

Building Integration System V5.0

Table of contents

1	Legal	5
1.1	Software License Agreement	5
1.1.1	Limited Warranty	5
1.1.2	Remedy	5
2	System Overview	6
2.1	About this manual	6
2.2	Intended audience	6
2.3	BIS single server systems	6
2.4	BIS multi-server systems	7
3	Planning information	10
3.1	System requirements for the BIS server	10
3.2	System requirements for BIS clients	12
3.3	Hardware for special server functions	12
3.4	An overview of the installation process	13
4	Performing a first-time installation	14
4.1	Setting up the network	14
4.1.1	Connecting server computers to the network	14
4.1.2	Installing prerequisite software Internet Information Services (IIS)	15
4.2	Preparing the database server	16
4.2.1	Procedures to set up database server topologies	18
4.2.2	Installing and publishing SQL server databases	20
4.2.3	Installing and configuring the SQL Server Reporting service	22
4.2.4	Preparing the remote database server for access from BIS	23
4.2.5	Securing the Reporting service on a remote database server	24
4.3	Installing the BIS software on the BIS login server	25
4.4	Firewall setup	30
4.5	Engine-specific post-installation information	30
5	Configuring DCOM and OPC servers	31
5.1	Technical background and introduction	31
6	Performing an upgrade installation	32
6.1	Prerequisites	32
6.2	Running the BIS installation wizard on the BIS server	33
6.3	Possible further actions	34
7	Updating to CA-signed certificates, with or without FQDN	35
7.1	Using the Bosch certificate tool	35
7.2	Trusted sites settings	37
8	Configuring BIS clients and tools	38
8.1	Configuring the web browsers for the Classic clients	38
8.2	Configuring the web browsers for the Smart clients	38
8.3	Importing a self-signed certificate from the BIS reporting service	39
8.4	Using strong passwords	40
8.5	Firewall setup	41
8.6	Installing optional BIS tools	41
8.7	Installing third-party software alongside BIS	41
9	Licensing your BIS installation	43
10	Maintenance and Deinstallation	44
10.1	Maintenance	44
10.2	Backing up and restoring configurations	44

10.3	Deinstallation	44
-------------	----------------	-----------

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.pdf

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

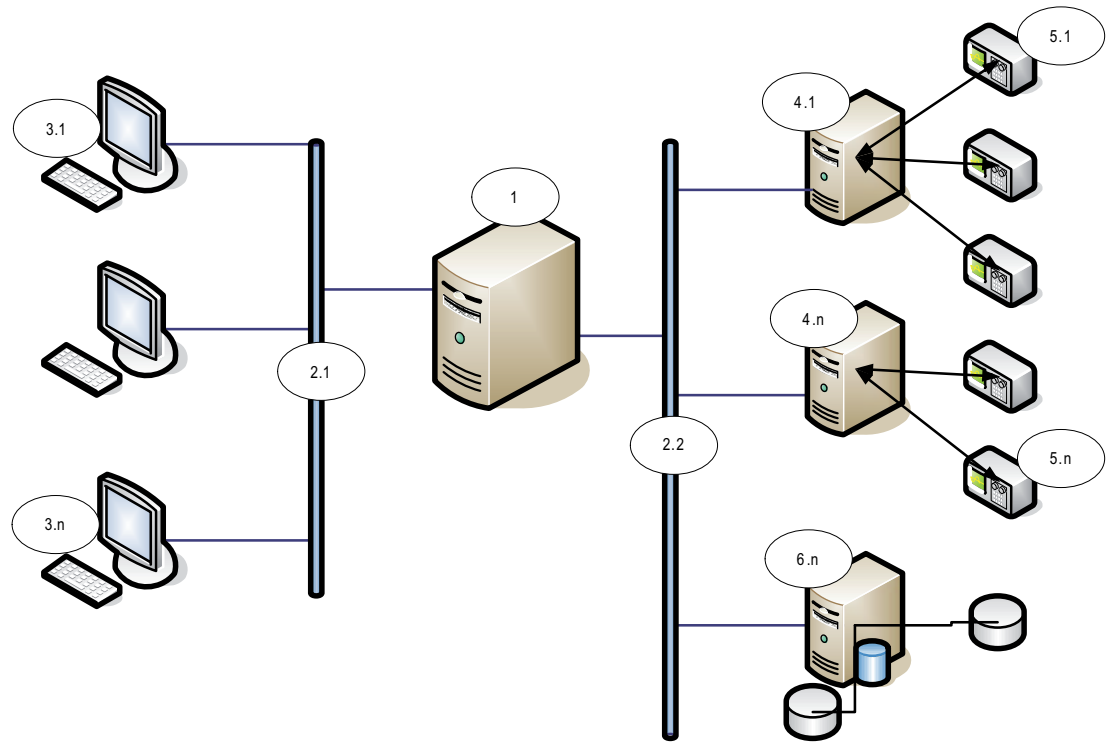


Figure 2.2: A complex single server BIS system

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.

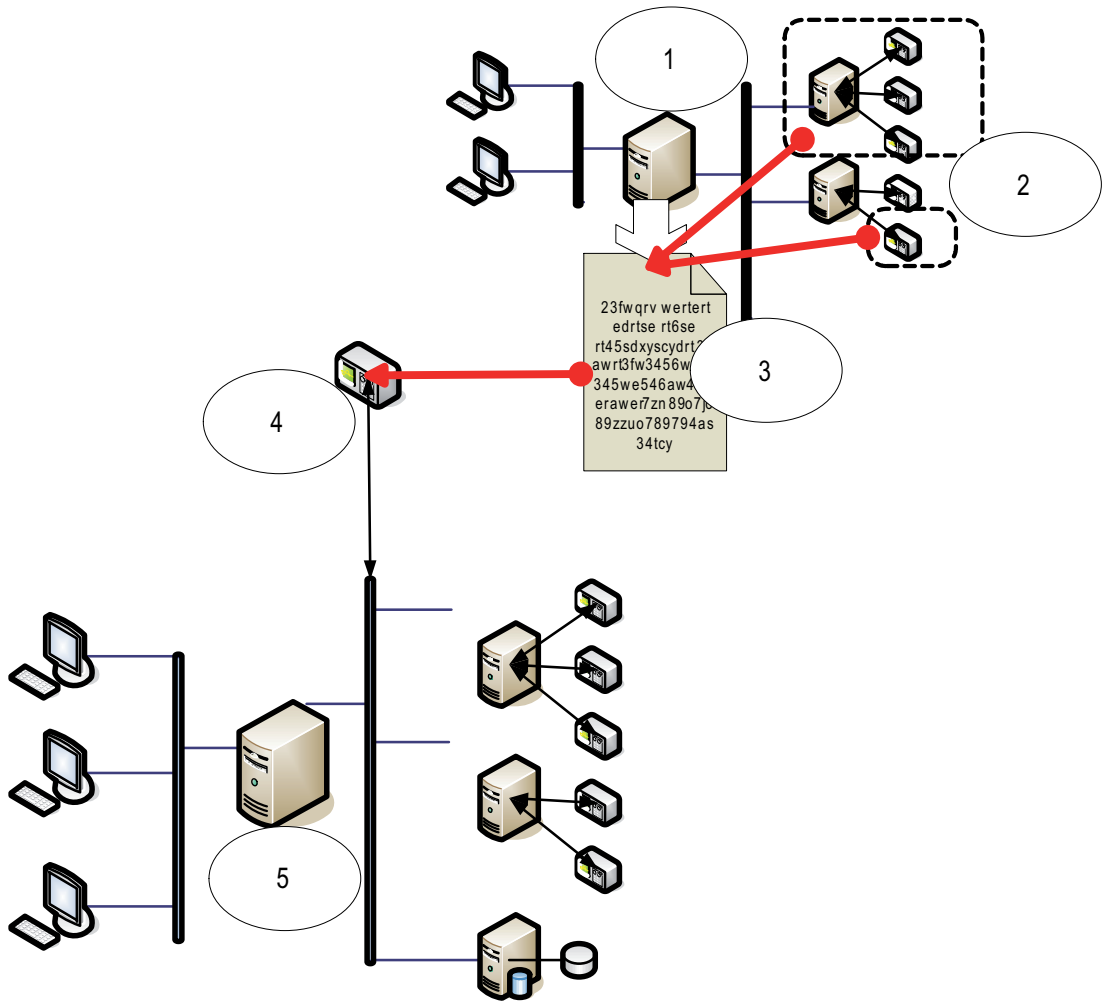
- The Provider server creates a configuration file that details exactly which information it should share with others.

