edition with advanced services
Other Software	<ul style="list-style-type: none"> - IIS 7.0 or 7.5 for Windows 7 and Windows 2008 Server R2 - IIS 8.5 for Windows 8.1 and Windows 2012 Server R2 - IIS 10.0 for Windows 10 - Note: IIS is not necessary on BIS connection servers - Internet Explorer 9, 10 or 11 in compatibility mode - .NET for various operating systems: <ul style="list-style-type: none"> - On Windows 7 and Server 2008: .NET 3.51 and .NET 4.0 - On Windows 8.1 and Server 2012: .NET 3.51 and .NET 4.5.1 (includes .NET 4.0) - On Windows 10: .NET 3.51 and .NET 4.6.1 (includes .NET 4.0) - Latest drivers and OS updates are highly recommended.
Minimum hardware requirements	<ul style="list-style-type: none"> - Intel i5 processor with at least 4 physical cores - 8 GB RAM (32 GB recommended) - 200 GB of free hard disk space - Graphics adapter with <ul style="list-style-type: none"> - 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

Other general requirements

- A TCP/IP network connecting BIS and database servers
- A unique name for each computer, no longer than 15 Latin characters without diacritic marks.
- US American or standard European date-time formats: MM/dd/yyyy or dd.MM.yyyy
- A user account with Windows administrator rights and password
- If the local security policy forbids the weak MgtS-Service password then create the MgtS-Service user manually with a compliant password.
- Antivirus software should be installed but must not be running during BIS installation.

General recommendations

- Use US regional settings, even if the language of your operating system is not US English.
- Copy the BIS installation files to a subdirectory of the main disk drive and install from there, not from the Windows desktop.



Notice!

Hyper-threading

On Systems with I5 / I7 / Xenon Processors BIS performance is improved if Hyper-threading is disabled.



Notice!

Primary Domain Controllers (PDCs) and Backup Domain Controllers (BDCs) are not supported as they do not provide the administration of local user accounts necessary for management systems.



Notice!

The performance of the system components will depend largely on the size of the system, i.e. the number of objects under BIS's control. To maximize performance BIS should always be run as a standalone application on an up-to-date computer in a subnet where there is no other business-critical traffic. Nevertheless Bosch recommends testing existing network hardware under projected network conditions, particularly if heavy use is to be made of IP cameras and image archiving.

3.2 System requirements for BIS clients

Clients	
Supported operating systems (standalone or client/server mode). Installations of BIS on other operating systems may succeed, but are entirely without warranty.	<ul style="list-style-type: none"> - Windows 7 SP1 (32 or 64 bit, Pro, Enterprise) - Windows Server 2008 R2 SP1 (64 bit, Standard, Datacenter) - Windows 8.1 (32 or 64 bit, Pro, Enterprise) - Windows Server 2012 R2 (64 bit, Standard, Datacenter) - Windows Server 2016 (64 bit, Standard, Datacenter) - Windows 10 (32 or 64 bit, Pro or Enterprise LTSB) <ul style="list-style-type: none"> - Note: with a Pro edition, updates must be deferred until 8 months after the release of the BIS version. For further information see the Microsoft technet page at https://technet.microsoft.com/en-us/itpro/windows/manage/introduction-to-windows-10-servicing
Other Software	<ul style="list-style-type: none"> - ASP.NET - Internet Explorer 9, 10 or 11 in compatibility mode (Note: The SEE client requires IE 9.0) - .NET for various operating systems:

Clients	
	<ul style="list-style-type: none"> - On Windows 7 and Server 2008: .NET 3.51 (for Video Engine with DiBos),and .NET 4.0 - On Windows 8.1 and Server 2012: .NET 3.51 (for Video Engine with DiBos),and .NET 4.5.1 (includes .NET 4.0) - On Windows 10: .NET 3.51 and .NET 4.6.1 (includes .NET 4.0)
Minimum hardware requirements	<ul style="list-style-type: none"> - Intel i5 or higher - 8 GB RAM (16 GB recommended) - 20 GB free hard disk space - Graphics adapter with <ul style="list-style-type: none"> - 256 MB RAM, - a resolution of 1280x1024 - at least 32 k colors - OpenGL® 2.1 and DirectX® 11 - 100 Mbit/s Ethernet card
Additional minimum requirements for VIE (Video Engine) clients	<ul style="list-style-type: none"> - 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



Notice!

It is recommended that neither the BIS login server nor connection servers be used as a VIE client, in order to rule out possible conflicts with other video components.

3.3

Hardware for special server functions

Server Function	Required Hardware
System networking (additional remote computers, network printers, control computers in the local network.	One Ethernet network card per network (OPC subsystems and client workstations may be on separate networks).
Single monitor operation	VGA graphics card to support a single monitor
Multiple monitor operation (up to four monitors)	VGA graphics card(s) to support the desired number of monitors
Subsystems and external systems such as bus couplers (non-network connections)	One serial interface COM port per connection (onboard or on an interface expansion card)
Additional log or alarm printers	One serial or parallel interface, depending on the printer (onboard or on an interface expansion card). Network printing is also possible.

