



**BOSCH**

# Building Integration System

**de**      Installationshandbuch



# Inhaltsverzeichnis

<b>1</b>	<b>Rechtliche Hinweise</b>	<b>5</b>
1.1	Softwarelizenzvertrag	5
1.1.1	Eingeschränkte Gewährleistung	5
1.1.2	Abhilfemaßnahme	5
<b>2</b>	<b>Systemüberblick</b>	<b>7</b>
2.1	Hinweise zu diesem Handbuch	7
2.2	Zielgruppe	7
2.3	BIS Einzel-Server-Systeme	7
2.4	BIS Multi-Server-Systeme	8
<b>3</b>	<b>Informationen zur Planung</b>	<b>11</b>
3.1	Systemvoraussetzungen für den BIS-Server	11
3.2	Systemvoraussetzungen für BIS-Clients	12
3.3	Hardware für zusätzliche Serverfunktionen	13
3.4	Übersicht des Installationsvorgangs	14
<b>4</b>	<b>Durchführen der Erstinstallation</b>	<b>15</b>
4.1	Einrichten des Netzwerks	15
4.1.1	Verbinden der Serverrechner mit dem Netzwerk	15
4.1.2	Installieren der erforderlichen Software für Internetinformationsdienste (IIS)	16
4.2	Vorbereiten des Datenbankservers	18
4.2.1	Verfahren zum Einrichten von Datenbankserver-Topologien	19
4.2.2	Installieren und Veröffentlichen von SQL Server-Datenbanken auf Datenbankservern	22
4.2.3	Installieren und Konfigurieren des SQL Server Reporting Service	24
4.2.4	Vorbereiten des Remote-Datenbankservers auf den Zugriff von BIS	25
4.2.5	Sichern des Reporting Service auf einem Remote-Datenbankserver	27
4.2.6	Letzte Schritte vor dem Starten der Installation auf dem Einwahlserver:	27
4.3	Installieren der BIS Software auf dem BIS-Einwahlserver	28
4.4	Einrichten der Firewall	33
4.5	Engine-spezifische Informationen nach Installationsabschluss	33
<b>5</b>	<b>Konfigurieren von DCOM und OPC-Servern</b>	<b>34</b>
5.1	Technische Hintergrundinformationen und Einführung	34
<b>6</b>	<b>Durchführen einer Upgrade-Installation</b>	<b>35</b>
6.1	Voraussetzungen	35
6.2	Starten des BIS Installation Wizard auf dem BIS-Server	37
6.3	Aktualisieren von durch Zertifizierungsstellen signierte Zertifikate	39
6.3.1	Aktualisieren der IIS-SSL-Bindung	39
6.3.2	Aktualisieren der Reporting Service-Bindung	39
6.3.3	Aktualisieren des Zertifikat-Fingerabdrucks	40
6.4	Mögliche weitere Aktionen	40
<b>7</b>	<b>Konfigurieren von BIS-Clients und Tools</b>	<b>41</b>
7.1	Konfigurieren selbstsignierter Zertifikate vom BIS-Server	41
7.1.1	Einstellungen für vertrauenswürdige Sites	42
7.2	Konfigurieren eines selbstsignierten Zertifikats vom BIS Reporting Service	42
7.3	Konfigurieren der Webbrowser für die Clients	43
7.3.1	Einstellungen für Internet Explorer (IE)	43
7.4	Verwenden sicherer Passwörter	45
7.5	Einrichten der Firewall	45
7.6	Installieren optionaler BIS-Tools	45
7.7	Installieren von Software eines Drittanbieters neben BIS	46

---

<b>8</b>	<b>Lizenzierung Ihrer BIS Installation</b>	<b>47</b>
<b>9</b>	<b>Wartung und Deinstallation</b>	<b>49</b>
<b>9.1</b>	Wartung	<b>49</b>
<b>9.2</b>	Sichern und Wiederherstellen von Konfigurationen	<b>49</b>
<b>9.3</b>	Deinstallation	<b>49</b>

# 1 Rechtliche Hinweise

## 1.1 Softwarelizenzvertrag



### Hinweis!

Diese Software ist sicherheitsrelevant. Beschränken Sie den Zugriff auf befugte Personen. Diese Software beinhaltet Funktionen zur Einrichtung von Sicherheitskennwörtern. Legen Sie geeignete Sicherheitsstufen und Kennwörter fest, bevor Sie Bedienern Zugriff auf diese Software gewähren. Schützen Sie den Originaldatenträger vor unbefugter Verwendung. Darüber hinaus sind Alarmzentralen der Bosch Sicherheitssysteme GmbH mit Kennwörtern zum Schutz vor unbefugtem Zugriff versehen. Diese Kennwörter müssen ebenfalls eingerichtet sein und geschützt werden. Das Programm und die Lizenz dürfen nicht ohne ausdrückliche schriftliche Genehmigung von Bosch an Dritte weitergegeben werden.