- 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 Server 2019 (64 bit, Standard, Datacenter) – Windows Server 2022 (64 bit, Standard, Datacenter) – (Workgroup only) Windows 10 Enterprise LTSC (64-bit) – Note: The default database delivered with this BIS Version is SQL Server 2019 Express edition with advanced services
Other Software	<p>Always install the latest drivers and OS updates.</p> <ul style="list-style-type: none"> – IIS 10.0 for Windows 10, Windows Server 2019 and Windows Server 2022 <p>Note: IIS is not necessary on BIS connection servers</p> <ul style="list-style-type: none"> – Internet Explorer 11 in compatibility mode, or Edge in IE-compatibility mode – Chrome, Firefox, Edge for Smart Client – .NET: <ul style="list-style-type: none"> – On Windows 10, Windows Server 2019 and Windows Server 2022: .NET 3.5.1, .NET 4.8, .NET 5.0 and Core 3.1.7
Minimum hardware requirements	<ul style="list-style-type: none"> – Intel i7 processor generation 8 – 16 GB RAM (32 GB recommended) – 250 GB of free hard disk space – 300 MB/s hard disk transfer rate – 10 ms or less average hard disk response time – Graphics adapter with <ul style="list-style-type: none"> – 256 MB RAM, – a resolution of 1920x1080 – at least 32 k colors – OpenGL® 2.1 and DirectX® 11 – WebGL2-compatible (for example, Intel UHD Graphics 600 class or comparable), non-virtualized – 1 Gbit/s Ethernet card – A free USB port or network share for installation files

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 local Windows unrestricted administrator rights and password
- Set a password for the `MgtS-Service` user in accordance with your password policy.
- Antivirus software should be used, but must not be running during BIS installation.

**Notice!**

Dedicated servers are recommended

To guarantee the highest levels of operability, availability and performance at all times, install each server system (access management, video management, intrusion detection or third party) on its own dedicated computer.

**Notice!**

HTTPS port 433 and Windows Admin Center

BIS installation needs HTTPS port 443 and tries to assign a certificate to this port. If there is still a certificate assigned and port is blocked by a different application, BIS setup will fail.

This will always happen if Windows Admin Center is or was installed on the computer.

Removing the Windows Admin Center will not free up the port. Please do not install BIS if Windows Admin Center is or was installed on the computer.

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 Server 2019 (64 bit, Standard, Datacenter) – Windows Server 2022 (64 bit, Standard, Datacenter) – Windows 10 (32 or 64 bit, Pro or Enterprise LTSC) <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 11 in compatibility mode, or Edge (Note: The SEE client requires IE 9.0) – Chrome, Firefox, Edge for Smart Client – .NET: <ul style="list-style-type: none"> – On Windows 10, Windows Server 2019 and Windows Server 2022: .NET 3.5.1, .NET 4.8, .NET 5.0 and Core 3.1.7
Minimum hardware requirements	<ul style="list-style-type: none"> – Intel i5 (Gen 6 / Skylake or newer) or higher, multiple cores – 8 GB RAM (16 GB recommended) – 25 GB free hard disk space – Graphics adapter with <ul style="list-style-type: none"> – 256 MB RAM – a resolution of 1920x1080 – at least 32 k colors – OpenGL® 2.1 and DirectX® 11 – WebGL2-compatible (for example, Intel UHD Graphics 600 class or comparable), non-virtualized – 100 Mbit/s Ethernet card
Additional minimum requirements for VIE (Video Engine) clients	<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).

Server Function	Required Hardware
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.
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. First time installation. Section *Performing a first-time installation, page 14*
2. Setting up the network. Section *Setting up the network, page 14*
3. Setting up the database server. Section *Preparing the database server, page 16*
4. Installing the BIS software on the BIS server. Section *Installing the BIS software on the BIS login server, page 25*
5. Installing/configuring the Firewall. Section *Firewall setup, page 30*
6. Configuring DCOM and OPC servers on the connection server(s). Section *Configuring DCOM and OPC servers, page 31*
7. Performing an upgrade. Section *Performing an upgrade installation, page 32*
8. Configuring the web browsers on the clients. Section *Configuring BIS clients and tools, page 38*
9. Installing optional BIS tools as required. Section *Installing optional BIS tools, page 41*
10. Licensing. Section *Licensing your BIS installation, page 43*

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. Preparing the database server
3. Installing the BIS software on the BIS server.
4. Installing/configuring a Firewall
5. Making any engine-specific adjustments to the installation.

NOTE: Before starting installation, check that the network is connected and DNS is working on IPv4 and IPv6 if enabled.

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 31*

4.1 Setting up the network

BIS typically runs in a TCP/IP network consisting of

- A **BIS login server**. The server that runs the main BIS application software is also commonly referred to as the **login server** or **BIS 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 and video cameras.
- 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.

Note that the BIS server can assume the functions of connection server and operator workstation as well as hosting its own databases, but this simple topology is not suitable for large systems, as it restricts performance.

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 remote servers

Network connections to any **database servers** (see *Preparing the database server, page 16*) 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 31* in this document).

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



Notice!

For the purposes of installation, disable any energy-saving “System standby” or “Hibernation” options on all computers that are part of the BIS System (BIS Login Server, Database servers, Connection Servers, BIS Clients). Also disable automatic update options on all computers during installation.

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 10, and Windows 2019 or 2022 Server respectively.

Windows 10		Windows 2019 Server and Windows 2022 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 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 - ISAPI Extensions - ISAPI Filters - WebSocket Protocol 		<p>..Application Development:</p> <ul style="list-style-type: none"> - ISAPI Extensions - ISAPI Filters - WebSocket Protocol
<p>..Common HTTP Features:</p>		<p>..Health and Diagnostics:</p>

Windows 10		Windows 2019 Server and Windows 2022 Server
<ul style="list-style-type: none"> - Default Document - Directory Browsing - HTTP Errors - Static Content 		<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 10		Windows 2019 Server and Windows 2022 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, disable the feature as follows for Windows 10:

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

4.2

Preparing the database server

Introduction

The BIS system requires a Microsoft SQL Server database and the Reporting service.