Server Function	Required Hardware
External devices e.g. backup storage device	Appropriate controllers

3.4

An overview of the installation process

A BIS installation generally consists of the following stages, which are described in the rest of this document.

1. Setting up the network. Section *Performing a first-time installation, page 13*
2. Installing the BIS software on the BIS server:
 - first-time Section *Performing a first-time installation, page 13* or
 - upgrade Section *Performing an upgrade installation, page 22*).
3. Installing/configuring the Firewall. Section *Firewall setup, page 20*
4. Configuring DCOM and OPC servers on the connection server(s). Section *Configuring DCOM and OPC servers, page 21*
5. Configuring the web browsers on the clients. Section *Configuring BIS clients and optional tools, page 26*
6. Installing optional BIS tools as required. Section *Installing optional BIS tools, page 27*
7. Licensing. Section *Licensing your BIS installation, page 29*

4 Performing a first-time installation

The recommended overall order of a first-time installation (hardware and software) of a BIS system is as follows, though not all steps will be necessary in all cases:

1. Setting up the network of computers where BIS and its database(s) are to run
2. Installing the BIS software on the BIS server.
3. Installing/configuring a Firewall
4. Making any engine-specific adjustments to the installation.

The configuration of DCOM settings for any connection server(s) participating in the BIS installation is handled separately in Section *Configuring DCOM and OPC servers*, page 21

4.1 Setting up the network

BIS typically runs in a TCP/IP network consisting of

- A **BIS server**. The server that runs the main BIS application software is also commonly referred to as the **login server**.
 - Note that in Multi-server BIS systems more than one BIS server may be present.
- Zero or more connection servers which communicate with peripheral devices such as detectors, alarm annunciators, entrances, video cameras etc.
- Zero or more **operator workstations**, also known as **BIS clients**. These are typically PCs, which each run the BIS user interface in a web browser.
- Zero or more separate database servers .

Nevertheless the BIS server can assume the functions of connection server and operator workstation as well as hosting its own databases.

4.1.1 Connecting server computers to the network

To manage the many systems of a building, the BIS server is typically connected to a network. It is not necessary for clients and subsystems to be on the same network, i.e. you can dedicate one network to the connected subsystems, and another network for BIS client PCs.

Server names

Each computer requires a unique name and a unique IP address. The following restrictions apply to server names:

- No longer than 15 characters
- No digit as the first character in the name
- No non-Latin characters, and no characters with diacritic marks. The NetBIOS name is recommended

Connections to database servers

Network connections to any **database servers** (see *Setting up a remote SQL Server computer to host the BIS databases*, page 16) to be used in the BIS configuration need to exist before installing the BIS software, because the installation wizard may need to browse for them.

Connection servers for running OPC server processes can, by contrast, be set up after installing the BIS software (refer to the hardware's own documentation and to section *Configuring DCOM and OPC servers*, page 21 in this document).

The Ethernet connections can be 10 or 100 or 1000BaseT (twisted pair). If the connection is directly from one network adapter to another then use a null-modem "crossover" cable.



Notice!

Disable any “System standby” or “Hibernation” options on all computers that are part of the BIS System (BIS Login Server, BIS Connection Servers, BIS Clients ...).

See also

- *Setting up a remote SQL Server computer to host the BIS databases, page 16*
- *Configuring DCOM and OPC servers, page 21*

4.1.2

Installing prerequisite software Internet Information Services (IIS)

IIS must be installed on the BIS Server before installing the BIS application. IIS is an optional Windows component for which you may need your Windows installation media.

A new IIS installation script `InstallIISForBIS.exe` is provided on the BIS installation medium in the directory `Tools\InstallIISForBIS\`. This script makes all the required settings listed in the table below. Note that the script requires .NET 4.0.

IMPORTANT: If you are not using the script to install IIS, omit the CGI feature. Otherwise ensure that the IIS installation includes the following settings on Windows 7, 8.1 or 10, and Windows 2008, 2012 or 2016 Server respectively.

Windows 7, 8.1 and 10		Windows 2008 Server R2 and Windows 2012 Server Windows 2016 Server
<p>Internet Information Services ..Web Management Tools: IIS 6 Management Compatibility</p> <ul style="list-style-type: none"> - [the settings] <ul style="list-style-type: none"> - IIS 6 Management Console - IIS 6 Scripting Tools - IIS 6 WMI Compatibility - IIS 6 Metabase and IIS 6 configuration compatibility - IIS Management Console - IIS Management Scripts and Tools - IIS Management Service 		<p>Web Server ..Common HTTP Features:</p> <ul style="list-style-type: none"> - Static Content - Default Document - Directory Browsing - HTTP Errors
<p>World Wide Web Services: ..Application Development Features:</p> <ul style="list-style-type: none"> - [On Windows 7 systems] <ul style="list-style-type: none"> - ASP.NET - .NET Extensibility - [On Windows 8.1 systems] <ul style="list-style-type: none"> - ASP.NET 3.5 and - ASP.NET 4.5 - .NET Extensibility 3.5 and - .NET Extensibility 4.5 - [On Windows 10 systems] <ul style="list-style-type: none"> - ASP.NET 3.5 and - ASP.NET 4.6 - .NET Extensibility 3.5 and - .NET Extensibility 4.6 		<p>..Application Development:</p> <ul style="list-style-type: none"> - [On Windows Server 2008 R2 systems] <ul style="list-style-type: none"> - ASP.NET - .NET Extensibility - [On Windows Server 2012 systems] <ul style="list-style-type: none"> - ASP.NET 3.5 and - ASP.NET 4.5 - .NET Extensibility 3.5 and - .NET Extensibility 4.5 - ISAPI Extensions - ISAPI Filters