### 1.1.1 Eingeschränkte Gewährleistung

Bosch Sicherheitssysteme GmbH gewährleistet, dass das Programm im Wesentlichen den veröffentlichten Spezifikationen und der Dokumentation entspricht, sofern es auf der Computerhardware und mit dem Betriebssystem eingesetzt wird, für das es entwickelt wurde. Bosch gewährleistet weiterhin, dass die magnetischen Datenträger, auf denen das Programm vertrieben wird, und die Dokumentation frei von Material- und Herstellungsfehlern sind. Bosch Händler, Distributoren, Vertreter und Mitarbeiter sind nicht befugt, diese Gewährleistung zu ändern oder zu ergänzen, weder in mündlicher noch in schriftlicher Form. Über den oben genannten Umfang hinaus übernimmt Bosch weder eine ausdrückliche noch eine stillschweigende Gewährleistung in Bezug auf das Programm und die Dokumentation, einschließlich der Qualität, Leistung, Handelbarkeit und Eignung für einen bestimmten Zweck.

### 1.1.2 Abhilfemaßnahme

Bosch ersetzt fehlerhafte Datenträger oder Dokumentation oder behebt wesentliche Programmfehler kostenfrei, sofern das Produkt mit Kaufnachweis innerhalb von 90 Tagen nach Lieferung an Bosch zurückgesendet wird. Kann Bosch die fehlerhaften Datenträger oder Dokumentation nicht ersetzen oder wesentliche Programmfehler nicht beheben, erstattet Bosch die Lizenzgebühr. Darüber hinaus bestehen keine weiteren Gewährleistungsansprüche. Da Programme inhärent komplex und möglicherweise nicht völlig fehlerfrei sind, müssen Sie Ihre Arbeit überprüfen. Bosch übernimmt keinerlei Haftung für direkte, indirekte, beiläufige Schäden oder Folgeschäden, die aus der Verwendung oder Nichtverwendung des Programms oder der Dokumentation resultieren, selbst wenn Bosch über die Möglichkeit solcher Schäden in Kenntnis gesetzt wird. Insbesondere haftet Bosch nicht für Kosten, einschließlich, jedoch nicht beschränkt auf, solche, die sich durch entgangene Gewinne, entgangene Verwendung der Computerprogramme oder Daten, Kosten für Ersatzprogramme oder Ansprüche Dritter ergeben. Bosch gewährleistet nicht, dass die lizenzierten Programme nicht unbefugt verwendet oder umgangen werden können. In keinem Fall übersteigt die Haftung von Bosch den Lizenzbetrag.

In manchen Ländern ist der Ausschluss oder die Beschränkung stillschweigender Gewährleistungen oder die Beschränkung der Haftung für beiläufige Schäden oder Folgeschäden nicht gestattet, so dass die obigen Beschränkungen oder Ausschlüsse für Sie möglicherweise nicht gelten.

Bosch Sicherheitssysteme GmbH behält sich alle nicht ausdrücklich gewährten Rechte vor. Kein Teil dieser Lizenz stellt einen Verzicht auf Rechte von Bosch unter den US-amerikanischen Urheberrechtsgesetzen oder sonstigen Bundes- oder Bundesstaatsgesetzen dar.

Sollten Sie Fragen zu dieser Lizenz haben, wenden Sie sich bitte schriftlich an: Bosch Sicherheitssysteme GmbH, Postfach 1111, 85626 Grasbrunn, Deutschland.

## 2 Systemüberblick

### 2.1 Hinweise zu diesem Handbuch

In diesem Handbuch werden die Software- und Hardwareinstallation, die erste Anmeldung und grundlegende Wartungsmaßnahmen behandelt. Nach Abschluss des Installationsvorgangs für die Software sind zudem weitere Schritte erforderlich. Diese Schritte werden unmittelbar im Anschluss an die Installation in einem Dokumentfenster angezeigt oder können über <installation drive>:\MgtS\Platform\Mandatory post installation BIS.pdf eingesehen werden.

### 2.2 Zielgruppe

Für die Installation von BIS sollten Sie mit folgenden Themen vertraut sein:

- Installation von Windows-Betriebssystemen und Anwendungen auf einem Server
- Netzwerk

### 2.3 BIS Einzel-Server-Systeme

#### Definition

Ein BIS Single-Server-System enthält nur einen BIS Einwahl-Server (auch BIS-Server genannt). Dieser kann zum Ausführen von OPC-Servern verwendet werden und kann null oder mehrere Anschalte-Server- und Datenbankserver-Rechner enthalten.