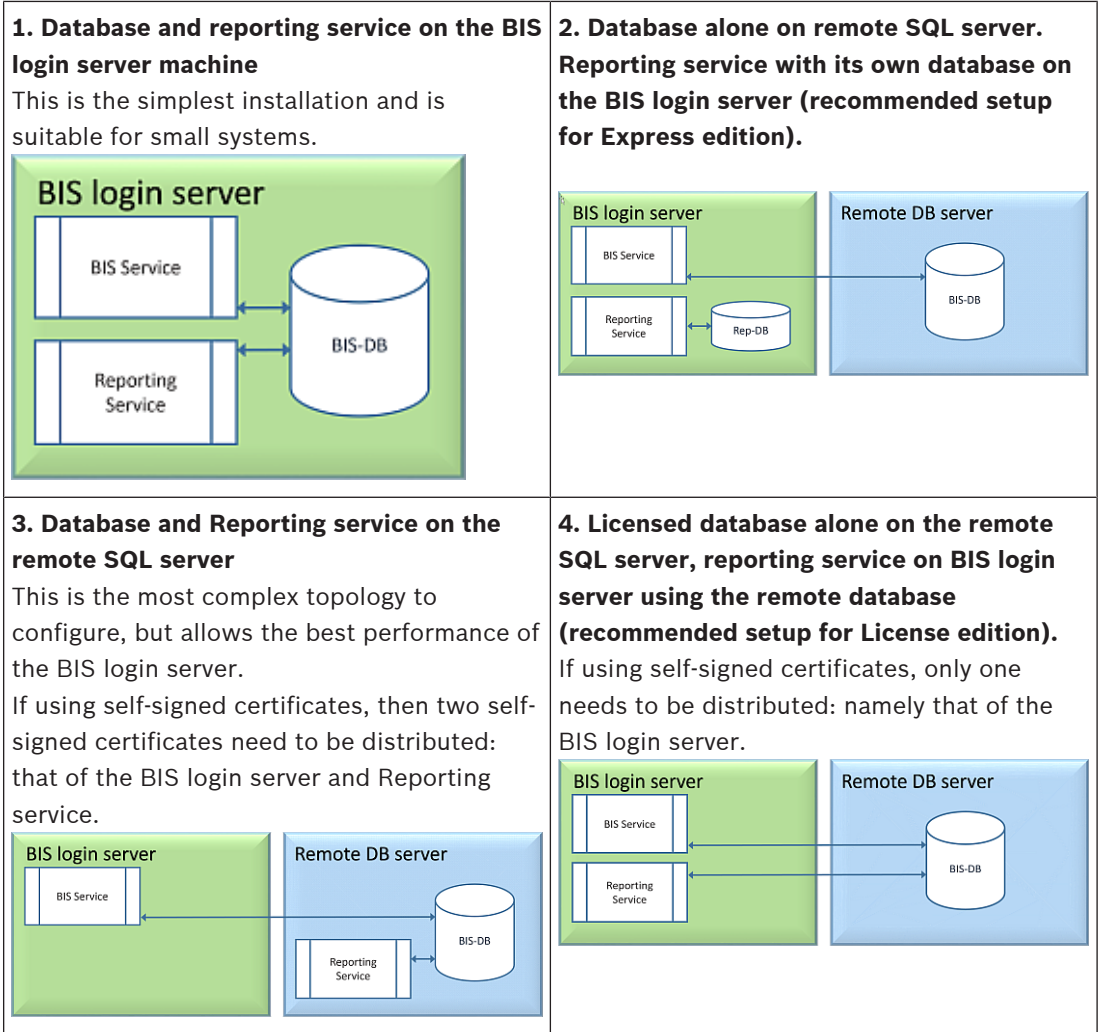
- You can install the **SQL Server database** on either the BIS login server or a separate computer. This separate computer is called a remote database server.

- You can install the **Reporting service** on either the BIS login server or the remote database server.

Overview of database server topologies

Because each of these 2 components can be installed remotely or locally (on the BIS login server), there are 2 x 2=4 possible database server topologies.

In order to proceed, select one of the 4 database server topologies.



Notice!

SQL Server compatibility issues

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 versions below 4.3 with SQL Server versions above SQL Server 2012.

BIS Supported SQL servers

Windows 2019 Server will support the following SQL Server versions:

2014 SP1

2016 SP2

2017

2019

Windows 2022 Server will support the following SQL Server versions:

2017

2019

Windows 10 Enterprise (LTSC) will support the following SQL Server versions:

2016

2017

2019



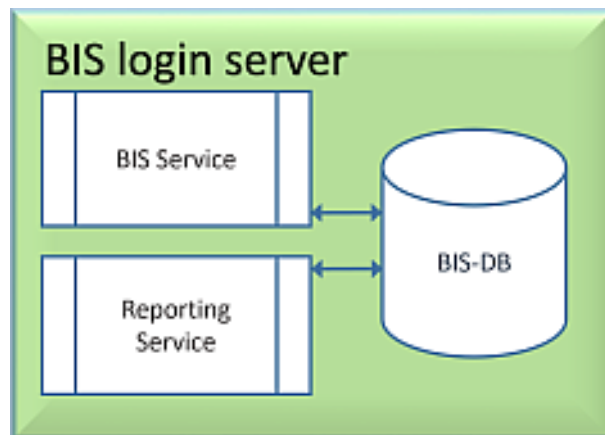
Notice!

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

4.2.1

Procedures to set up database server topologies

Topology 1: Database and reporting service running on the BIS login server machine



If you wish to use the free Express Edition of the SQL Server, as provided by BIS, then no extra preparation is required. The BIS installation will create the required SQL server instances. You may proceed to *Installing the BIS software on the BIS login server, page 25*

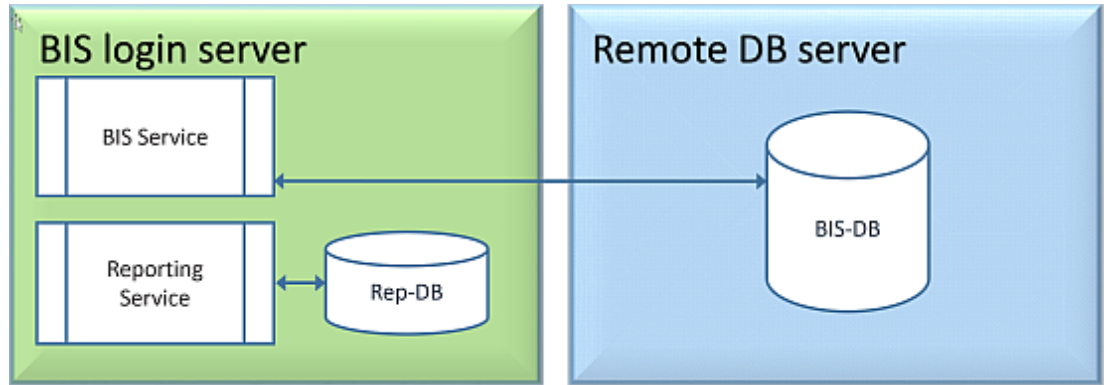
If the wish to use a licensed version of SQL Server for greater capacity, then perform the following procedures, before installing the BIS software:

Procedure 1: *Installing and publishing SQL server databases, page 20*

Procedure 2: *Installing and configuring the SQL Server Reporting service, page 22*

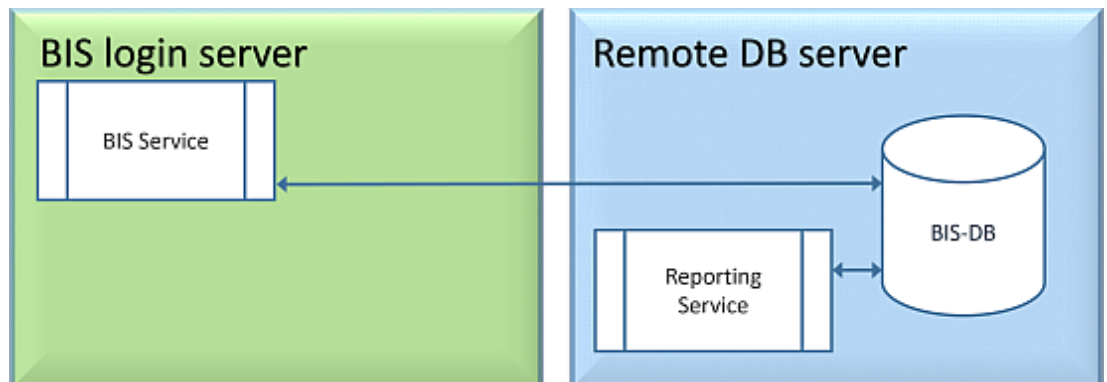
Conclude with: *Installing the BIS software on the BIS login server, page 25*

Topology 2: Database alone on remote SQL server. Reporting service with its own database on the BIS login server (recommended setup for Express edition).