Windows 7, 8.1 and 10		Windows 2008 Server R2 and Windows 2012 Server Windows 2016 Server
<ul style="list-style-type: none"> - ISAPI Extensions - ISAPI Filters 		
<p>..Common HTTP Features:</p> <ul style="list-style-type: none"> - Default Document - Directory Browsing - HTTP Errors - Static Content 		<p>..Health and Diagnostics:</p> <ul style="list-style-type: none"> - HTTP Logging - Request Monitor
<p>..Health and Diagnostics:</p> <ul style="list-style-type: none"> - HTTP Logging - Request Monitor 		<p>..Security:</p> <ul style="list-style-type: none"> - Windows Authentication - Request Filtering - IP and Domain Restrictions
<p>..Performance Features:</p> <ul style="list-style-type: none"> - Static Content Compression 		<p>..Performance:</p> <ul style="list-style-type: none"> - Static Content Compression
<p>..Security:</p> <ul style="list-style-type: none"> - IP Security - Request Filtering - Windows Authentication 		<p>Management Tools:</p> <ul style="list-style-type: none"> - IIS Management Console - IIS Management Scripts and Tools - Management Service <p>....Management Compatibility:</p> <ul style="list-style-type: none"> - - IIS 6 Metabase Compatibility - IIS 6 WMI Compatibility - IIS 6 Scripting Tools - IIS 6 Management Console

Windows 8.1 and 10		Windows 2012 Server and Windows 2016 Server only
<p>.NET Framework 3.5</p> <ul style="list-style-type: none"> - Windows Communication Foundation (WCF) HTTP Activation - Windows Communication Foundation (WCF) Non-HTTP Activation <p>.NET Framework 4.5 (4.6 for Windows 10) Advanced Services, WCF services</p> <ul style="list-style-type: none"> - HTTP Activation 		<p>.NET Framework 3.5 features</p> <ul style="list-style-type: none"> - HTTP Activation - Non-HTTP Activation <p>.NET Framework 4.5 features, WCF services</p> <ul style="list-style-type: none"> - HTTP Activation

Disabling the IIS CGI feature

If IIS is already installed with CGI, the feature should be disabled as follows for Windows 7 and Windows Server 2008 R2:

- Windows 7, 8.1 and 10: **Start > Control Panel > Programs > Turn Windows features on or off > Internet Information Services > World Wide Web Services > Application Development Features > CGI**

- Windows Server 2008 R2 and 2012: **Start > Control Panel > Administrative Tools > Server Manager > Remove Role Services > Web Server > Application Development > CGI**

4.1.3

Setting up a remote SQL Server computer to host the BIS databases

If you wish your BIS installation to use databases over the network on separate servers then these servers should be set up before starting the BIS installation. The instructions for this can be found on the BIS installation medium under: <language folder>\BIS\Tools \BISRemoteSQLServerSetup\Readme.rtf

In the same directory is an installation kit which should be run on each of the remote database servers.

**Notice!**

Limitation

A remote SQL Server computer that is used for Reporting Services can only serve one BIS installation.

**Notice!**

Instance name and computer name

Ensure that the name of the database instance is no longer than 15 characters and does not match the name of the computer.

4.2

Installing the BIS software on the BIS server

Before you begin

For the installation, use an account with local administrator permissions, preferably the **Administrator** account itself. Verify by typing **ipconfig** to a command prompt that the server has an IP address. Ensure that you have your MS Windows installation media to hand, in case the BIS installation wizard requires extra features.

BIS will not install if a firewall is active. The BIS installation wizard is able to disable the Windows firewall, however any other firewalls should now be disabled manually before starting the BIS installation procedure.

**Notice!**

Installation to local computer only

The BIS installation kit may be on a separate networked computer, but setup.exe will only install BIS to the computer which invoked it.

**Notice!**

Avoid special characters

Use no special or non-Latin characters in BIS (e.g. Chinese, Russian, ä, é, ô, /, #, %, \$, |, !, ~, ‘). Use only non-diacritic (7-bit ASCII), alphanumeric characters [A-z] [0-9] plus underscore. This applies to any characters typed into the BIS installation wizard or configuration browser, including passwords.