#### Abbildung

BIS Installationen können in ihrer Größe und Komplexität erheblich variieren. Im Folgenden sehen Sie eine kleine und eine komplexe BIS Installation mit einem einzelnen Server.



Abbildung 2.1: Kleines BIS Single-Server-System

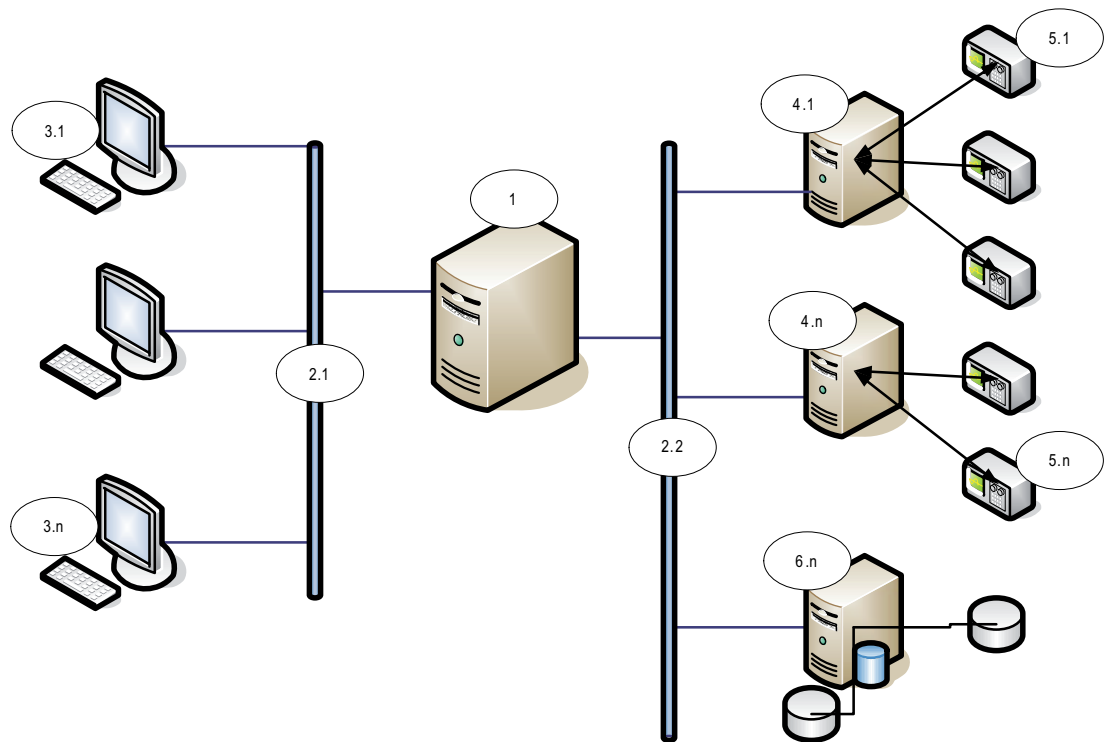


Abbildung 2.2: Komplexes BIS Single-Server-System

Nr.	Name	Funktion
1	BIS (Einwahl-) Server	Führt die BIS Anwendung aus. Der BIS Server fungiert als OPC-Client.
2.1 bis 2.n	Netzwerk(e)	Überträgt Signale
3.1 bis 3.n	BIS Client-Bedienplätze	Führen die BIS Benutzeroberfläche aus
4.1 bis 4.n	Anschalte-Server	Führen OPC-Serverprozesse aus.
5.1 bis 5.n	OPC-Gerät(e)	Interagieren mit der Außenwelt
6.1 bis 6.n	Datenbankserver	Speichert BIS Daten für das Logbuch und Engines

## 2.4

### BIS Multi-Server-Systeme

#### Definition

In einem BIS Multi-Server-System tauschen mindestens zwei BIS Einzel-Server-Systeme Informationen miteinander aus. BIS Multi-Server-Systeme können hierarchisch oder als Peer-to-Peer-Netzwerke aufgebaut werden.

#### Übersicht über die Implementierung

Die teilnehmenden BIS Einzel-Server-Systeme können Anbieter von Informationen, Verbraucher von Informationen oder beides gleichzeitig sein.

- Der Anbieter-Server erstellt eine Konfigurationsdatei, in der genau angegeben ist, welche Informationen er mit anderen teilen soll.