On the remote SQL server machine, you can use either a licensed SQL server or the Express Edition. If you use a licensed SQL server, it is recommended to use Topology 4. Perform the following procedures, before installing the BIS software:
 Procedure 1: *Installing and publishing SQL server databases, page 20*
 Procedure 2: *Preparing the remote database server for access from BIS, page 23*
 Conclude with: *Installing the BIS software on the BIS login server, page 25*

Topology 3: Database and Reporting service on the remote SQL server



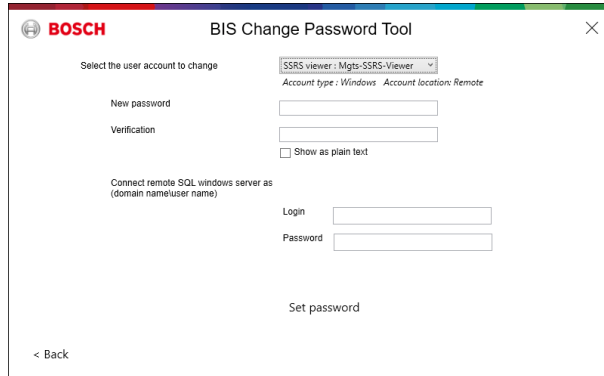
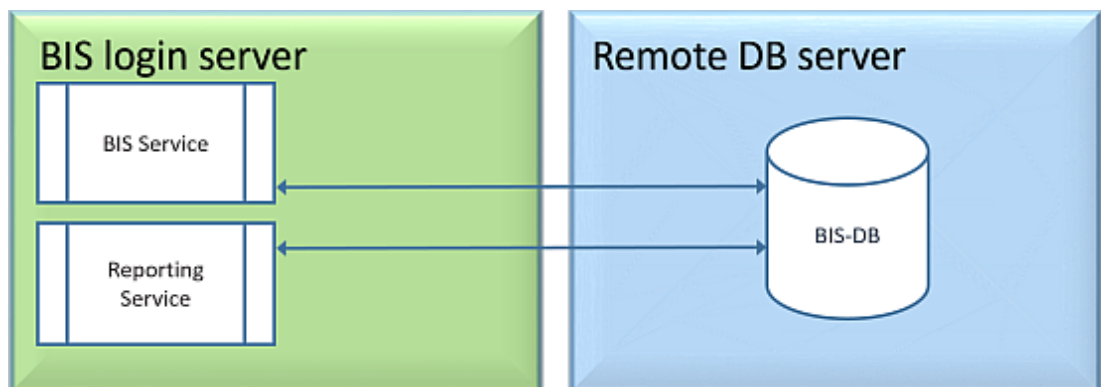
On the remote SQL server machine, you can use either a licensed SQL server or the Express Edition.

IMPORTANT: Make sure that the installer administrator user account in BIS Login Server has admin rights to access the remote database server. This is required for BIS installation to deploy the reports in the remote SQL Server Reporting instance.

Perform the following procedures, before installing the BIS software:
 Procedure 1: *Installing and publishing SQL server databases, page 20*
 Procedure 2: *Installing and configuring the SQL Server Reporting service, page 22*
 Procedure 3: *Preparing the remote database server for access from BIS, page 23*
 Procedure 4: *Securing the Reporting service on a remote database server, page 24*
 Conclude with: *Installing the BIS software on the BIS login server, page 25*

Important note for Topology 3 only:

After BIS successfully installing on the BIS login server machine, you must run the BIS Change Password Tool (C:\MgtS\Tools\ChangePassword) as Administrator to change the **MgtS-SSRS-Viewer** password. You do not require the old password if you run the tool as Administrator.

**Topology 4: Database alone on the remote SQL server, reporting service on BIS login server using the remote database (recommended setup for Licensed edition).**

- On the remote database server you must use a licensed version of SQL server.
- On BIS login server machine, use a licensed version of Reporting service

Perform the following procedures, before installing the BIS software:

Procedure 1: *Installing and publishing SQL server databases, page 20*

Procedure 2: *Preparing the remote database server for access from BIS, page 23*

Procedure 3: **On the BIS login server:** *Installing and configuring the SQL Server Reporting service, page 22*

Conclude with: *Installing the BIS software on the BIS login server, page 25*

4.2.2**Installing and publishing SQL server databases**

On the machine where the SQL Server is to run, perform the following procedures:

**Notice!**

Always use the latest releases and service packs for your SQL Server version.

1. Ensure that the hostname is no longer than 15 characters (as per Microsoft NETBIOS rules)
2. Ensure that the user **Administrator** has a password.
3. Reboot database server computer and log in as **Administrator**.
4. Disable any automatic power-saving standby option.
5. Disable the firewall. The firewall must remain disabled throughout the installation. Reactivate it after completing the installation, as described in the document `BIS_Firewall_Configuration.pdf`



Notice!

Instance name

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

Installing SQL Server on the database server computer

Decide whether you wish to use the Express Edition of SQL 2019 (delivered on the BIS installation media <BIS Installation media>\3rd_Party\SQL20xx\1033\) or your own licensed version. Execute the corresponding `setup.exe` with the following options:

Option 1: Execute in command line with parameters

From the `setup.exe` location, execute the following command, substituting the <instance names> and <strong password> parameters:

```
DOS> Setup.exe /QS /ACTION=Install /FEATURES=SQL,FullText
/InstanceID="<instance name>" /InstanceName="<instance name>"
/IACCEPTSQLSERVERLICENSETERMS /SECURITYMODE=SQL /SAPWD=<strong password>
/TCPENABLED=1 /SQLSYSADMINACCOUNTS="Administrators"
```

For example, if

- *<instance name>* = BIS
- *<strong password>* = !Admin3t!Admin3t

the command would be:

```
Setup.exe /QS /ACTION=Install /FEATURES=SQL,FullText /InstanceID="BIS"
/InstanceName="BIS" /IACCEPTSQLSERVERLICENSETERMS /SECURITYMODE=SQL
/SAPWD=!Admin3t!Admin3t /TCPENABLED=1
/SQLSYSADMINACCOUNTS="Administrators"
```

Option 2: Execute without parameters

1. Click **OK** when prompted to change the core role to newer framework and installer. Wait until the **Installation Center** appears
2. Select the **"Installation"** tab on the left menu bar
3. Click **"New SQL Server stand-alone Installation or add features to an existing installation"**
4. Click **Next** will check for the installation files and setup will install its support files automatically
5. Select **"Perform a new installation of SQL Server 2019"**
6. Accept the license terms and click **Next**
7. Select the "Database Engine Services" under **Instance Features**

8. Provide the named instance (Example: BIS) and do **not** proceed with default instance name "SQLExpress".
9. Click **Next** to continue
10. Change the "**Startup Type**" to `Automatic` for "**SQL Server Database Engine**" and "**SQL Server Browser**"
11. Select `Mixed Mode` for "**Authentication Mode**" and provide a strong password for the "**sa**" user in accordance with your password policy.
 - Make careful note of the **sa** password, as it will be required for the installation of BIS.
12. Under **Specify SQL Server administrators**: add at least one Windows user, or preferably a user group, that will be authorized to manage the SQL Server, e.g. Administrator or Administrators
13. Click **Next** to start the installation
 - When installation has completed, make sure "**Install successful**" message is displayed

Publishing the SQL instance, to make it visible on the network during the installation of BIS software.

1. Click **Start > Microsoft SQL Server 2019 > SQL server 2019 configuration manager**
2. Expand, "**SQL Server Network Configuration**" and select Protocols for <INSTANCE>, enable "**Named Pipes**" and "**TCP/IP**" <INSTANCE> is provided during SQL setup, example: BIS/BISACE
3. Enable "**Named Pipes**" and "**TCP/IP**" for the SQL Native Client, client protocols.
4. Right click "**Protocols for <INSTANCE>**", select "**Properties**" and select "**Flags**" tab. Under it set "**Force Encryption**" to "**Yes**" to enable encrypted communication between BIS server and SQL server.
5. Under **SQL Server services > SQL Server Browser > Properties > Service** make sure "**Start Mode**" of the service "**SQL Server Browser**" is `automatic`.
6. Reboot the computer.

Installing a second instance for ACE

- If Access engine is to be installed with BIS, then create an additional SQL instance. Repeat the procedures in this chapter to install the additional SQL instance, providing a name like `ACE` or `BIS_ACE`.