Step	Action	Effect(s), Notes, Explanations
1	Right-click setup.exe and select Run as administrator .	<p>The language selection dialog opens.</p> <p>Notes:</p> <ul style="list-style-type: none"> - Apart from German and Russian all installations are currently performed in English. - To display Russian characters properly on a non-Russian operating system you must change the system locale to Russian. - Once BIS has been installed in a particular language that language can not be changed by a subsequent update installation on the same computer.
2	Select the interface language of your new BIS system and click Next>	<p>The BIS installation preparation wizard opens. The wizard searches the PC for existing software required by BIS and adapts the installation agenda accordingly. Depending on what is already available the wizard will mark the following prerequisite software for installation along with BIS</p> <ul style="list-style-type: none"> - Windows Installer - Required versions of the Microsoft .NET Framework. Note that if not installing BIS on Windows 7 then you will be prompted to install .NET Framework 3.5 separately from your Operating System’s installation media. - SQL DMO/SMO support
3	Click Next>	<p>If the installation wizard detects an active Windows firewall then click Yes, I want to disable the Windows Firewall, then click Next> to disable it. Other firewalls must be disabled manually outside of the BIS installation procedure before proceeding.</p>
		<p>By default, the installation wizard installs the MgtS directory at the root level of the local C: drive. If this location is acceptable, click Next>. If you wish to select a different installation path (local drives only), click Browse.</p>
		<p>The Select Features dialog appears</p>
4	Use the BIS feature selection window to identify which BIS features you wish to install.	<p>Select only the engine(s) and connection(s) that you have purchased from Bosch. Without being licensed other features will not be usable, and will only take up disk space. The default installation includes all BIS features. Use the drop-down menus to exclude features that you do not wish to install.</p>
5	Click Next>	<p>The next stage of the installation process is the setting up of database instances for those selected engines and features that require them (Event Log/Security Engine, Access Engine, and, in the next step, Reporting Services).</p> <p>If you already own high-capacity SQL Server licenses you can use these for BIS. Else BIS can install limited-capacity fresh instances for you (see: <i>SQL Server compatibility issues, page 18</i> below).</p>

Step	Action	Effect(s), Notes, Explanations
		There are basically 3 possibilities regarding the availability of suitable SQL Server instances, described as A , B and C below:
	Availability of suitable SQL Server instances	Action
A	No suitable (*) SQL Server instance exists on the login server or on the network	> Click the Create button. BIS will set up separate instances of its current default version of SQL Server Express Edition with Advanced Services for: <ul style="list-style-type: none"> - Event Log/Security Engine (SEE only if required) - Reporting Services - (if required) Access Engine
B	A suitable (*) SQL Server instance can be found by browsing the login server or the network.	> Click the Browse button to select an instance by browsing the network.
C	A suitable (*) SQL Server instance exists but can not be found by browsing the login server or the network.	> Enter the instance manually in the text field for the SQL Server Name using the syntax: <computername>\<instancename> , e.g. MYSERVER\MYINSTANCE.
(*) For an explanation of "suitable" see the cautionary note <i>SQL Server compatibility issues</i> , page 18 below.		

SQL Server compatibility issues

Notice!

SQL Server compatibility issues affecting SQL Server options B (Browse) and C (manual entry) above:

The following combinations are incompatible:

Access Engine (ACE) with the unnamed instance (LOCAL) of any SQL Server

Access Engine (ACE) with Event log/Security Engine together on the same instance of any SQL Server Express Edition.

BIS Reporting Services with SQL Server versions below 2008.

BIS in general with SQL Server versions below 2005 SP2. Such databases need to be upgraded manually before they can be used with BIS.

BIS versions below 4.3 with SQL Server versions above SQL Server 2012 (BIS on Windows 10 Enterprise LTSB will only be supported with SQL 2014)

Windows 8.1 and Windows 2012 Server with SQL Server versions below SQL Server 2012.

Note that BIS will nevertheless cooperate with separate database servers running Windows 7 or Windows 2008 Server R2 and SQL Server versions below SQL Server 2012, with the limitations described below.

Windows 2016 Server will support only SQL Server 2012 SP2 and SQL Server 2014 SP1





Notice!

For BIS SQL Server instances hosting Access Engine (ACE) you must use **SQL-Authentication** and not Windows authentication. If you browse or enter existing instances for ACE, then enter the “sa” password of that instance in the dialog box.

SQL Server Express Edition cannot use more than 1GB of RAM and cannot handle databases larger than 10 GB.

Step	Action	Effect(s), Notes, Explanations
6	Using the actions (A,B,C) described above, configure the instances you require for Event Log/SEE and Access Engine.	<p>IMPORTANT - Only when creating a new database instance: always take the <code>sa</code> user for the administrator account.</p> <p>The BIS installation wizard stores your choices for the database installation.</p>
7	Similarly, use the BIS installation wizard to locate on the network an instance of the Microsoft SQL Server for BIS Reporting Services.	<p>IMPORTANT NOTE: This step only occurs if you chose action B or C in the step above, because if a new instance was created for the Event Log in the previous step, then Reporting Services will automatically be activated on the same instance.</p> <p>This Reporting Services database can be a separate named instance, or can share an SQL 2008 or later instance with Event log/SEE.</p> <ul style="list-style-type: none"> - To create a separate instance (e.g. if no name appears in the text box labeled Report Server Instance) click the Create button. A pop-up window appears suggesting the name BISREPORTS. Confirm (recommended) or change the instance name then click OK to return to the previous window and continue the installation. - To search for SQL Server instances on remote nodes, enter the name of the remote node manually and click the Browse button. - To share an instance, select the check box: Use the same SQL Server as for Event Log



Step	Action	Effect(s), Notes, Explanations
8	Click Next>	<ul style="list-style-type: none"> – SQL Server installs. – The BIS application installs. – All requested databases are installed. – The BIS installation wizard finishes installing the application.
9	Click Finish.	The Mandatory Post Installation BIS.rtf file opens.
10	Please read and follow the directions in this file, then close the window.	The file contains important information and instructions.
11	You must restart the PC to complete the BIS installation. Click Yes to restart the PC.	<p>The first-time installation of the BIS application is complete. An icon for the BIS Manager has appeared on the desktop.</p> <p>The default username and password is Administrator. Note that the password (but not the username) is case-sensitive.</p>
12	After completing the installation, use the License tab in the BIS Configuration Manager to initiate the licensing procedure.	See <i>Licensing your BIS installation, page 29</i>
13	Create an initial configuration in the BIS Manager	See BIS Configuration online help for instructions. Press the F1 key when in the BIS Manager.

4.3 Firewall setup

Windows versions install their own firewalls, which need only be configured. Please install any other firewalls as per the manufacturer's instructions. Please configure your firewall (Windows or third party) for use with BIS as described in the file <installation_drive>:\MgtS\Platform\BIS_XP_Firewall_Configuration.rtf

Note: there are historical reasons for the name of the file. It is **not** restricted to Windows XP.

4.4 Engine-specific post-installation information

The various BIS engines may require additional settings after the main BIS installation. Depending on which engines you are using, please consult the engine-specific installation guides in the respective subdirectories of <installation_drive>:\MgtS\

5 Configuring DCOM and OPC servers

This section is only relevant if you wish to install OPC servers, particularly third-party OPC servers.

5.1 Technical background and introduction

The main task of the BIS application on the BIS (login) server is to collect information from, and pass commands to, OPC Server processes. These processes, known as OPC servers, are themselves standardized interfaces to a wide variety of devices e.g. door controllers, fire alarms and cameras.

The OPC server processes often run not on the BIS server computer, but on remote computers known as **connection servers**. The network communication between a BIS server and a connection server is handled using DCOM (Distributed Common Object Model) and a common user account called **MgtS-Service**. The OPC server in effect assumes the identity and credentials of the MgtS-Service user account.

For this to function, the following need to be done:

- The MgtS-Service user account must exist on the connection server
- MgtS-Service must have sufficient access rights to launch and activate, both locally and remotely
- The OPC server installation routine, if available, must be executed. **Note:** Depending on the manufacturer these routines can be more or less comprehensive. Many will include the following tasks, but some tasks may need to be done manually. In all cases, please consult the documentation of the OPC server concerned:
 - Installing the OPC core components.
 - Preparing DCOM to support the OPC server.
 - Installing the OPC server.
 - DCOM configuration of the newly installed OPC server, e.g. its user identity (usually set to MgtS-Service).

These procedures are described in a separate document on the BIS installation medium:

DCOM Configuration.rtf

Connecting OPC servers to a BIS installation

OPC servers vary greatly in their complexity, and consequently in the complexity of the procedures to connect them to a BIS installation. For details on connecting individual OPC servers, please consult the **BIS Configuration Guide** online help.

6 Performing an upgrade installation



Notice!

Compatibility with existing panels

There may be version conflicts between the new BIS version and the OPC servers of any fire or intrusion panels already in your installation (e.g. Bosch FPA or MAP panels). To avoid such conflicts Bosch urgently recommends that you upgrade these panels to the latest firmware **before** starting the BIS upgrade installation.

The following are the major steps in upgrading a BIS system:

1. Plan your upgrade path depending on your starting version, your target version, and whether or not you are using the Access Engine. See the tables of upgrade paths below.
2. Ensure that the hardware, prerequisite software and license file have been upgraded to the specifications in *Planning information, page 9*, and that there is no incompatibility with your existing databases, see the information panel SQL Server compatibility issues in the section *Installing the BIS software on the BIS server, page 16*
3. Stop the BIS system (and ACE, if installed)
4. Carry out any necessary upgrades of SQL server.
5. Run the BIS setup on the BIS server.

These steps are described in more detail in the sections below.