4.2.3

Installing and configuring the SQL Server Reporting service

On the machine where the Reporting service is to run, perform the following procedures:

Installing the Reporting Service

1. Open the reporting service executable location, either express version delivered with BIS `<BIS installation media>\3rd_Party\SQL20xx\` or the location of your separately-licensed reporting service.
2. From that location, right click `SQLServerReportingServices.exe` and run as Administrator
 - The setup wizard for the **SQL Server Reporting Service** opens.
3. Enter the product license key if SQL server is installed with the licensed edition.
4. Proceed through the setup
5. After installation, restart the computer.

Completing the installation

1. The wizard displays a confirmation message.
2. Run `services.msc` and make sure `SQLServerReportingServices` is running on the installed machine. If not, start the service manually.

Configuring the Reporting Service

Note: The steps below are required only for topology 3. Refer to *Topology 3: Database and Reporting service on the remote SQL server*, page 19.

1. Open a DOS command window as Administrator
2. Change directory to:
 - `<Program Files>\Microsoft SQL Server Reporting Services\Shared Tools\`
3. From this location execute the following command, substituting for the machine and instance names:

```
DOS> RSConfig.exe -c -s [DBMachineName]\[InstanceName]
-d ReportServer${InstanceName} -a Windows -i SSRS
- DBMachineName - Is the machine where the SQL instance is created
- InstanceName - Is the name provided during the SQL instance creation
- For example:
- If the SQL is installed in the machine "SGPBISSQLSERVER" and Instance Name is "BIS",
then the command will be:
RSConfig.exe -c -s SGPBISSQLSERVER\BIS -d ReportServer$BIS -a Windows -i
SSRS
```

4.2.4

Preparing the remote database server for access from BIS

Creating a user account for backup and restore

On the remote SQL server machine, run the `BisAccessRights.exe` as administrator from the BIS installation medium under

`<Installation media>_Install\AddOns\BIS\RemoteSQL\BISRightsSetup` folder.

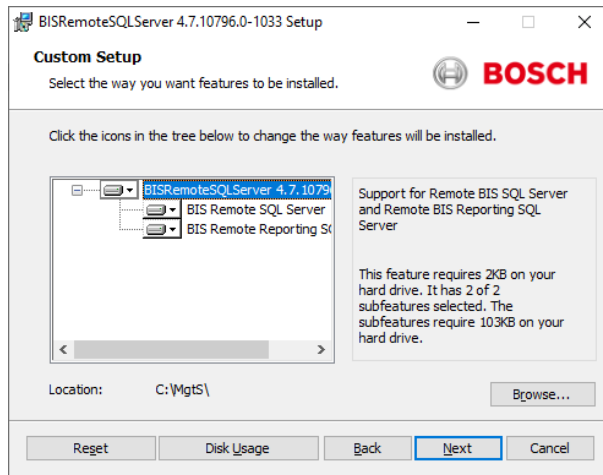
It will prompt to enter password for the **Mgts-Service** account. Set the password according to your security policies and note it carefully as it will be required for the BIS installation on the login server.

Reporting Service database setup

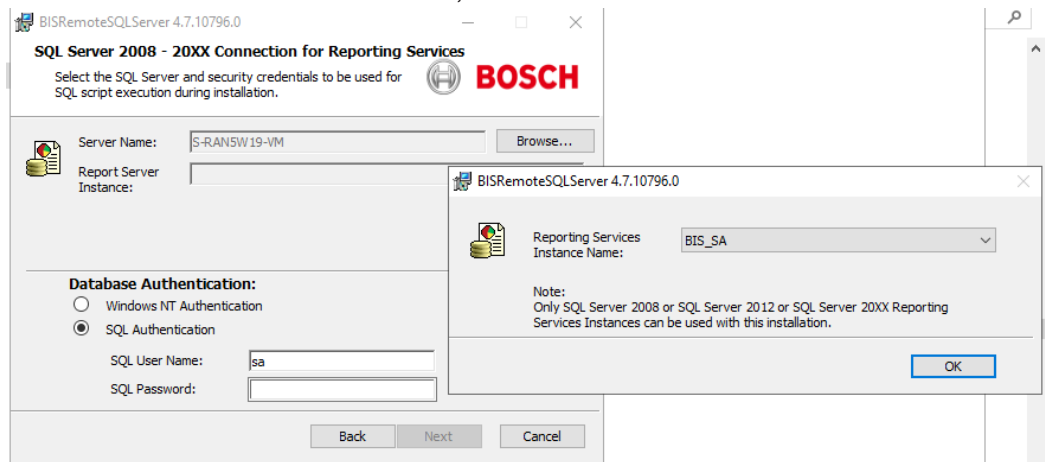
Note: The steps below are required only for topology 3. Refer to *Topology 3: Database and Reporting service on the remote SQL server*, page 19.

On the remote database server:

1. Copy the contents from location `<Installation media>\3rd_Party\SQLSMO20xx\` to `C:\Windows\SysWOW64\`
2. Right-click and run as administrator the installation file `install.exe` under `<Installation medium>:\<Language_ID>\BIS\Tools\BISRemoteSQLServerSetup\`
3. Keep both features selected and click **Next** to select reporting service instance.



4. Click the **Browse** button to select the SQL instance that is configured during Reporting Service installation. Refer to , page 23. Normally, the instance name will be **BIS**. If you have created a different instance name, select that instance name.



5. Click **OK** to return to the previous window.
6. Use SQL authentication, with username `sa` and the password you noted during installation above.
7. Click **Next** and click **Install** on next page to perform the installation
8. Upon completion of installation, reboot the remote database server computer.

4.2.5

Securing the Reporting service on a remote database server

When the Reporting service runs on a remote database server, the BIS login server and BIS clients require a certificate from the Reporting service, in order to access it securely over the network.

Both self-signed and CA-signed certificates can be used. The following procedures describes how to create and deploy:

- Self-signed certificates
- CA-signed certificates

Self-signed certificates

1. On the remote database server, execute the `BoschCertificateTool.exe` as an administrator from the <installation medium> under `_Install\AddOns\BIS\RemoteSQL\Certificate` folder. For more information, refer the readme file from the same folder location.

2. Copy and install this self-signed certificate as a trusted root certificate on the BIS Server and all Client machines.
 - For detailed instructions see *Importing a self-signed certificate from the BIS reporting service, page 39*

CA-signed certificates

If you have a CA signed certificate, it is not required to create a self-signed certificate. Instead, bind that CA-signed certificate to the Reporting service web URL.

To bind the CA signed certificate, use the same `BoschCertificateTool.exe` as an administrator from the <installation medium> under `_Install\AddOns\BIS\RemoteSQL\Certificate` folder. For more information, refer to the readme file from the same folder location.

4.3 Installing the BIS software on the BIS login server

Before you begin

Make sure that one of the following applies:

- You are installing all system components on the BIS login server, with a free MS SQL Server Express edition.
- You have configured one of the database topologies described in the previous chapter *Preparing the database server, page 16*

For the installation, use an account with local administrator permissions, preferably the **Administrator** account itself. Verify 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!

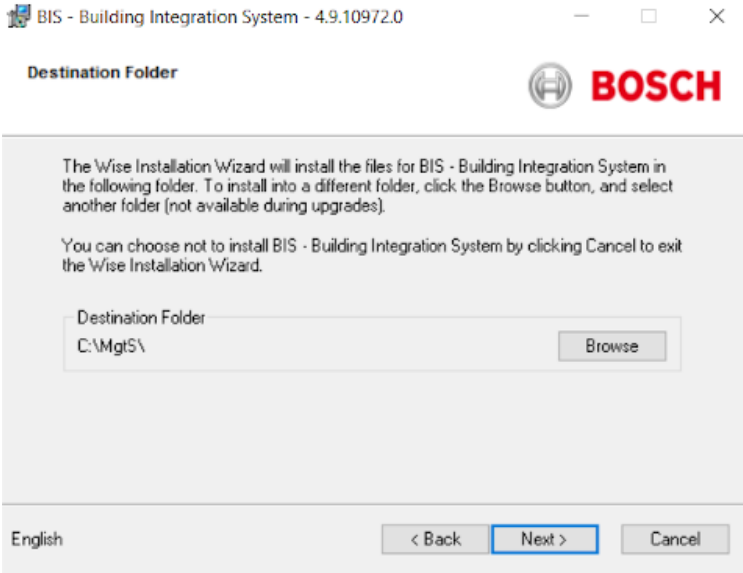
Installation to local computer only
 The BIS installation kit may be on a separate networked computer, but `setup.exe` will only install BIS to the computer which invoked it.