6.1 Prerequisites and assumptions

The following tables describe the supported upgrade paths for BIS versions, both without and with Access Engine (ACE). Do not proceed unless your proposed upgrade path is supported. It may be necessary to perform the upgrade in multiple stages, see *Deinstallation, page 30*

Note that an update installation to the latest BIS version will always remove previous versions, but will provide continuity by preserving the configurations, and converting and preserving the databases with their contents.

Nevertheless see the **Notice** panels about MS SQL Server 2000 and WCF customizations below.

from/to	BIS 1.4.8	BIS 2.0	BIS 2.1	BIS 2.2	BIS 2.3	BIS 2.4	BIS 2.5	BIS 3.0	BIS 4.0	BIS 4.1	BIS 4.2	BIS 4.3	BIS 4.4	BIS 4.5	BIS 4.6
BIS 1.4.1	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
BIS 1.4.8		✓	✓	✓	✓	✓	✓	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*
BIS 2.0			✓	✓	✓	✓	✓	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*
BIS 2.1				✓	✓	✓	✓	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*
BIS 2.2					✓	✓	✓	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*
BIS 2.3						✓	✓	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*
BIS 2.4							✓	✓	✓	✓	✓	✓	✓	✓	✓
BIS 2.5								✓	✓	✓	✓	✓	✓	✓	✓
BIS 3.0									✓	✓	✓	✓	✓	✓	✓
BIS 4.0										✓	✓	✓	✓	✓	✓
BIS 4.1											✓	✓	✓	✓	✓
BIS 4.2												✓	✓	✓	✓
BIS 4.3													✓	✓	✓
BIS 4.4														✓	✓
BIS 4.5															✓

Notice!

*) MS SQL Server 2005



Microsoft SQL Server 2014 SP1 or later can not convert backup databases directly from an SQL Server version before 2005 SP3. If you still have backup databases from before SQL Server 2005 SP3 you will need to carry out an interim upgrade to version BIS 2.5 (with its SQL Server 2008) first, before you can upgrade to BIS versions 4.x (which have SQL Server 2012).

Microsoft SQL Server 2005 SP3 is the minimum version for an upgrade to Microsoft SQL Server 2014.



Notice!

Multi-Server BIS and customized WCF configurations

If you have made manual changes to the WCF configuration file:

`\MgtS\Platform\BisClientProxyWcfServer\BisClientProxyWcfServer.exe.config`

in BIS 4.0, these will also be migrated to BIS 4.1 and newer versions. Before customizing this

file refer to the specialist documentation in `\MgtS\Platform\WCF Configuration.pdf`

from \ to	BIS 1.4.8	BIS 2.0	BIS 2.1	BIS 2.2	BIS 2.3	BIS 2.4	BIS 2.5	BIS 3.0	BIS 4.0	BIS 4.1	BIS 4.2	BIS 4.3	BIS 4.4	BIS 4.5	BIS 4.6
BIS 1.4.1(ACE >= 1.2.50)	✓	X	X	X	X	X	X	X	X	X	X	X	X	X	X
BIS 1.4.8		✓	X	X	X	X	X	X	X	X	X	X	X	X	X
BIS 2.0			✓	X	X	X	X	X	X	X	X	X	X	X	X
BIS 2.1				✓	X	X	X	X	X	X	X	X	X	X	X
BIS 2.2					✓	X	X	X	X	X	X	X	X	X	X
BIS 2.3						✓	X	X	X	X	X	X	X	X	X
BIS 2.4							✓	X	X	X	X	X	X	X	X
BIS 2.5								✓	✓	✓	✓	✓	✓	✓	✓
BIS 3.0									✓	✓	✓	✓	✓	✓	✓
BIS 4.0										✓	✓	✓	✓	✓	✓
BIS 4.1											✓	✓	✓	✓	✓
BIS 4.2												✓	✓	✓	✓
BIS 4.3													✓	✓	✓
BIS 4.4														✓	✓
BIS 4.5															✓

6.2 Running the BIS installation wizard on the BIS server

Perform the following procedure to upgrade an existing BIS installation without losing the current data and configuration files. For this description of an upgrade installation it is assumed that a working BIS configuration is being upgraded, and that the network of computers involved is already up and running.

Step	Action	Effect(s), Notes, Explanations
1	Back up your BIS installation files, or create an image of the hard disk that contains the BIS installation.	
2	Close all BIS windows, and stop the BIS server.	
3	Insert the BIS installation medium into your server and perform the installation procedure as described in <i>Installing the BIS software on the BIS server, page 16</i>	Notes: For BIS update installations, and when reusing database instances, the database administrator user need no longer have the username <code>sa</code> A BIS upgrade installation automatically updates the Event Log database also. Database backups from previous BIS versions can be updated using the DB Migration button on the Event Log tab of the BIS Manager. See the BIS Configuration online help for details.
4	When you reach the BIS Select Features screen, select the new BIS features to install, then finish the installation as described in <i>Installing the BIS software on the BIS server, page 16</i>	
5	The Mandatory post installation BIS.rtf file opens. Please read and follow the directions in this file carefully, as they are particularly relevant to the new version.	
6	After completing the installation, use the License tab in the BIS Configuration Manager to initiate the licensing procedure.	See <i>Licensing your BIS installation, page 29</i>
7	Create or import an existing configuration in the BIS Manager	See BIS Manager online help for instructions (press the F1 key when in the BIS Manager).