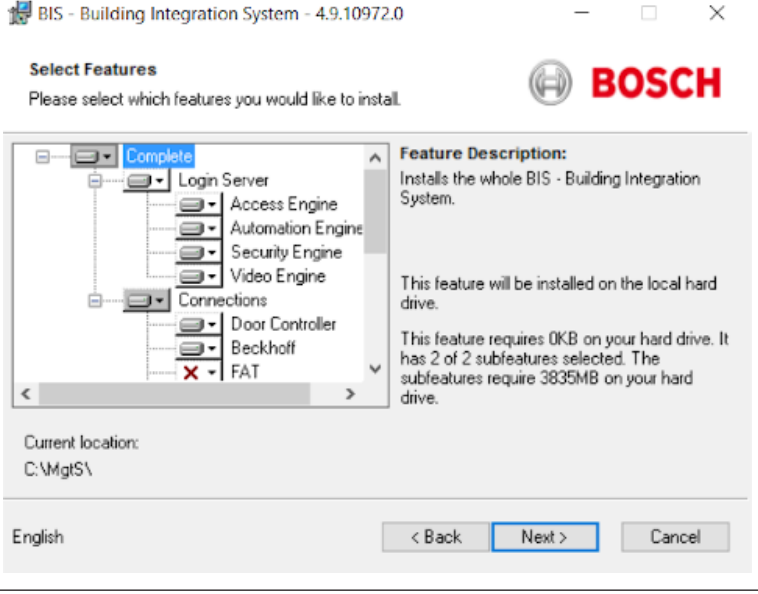
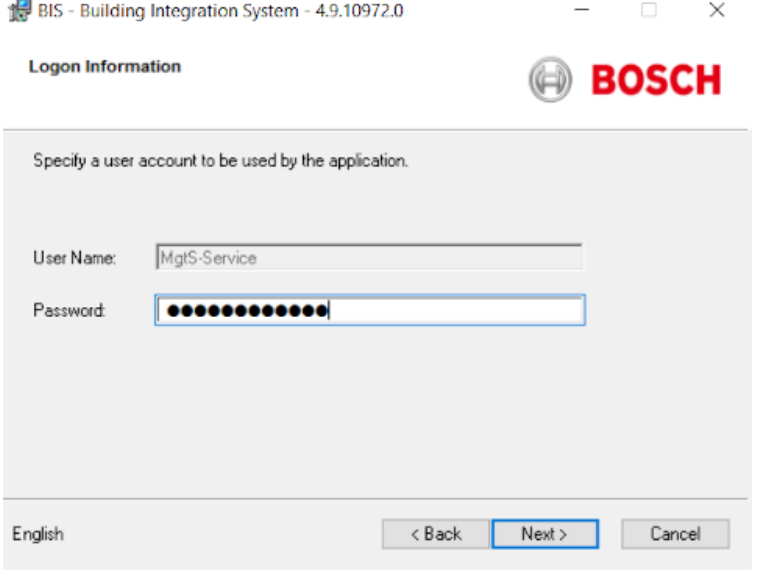


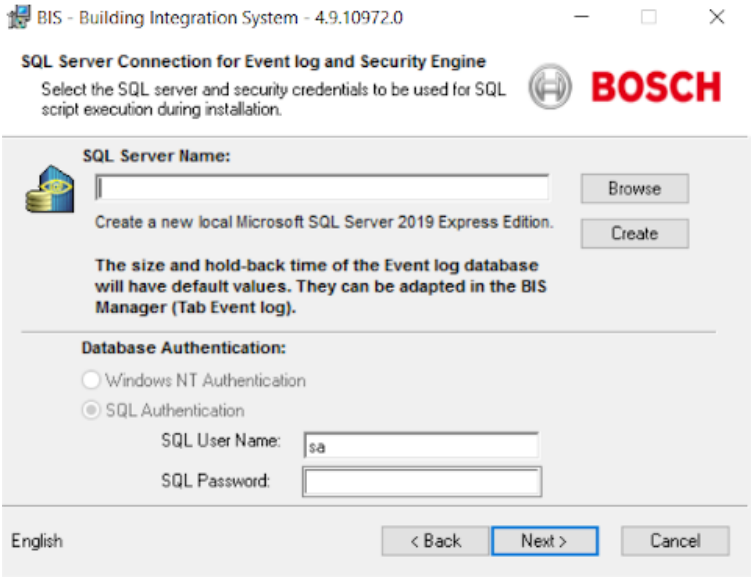
Notice!

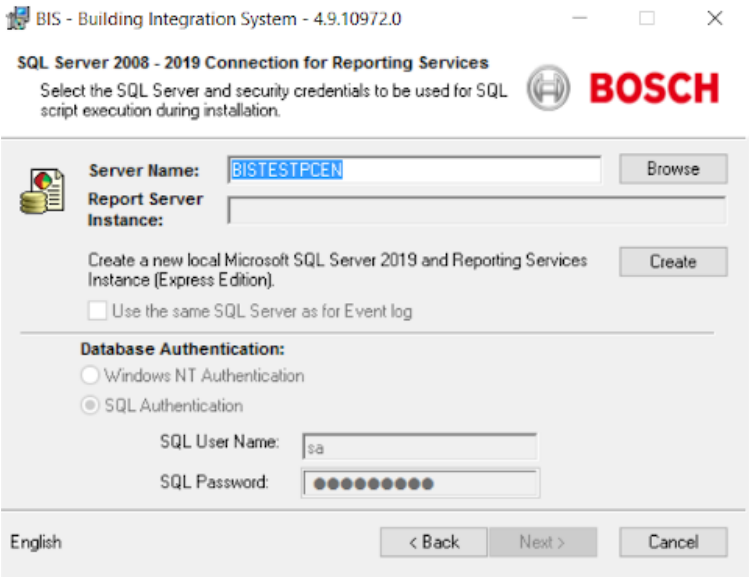
Avoid special characters
 Use no special or non-Latin characters in BIS (e.g. Chinese, Russian, ä, é, ô, /, #, %, \$, |, !, ~, ‘). Use only non-diacritic (7-bit ASCII), alphanumeric characters [A-z] [0-9] plus underscore. This applies to any characters typed into the BIS installation wizard or configuration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

Step	Action	Effect(s), Notes, Explanations
1	Right-click setup.exe and select Run as administrator .	The language selection dialog opens. Notes: <ul style="list-style-type: none"> - Apart from German and Russian all installations are currently performed in English.

Step	Action	Effect(s), Notes, Explanations
		<ul style="list-style-type: none"> - 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 OK	<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. - SQL DMO/SMO support and others
3	Click Install	<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>

Step	Action	Effect(s), Notes, Explanations
		
5	Set MgtS-Service account password	The setup will create a windows user account for the BIS services to run and to access the remote servers (if any). Key in the same password that configured in the remote server.
		
6	Click Next>	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).

Step	Action	Effect(s), Notes, Explanations
7	Configure the instances you require for Event Log/SEE and Access Engine.	 <p>IMPORTANT NOTE: When creating a new SQL instance, the "sa" user-id and password that you entered will be used to create an administrator account. So please remember the password that you entered.</p> <p>If the SQL Server instance is not pre-installed manually, you can click Create to install SQL instance (Express edition). Normally, this action is required for Topology 1 setup only. Refer to <i>Topology 1: Database and reporting service running on the BIS login server machine, page 18</i>.</p> <p>Upon clicking the Create button, a pop-up window appears suggesting the name of the instance as BIS. Confirm (recommended) or change the instance name, then click OK to return to the previous window and continue the installation.</p> <p>If the SQL Server instance is already installed manually, click the Browse button to display all the available SQL instances in the network. In case that the available SQL instance is not shown, enter the instance name in the text field for the SQL Server Name using the syntax: <computername>\<instancename>, for example MYSERVER\BIS.</p> <p>Select the instance name and click OK to return to the previous window to continue with the installation.</p> <p>Note: If Access Engine feature is selected for installation, then on clicking Next>, similar dialog will display for SQL instance creation/selection for Access Engine feature.</p>

Step	Action	Effect(s), Notes, Explanations
8	Similarly, use the BIS installation wizard to specify the Reporting Service installed server name and select the Reporting Service Instance.	
		<p>IMPORTANT NOTE: This step only occurs if you choose pre-installed SQL Server 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 installed and use the same SQL instance created for the Event Log database.</p> <p>If the Reporting service is not pre-installed manually, you can click the Create button to install the Reporting Service and separate SQL instance (Express edition) for the reporting database. Normally, this action is required for Topology-2 only. Refer to <i>Topology 2: Database alone on remote SQL server. Reporting service with its own database on the BIS login server (recommended setup for Express edition).</i>, page 19.</p> <p>Upon clicking 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.</p> <p>If the Reporting Service is already installed, make sure that the Server Name field contains the correct server name (by default, it displays the BIS Login Server name). If the Reporting Service is installed in the remote server then change the server name and click the Browse button to select the SQL instance. Click OK to return to the previous window and continue the installation.</p>
9	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.

Step	Action	Effect(s), Notes, Explanations
10	Click Finish .	The Mandatory Post Installation file opens.
11	Please read and follow the directions in this file, then close the window.	The file contains important information and instructions.
12	You must restart the PC to complete the BIS installation. Click Yes to restart the PC.	The first-time installation of the BIS application is complete. An icon for the BIS Manager has appeared on the desktop.
13	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 43</i>
14	Create an initial configuration in the BIS Manager	See BIS Configuration online help for instructions. Press the F1 key when in the BIS Manager.

4.4 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_Firewall_Configuration.pdf

4.5 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.pdf

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 10*, 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 login server, page 25*
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

The following table describes the supported upgrade paths for BIS versions, both with and without Access Engine (ACE).

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 panel about WCF customizations below.

BIS upgrade

From/To	BIS 4.5	BIS 5.0
BIS 4.2	✓+	X
BIS 4.3	✓+	X
BIS 4.4	✓+	X
BIS 4.5		✓+
BIS 4.6.*		✓+
BIS 4.7		✓+
BIS 4.8		✓+
BIS 4.9.*		✓+

Symbol	Explanation
X	Not recommended due to OS and SQL server limitations
✓	Approved upgrade destinations
+	Approved upgrade starting point If and only if you use OS and SQL server versions that are compatible with the destination version
*	Wildcard for the digits 1 or 2

Note on upgrading from BIS versions below 4.5

Due to incompatibilities in the supported operation systems and SQL Server versions, we recommend upgrading any versions older than 4.5 to 4.5 first. After that, do a backup, install the latest OS with the same server name and installation path, restore the backup and run a repair installation to update the ACE Database, if you are using ACE.



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`

Refer to

- *Deinstallation, page 44*

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	Notes:

Step	Action	Effect(s), Notes, Explanations
	procedure as described in <i>Installing the BIS software on the BIS login server, page 25</i>	After BIS installation, If needed, 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 login server, page 25</i>	
5	The Mandatory post installation BIS.pdf 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 43</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).
8	If system is upgraded from 4.9 or below.	During upgrade it will create a new self-signed cert and overwrite the existing bindings. If CA-signed certificate was used earlier then re-assign the existing CA-signed certificate, refer to <i>Updating to CA-signed certificates, with or without FQDN, page 35</i> .

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 14* starting with *Firewall setup, page 30* and then proceed to *Configuring DCOM and OPC servers, page 31*.

7 Updating to CA-signed certificates, with or without FQDN

To update a CA-signed certificate or a new self-signed certificate, with or without fully-qualified domain names (FQDN), use the Bosch certificate tool `BoschCertificateTool.exe` included in the subfolder of your installation media. Documentation for the tool can be found in the same folder.

You can use FQDN with the following applications and network setups:

	BIS	ACE	AMS	Visitor Manager	Occupancy monitor	Importer Exporter
Network setup						
Workgroup	X	X	X	X	X	X
FQDN (sd)	X(1)	X(1)	X(1)	X(1)	X(1)	X(1)
FQDN (cd)	X(1)					

- X** Supported
- X(1)** Supported if you add the alternate hostname by means of the Bosch certificate tool
- FQDN(sd)** Single domain, standard DNS
- FQDN(cd)** Cross-domain

7.1 Using the Bosch certificate tool

Execute the Bosch certificate tool on the BIS Login Server machine only. If the SQL Reporting Server is running on a separate machine, execute the tool on that machine as well.



Caution!

Take note that the Bosch certificate tool on the BIS Login Server and the Bosch certificate tool on the SQL Reporting Server are different tools. While the executables use the same name, their configuration is different. Use only the tool from their own folders as specified in the instructions.

For BIS Login Server, the tool is in the folder: `\Mgts\Certificate`

For Remote SQL Reporting Server, the tool is in the folder:

`_Install\AddOns\BIS\RemoteSQL\Certificate`

Prerequisite

Make sure that .NET 5 runtime is installed on that computer. Otherwise, install `windowsdesktop-runtime-5.0.5-win-x64.exe` delivered with the BIS installation package. The file is located in the `<BIS Installation media>\3rd_Party\dotNET\5.0` folder.

**Notice!**

The certificate tool will not assign the certificate to the SQL Server instances. By default, SQL Servers instances run with an internal self-signed certificate. If you would like to change this behavior, use the SQL Server Configuration Manager to assign a different certificate to the SQL Server.

Procedure

Follow the procedure below on the SQL Login Server. Repeat the procedure on the SQL Reporting Server using its own certificate tool if the SQL Reporting Server is running on a separate machine.

1. Navigate to the following subfolder of your installation folder.
 - For BIS Login Server: `\Mgts\Certificate`
 - For Remote SQL Reporting Server:
`_Install\AddOns\BIS\RemoteSQL\Certificate`
2. Run as Administrator `BoschCertificateTool.exe`
3. The **Delete old certificates** check box is selected by default. If the check box is not selected, select it now.
4. Select the check box **Alternative Hostnames** and enter the hostname in the text field to add the names in the certificates' Subject Alternative Name (SAN) field.
5. Select the check box **Custom root certificate** and navigate to the location of your PFX file.
6. Enter the password that you received from your Certificate Authority (CA) in the **Password** text box.
7. Click **Generate**.
 - The tool generates your certificate `CER` file.
 - If the generation fails repeatedly, contact technical support.
8. Reboot your system.
9. Proceed to install this certificate on your client machines.

Notes on the certificate tool options

- Delete old certificates
 - selected by default
 - removes child certificates from the Computer Certificate Store of the server, if they are invalid or no longer needed
 - does NOT delete root certificates from Computer Certificate Store
- Alternative Hostnames
 - adds the provided names in the certificates' Subject Alternative Name (SAN) field
 - should be set if the system is operating in a domain environment, for example, `Access_System_Name.your.domain`
- Custom root certificate
 - imports another certificate authority
 - must be a signing certificate with private key provided as PFX file
 - Note that if a custom certificate becomes expired or invalid in some way, the access system will not be fully operational until the certificate is replaced with a valid one.

For BIS Login Server, the public root certificate is exported automatically to `C:`

`\inetpub\wwwroot\ as <SERVERNAME>.CER.`

For Remote SQL Reporting Server, the public root certificate is exported automatically to `C:\MgtS\as <SERVERNAME>.CER`.

For more information, refer to the README file from the same folder location.

Refer to

– *Configuring BIS clients and tools, page 38*

7.2

Trusted sites settings

If the BIS Login Server has to be accessed using FQDN, add the HTTPS FQDN URL of the BIS Login Server as a trusted site on all clients.