6.3 Possible further actions

If in your upgrade you are expanding your system, such as adding new OPC servers, then further actions may be necessary, see *Performing a first-time installation, page 13* starting with *Firewall setup, page 20* and then proceed to *Configuring DCOM and OPC servers, page 21*.

7 Configuring BIS clients and optional tools

After installing the BIS application we proceed with the configuration of the client software and optional software tools.

7.1 Configuring the web browsers for the clients

The BIS client runs within an MS Internet Explorer web browser. The URL used is either that of the BIS Server, or `http://localhost` if the client is to run on the BIS server itself. To ensure trouble-free communication between the various components of the BIS system the browser's security settings need to be modified from the defaults. These changes need to be made for all browsers that run the BIS Client, regardless of user and operating system.

7.1.1 Settings for Internet Explorer (IE)

Making browser settings with a .REG file

The simplest way to change the browser settings is to use the prepared registry command file. Proceed as follows after installing the BIS server software.

1. On the BIS server open this URL in your Internet Explorer: `http://localhost/ClientDeploy/tools.aspx`
2. From the aspx page download the following file:
`IE_InternetSettings_Zone2_TrustedSites_BIS.zip`
3. Extract the `.reg` file from the `.zip` file
4. Using accounts with administrator privileges, execute the `.reg` file on each of the BIS client computers.
 - **Effect:** The IE settings are made globally via the Windows registry.

Making browser settings manually

It is possible, though more error-prone and therefore not recommended, to make or adjust the browser settings manually. Proceed as follows.

1. Open Internet Explorer and navigate to the **Internet Options** page for that browser version, e.g. Select **Tools** (or the cog icon) > **Internet Options**.
2. If you want the BIS operator logon screen to load automatically when the operator launches Internet Explorer, use the General tab to set the home page address to `http://<BisServerName>` (i.e. the URL address of your BIS server).
3. Select tab:**Security** > icon:**Trusted Sites** button:**Sites**
4. If present, clear any selection from the check box **Require server verification (https) for all sites in this zone**.
5. Enter `http://<BisServerName>` (replacing `<BisServerName>` with the name of your own BIS server) and click the **Add** button to add it to the list of trusted sites.
If you are configuring this client on the BIS server, add `http://localhost` also.
6. Click button:**Close**
7. Remaining under tab:**Security** > icon:**Trusted Sites**, click button:**Custom Level...**
8. From the BIS installation medium, locate and open the file
`<language folder>\Documents\BIS platform\IE-Settings.xls`
9. In **IE-Settings.xls**, open the tab pertaining to your browser version.

10. Depending on your default security level **Medium**, **High**, or **Custom**, enable or disable the controls as shown in the respective column in **IE-Settings.xls**, then click **OK**.
NOTE: If your security level is none of the above, we recommend that you start from a default level of **Medium**.
11. Restart Internet Explorer for the settings to take effect.



Notice!

The Windows setting **Update Root Certificates** causes the operating system to validate each certificate via the Microsoft Windows Update Server, generating an entry in the Event Log. To prevent this, clear the check box **Update Root Certificates** in the following dialog:

Start > Control Panel > Add or Remove Programs > Add/Remove Windows Components

7.2

Firewall setup

To configure a firewall on the clients, proceed as described for the BIS server in *Firewall setup*, page 20

7.3

Installing optional BIS tools

BIS provides optional tools for the following tasks:

- Limiting the network bandwidth used by BIS
- Checking detailed information about a BIS client PC
- Creating and modifying SQL Server reports for the BIS Event Log
- Running applications designed to target the .NET Framework 2.0, 3.5, 4.0 and 4.6.1

Use of these tools is described in the BIS Configuration online help. They can be installed on the BIS server and/or on the BIS clients from an active server page on the BIS Server. The installation procedure is as follows:

1. Start Internet Explorer
2. Enter the following URL: **http://<BisServerName>/ClientDeploy/Tools.aspx** (Substitute your own BIS server name). **Note:** if Internet Explorer no longer shows an address field, the same effect can be achieved by clicking **Start > Run** and entering **ieexplore http://<BisServerName>/ClientDeploy/Tools.aspx**
3. The download page appears. Click the **Download** button for the desired tool.
4. A confirmation dialog appears, click **Run**.
5. The effect depends on the tool chosen:
 - The NetLimiter program installs and requires a reboot.
 - The Client Information tool starts immediately
 - The Report Builder can be installed directly after pressing **Download...**
 - The .NET Framework (2.0, 3.5 or 4.0) runtime can be installed directly after pressing **Download...**

Note that this applies only to Windows 7 and 2008 Server R2 systems. On Windows 8.1 and Server 2012 systems Microsoft installation media will be required.

ChangePassword tool

As of BIS 4.6 a new tool has been added to maintain the passwords of BIS system users, that is both Windows operating system (OS) and SQL users.

Consult the BIS Configuration help for details.

7.4 Installing third-party software alongside BIS

Background

As a business-critical security system BIS should always be run on dedicated computers. The addition of third-party software, if unavoidable, requires careful consideration and planning.



Notice!

Bosch urgently recommends you install the third-party software first on an offline test system before installing on a live production system.

Procedure

Always perform the following steps and keep careful record of them in case technical support is later required.

1. Before installing third party software on the live system:
 - Verify that constraints and requirements of the third-party software do not conflict with those of BIS
 - Create a restore point
 - Create a backup of the BIS system
2. After installing third party software on the live system
 - Verify that BIS is fully operational.

8 Licensing your BIS installation

Licenses for BIS 4.0 and above are ordered online and delivered electronically. Proceed as follows:

1. Order the licenses you require from your local Bosch order desk or sales organization. You will receive an email from them containing your authorization number.



Notice!

Emergency licensing

Licenses are strictly hardware-bound. If due to some emergency you need to change your server hardware, please call your local Bosch partner or service representative. Bosch may then either port your licenses to the new hardware IDs, or provide time-limited emergency licenses.

2. Start the BIS Manager
3. On the **License** tab, click the **Start License Manager** button.
 - **Effect:** The License Manager dialog box is displayed.
4. Select the check boxes for the software package, the features, and the expansions that you have ordered. For the expansions, enter also the number of units required.
5. Click the **Activate...** button.
 - **Effect:** The **License Activation** dialog box is displayed containing your computer signature.
6. Write down the computer signature or copy and paste it into a text file.
7. On a computer with Internet access, enter the following URL into your browser:
<https://activation.boschsecurity.com>
If you do not have an account to access the Bosch License Activation Center, either create a new account and log on (recommended), or click the link to activate a new license without logging on. Note that for SMA (software maintenance agreement) licenses an account is always required. An account has the further advantage of keeping track of all your activations for future reference.

Follow the instructions on the website to obtain the License Activation Key.

8. Return to the software. In the **License Activation** dialog box, type or paste in the License Activation Key obtained from the Bosch License Activation Center and click the **Activate** button.
 - **Effect:** The software packages are activated for the computer.
9. Click the **Refresh** button to view the modified set of activated licenses



Notice!

Effects of hardware and software changes

Changes to the hardware of the BIS login server may invalidate your license and cause BIS to stop functioning. Please check with technical support before making changes to the BIS login server.

9 Maintenance and Deinstallation

This chapter describes the main tasks you need to perform to keep a BIS installation in working order, or to deinstall the software cleanly.

9.1 Maintenance

BIS systems are often business-critical both in the data they contain and in their functionality. Bosch therefore strongly recommends that you use a RAID array or SAN (Storage Area Network) and that this be properly maintained. Be sure to monitor the system disks regularly for read/write errors, lack of space and fragmentation.

The BIS Error log (**BIS Manager** > tab:**Error log**) provides valuable information on problems encountered by the system.

Bosch provides technical support through the usual channels, as arranged through your dealer. If you need to provide detailed information about your configuration then in the **BIS Manager** click tab: **Error log** > button:**Start Configuration Collector**. The Configuration Collector tool is part of every BIS installation and has its own online help.

9.2 Backing up and restoring configurations

Your operative BIS configurations should be backed up regularly, and whenever important changes have been made. This can be done in two ways:

- manually in the BIS Manager: make sure the system is **running**, then click tab: **Backup / Restore configuration** > button: **Backup**
- automatically as a scheduled job in BIS itself. See the BIS Configuration online help for instructions.

The default directory for configuration backups is **<installation_drive>:\Backup**

To restore a configuration backup, first make sure that the BIS application is **stopped**, then use the same tab **Backup /Restore configuration** > button: **Restore** in the BIS Manager. If you restore a configuration from an older version of BIS, then any necessary conversions are carried out automatically when the new BIS version loads the old configuration.

9.3 Deinstallation

Deinstallation may be necessary, for example, when upgrading from one BIS version to another, if the upgrade path is not supported, see *Prerequisites and assumptions, page 22*



Notice!

The BIS installation wizard does not remove third party products, such as Microsoft SQL Server, as they may be required by other applications on your computer. If you subsequently re-install BIS without deinstalling Microsoft SQL Server manually, then the wizard will install BIS upon the existing databases.

1. First stop the BIS Server in the BIS manager tab:**System Start/stop** > Button:**Stop Server component**
2. Deinstall the BIS Software via standard Microsoft Windows software administration, e.g. under Windows 7 click **Start** > **Control Panel** > **Programs and Features** . The computer lists all installed software packages. From this list select **BIS - Building Integration System**, click the **Remove** button and follow the directions given by the configuration program
3. In the same way, remove any packages whose names start with “BIS”.
4. Reboot the computer after deinstallation



Bosch Security Systems B.V.

Torenallee 49
5617 BA Eindhoven
Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2019