For example, if your BIS Login server is running on `BISServer.Customer.com`, go to the Internet Explorer settings menu > **Internet Options** > tab:**Security** > **Trusted sites** > button:**Sites** and add the site `https://BISServer.Customer.com`.

If the SQL Reporting Server is running on a remote computer, and should be accessible only by FQDN, change the URL registry on the BIS Login Server to the FQDN URL.

For example, if your SQL Reporting Server is running on `ReportServer.Customer.com`, go to the BIS Login Server registry,

`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Security Systems\Platform` and change the `ReportingServicesURL` value from `ReportServer` to `ReportServer.Customer.com`. In this case, you must create a certificate with the FQDN as an alternative hostname.

8 Configuring BIS clients and tools

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

8.1 Configuring the web browsers for the Classic clients

The BIS Classic Client runs within an MS Internet Explorer (IE) web browser or Microsoft Edge (Chromium-based) web browser. 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 on all the BIS Classic Client computers, regardless of user and operating system.

The simplest way to change the browser settings is to proceed with the following steps.

1. Open IE or Edge browser.
2. Enter the URL `http://<Name_of_BIS_Server>/<Name_of_BIS_Server>.zip` to download the zip package. For example, if the name of your BIS server is `MYBISSERVER`, then the URL will be `http://MYBISSERVER/MYBISSERVER.zip`.
3. Unzip the package and execute `InstallBISClient.bat` with administrator privileges. This will automatically execute the following tasks and launch the BIS client application.
 - Install BIS Server certificate for HTTPS secure communication.
 - Configure browser security settings and trusted site.
 - If Edge browser is installed, it will configure Edge to run in IE mode and update the sites list.
 - Create `BISClient` shortcut on the desktop.

Note: If you upgrade or change certificates on the server, redo the steps above to update all settings.

8.2 Configuring the web browsers for the Smart clients

Introduction

The BIS Smart Client is installed by default along with the BIS installation. To access the BIS Smart Client, use non Internet Explorer web browsers like Microsoft Edge (Chromium-based), Google Chrome or Mozilla Firefox.

For Google Chrome and Mozilla Firefox, go to `https://<Name_of_BIS_Server>` and the BIS Smart Client screen automatically loads. For Microsoft Edge, go to `https://<Name_of_BIS_Server>/SC`.

Note: Certificates are created for a particular hostname, therefore attempts to log in using `https://localhost` will fail. Always use the hostname in the URL, `https://<Name_of_BIS_Server>`

If BIS Classic client configuration is not done on client machine, then BIS Server self-signed certificate has to be manually downloaded and installed.

Downloading the self-signed BIS certificate from a browser

1. On the client mobile device, open the certificate's URL in a browser. For example, if the name of your BIS server is MYBISSEVER, then the URL will be `http://MYBISSEVER/MYBISServer.CER`



Notice!

HTTPS is not yet configured at this stage, therefore you must download the certificate via HTTP.

If the BIS server webpage is already being accessed by HTTPS, then you may not be able to download the certificate. In this case, clear the browser history and reload the URL via HTTP.

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

Installing self-signed certificates on a client computer, or on the BIS login server

1. Double click the certificate's .CER file to open it.
2. On the **General** tab, click **Install Certificate**
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 installing certificate.

Installing self-signed certificates on a client mobile device

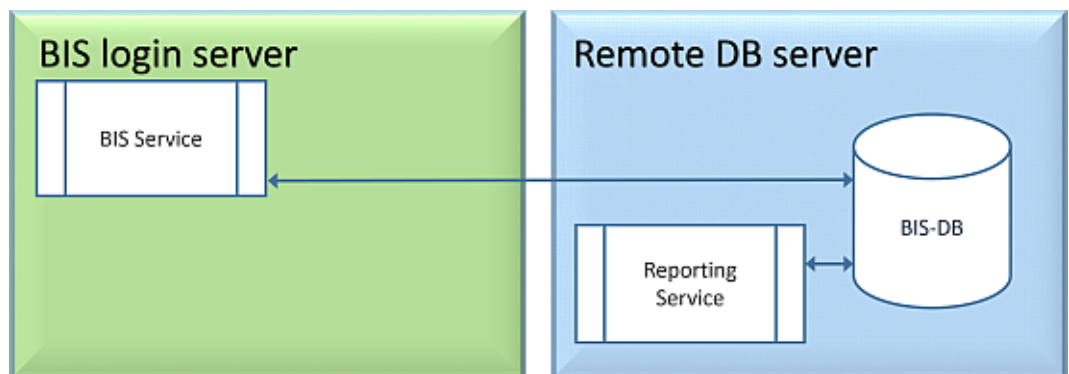
1. On the mobile device open the device settings and type `certificate` to search for the certificates installation menu.
2. Select **Install certificate from storage** (or similarly named menu item, depending on your operating system).
3. Select the imported certificate and install it. Note that some devices will install certificates automatically when you open the certificate.

8.3

Importing a self-signed certificate from the BIS reporting service

Introduction

This section applies only to server topology 3, where the BIS reporting service is running on the remote database server, and **not** on the BIS login server. In all other topologies the BIS reporting service does not need its own certificate. Refer to *Topology 3: Database and Reporting service on the remote SQL server, page 19*.



Copy and install the self-signed certificate as a trusted root certificate on the BIS Server and all client machines.

Copying the certificate

1. Copy the .CER file located at C:\Mgts folder in the remote SQL Reporting Server machine to the BIS Login server and all BIS clients.
2. Use the following procedure to install the certificate on each of these computers.

Installing self-signed certificates on a client computer, or on the BIS login server

1. Double click the certificate's .CER file to open it.
2. On the **General** tab, click **Install Certificate**
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 installing certificate.

Notice: Instead of installing BIS reporting server self-signed certificate to all client machine, you can also use the existing self-signed BIS Login Server root certificate to BIS reporting server.

1. Export the root certificate from BIS Login server.
2. Assign the certificate to BIS reporting server.

Exporting root certificate

1. On the BIS Login Server, execute the Windows certificates snap-in **Certlm.msc**.
2. In the Certlm program, navigate to Certificates Local Computer > Personal > Certificates.
3. Right-click on "*Bosch Security System Internal CA - BISAMS*" Issued To certificate and select **All Tasks > Export**.
4. Click Next and select "**Yes, export with private key**" and continue through the wizard, by taking only the default values.
5. Select **Password** check box and enter any password to secure the certificate.
6. Save the PFX file (the certificate) to a convenient location from which you can copy it easily to remote Reporting Server.
7. When you have saved the file, close Certlm.msc.

Assigning the certificate

To assign the self-signed root certificate (PFX file), use the BoschCertificateTool.exe from the <installation medium> under _Install\AddOns\BIS\RemoteSQL\Certificate folder. For more information, refer to the README file from the same folder location.

8.4 Using strong passwords

To enhance security, the system forces all users to set a strong password when they log on to a Windows client with a default password, which is the same as the username.

Follow the instructions in the **Change password** dialog to reset the password in accordance with the password policy.



Notice!

The systems rejects all logons with default password at mobile web clients until you have set a strong password in a Windows client.

8.5 Firewall setup

To configure a firewall on the clients, proceed as described for the BIS server in *Firewall setup, page 30*

8.6 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 4.8

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: `https://<Name_of_Bis_Server>/ClientDeploy/Tools.aspx` (Substitute the name of your own BIS server). **Note:** if Internet Explorer no longer shows an address field, the same effect can be achieved by clicking **Start > Run** and entering **ie** `https://<Name_of_Bis_Server>/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...**

ChangePassword tool

As of BIS 4.6 and above 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.

8.7 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.

9 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 your server may invalidate your license and cause the software to stop functioning. Please check with technical support before making changes to the server.

10 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.

10.1 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.

10.2 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.

10.3 Deinstallation

Deinstallation may be necessary, for example, when upgrading from one BIS version to another, if the upgrade path is not supported, see *Prerequisites, page 32*



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., 2023

Building solutions for a better life.

202304171650