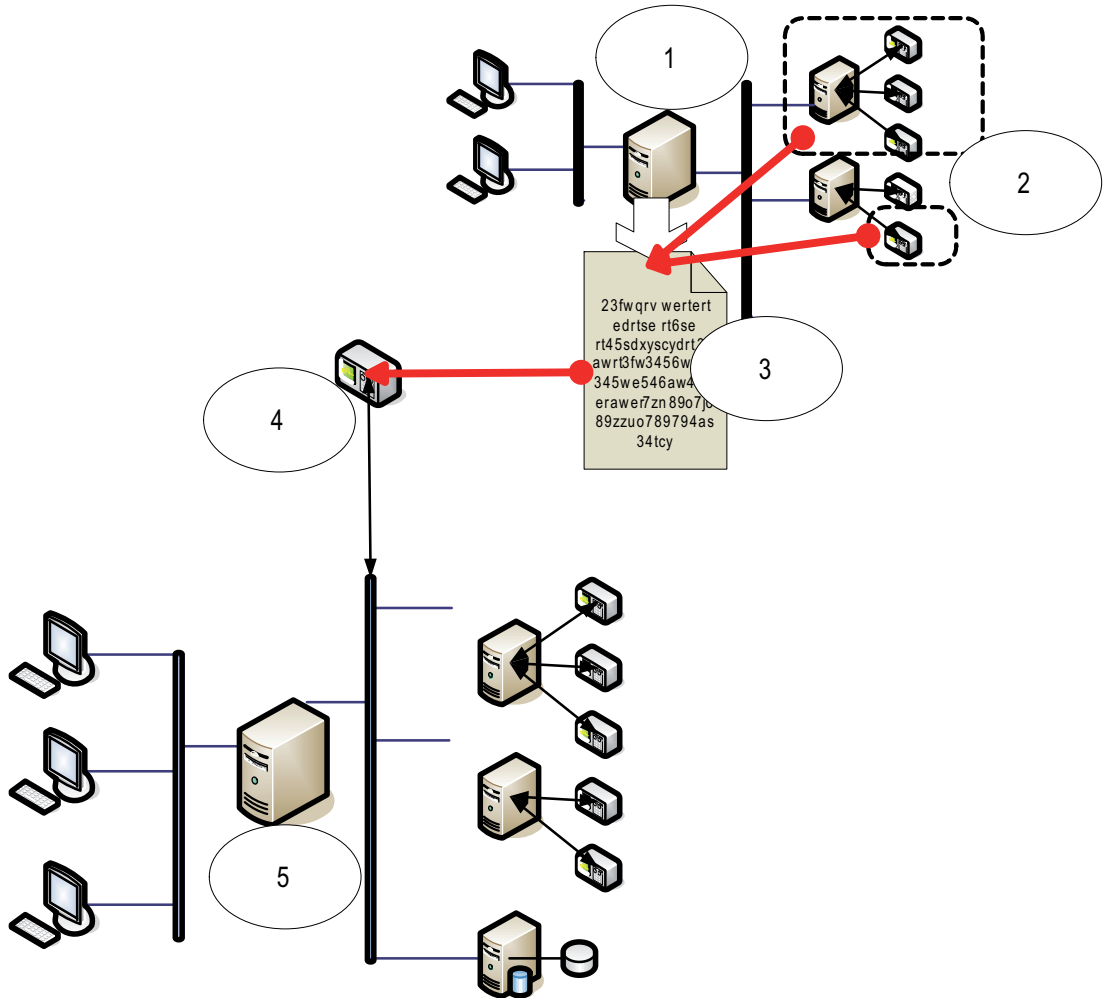


- Der Verbraucher-Server konfiguriert und durchsucht den Anbieter-Server als Remote-OPC-Server.

Beliebige vom Anbieter-Server überwachte Informationen können an den bzw. die Verbraucher-Server übergeben werden. Normalerweise umfassen diese Informationen OPC-Adressen, Statusänderungen, Befehle und Alarme.

**Abbildung**

Der Einfachheit halber wird im Folgenden die Wechselwirkung zwischen einem Anbieter und einem Verbraucher dargestellt. Die Größe und Komplexität des BIS Multi-Server-Systems wird durch den Netzwerkverkehr und die Kapazität des Verbraucher-Servers zur Verarbeitung der eingehenden Daten begrenzt.



Nr.	Name	Funktion
1	Anbieter-Server	Eine Art von BIS-Server, der für andere BIS Einzel-Server-Systeme Informationen bereitstellt.
2	Die Untergruppe der Adressen, die der Anbieter-Server teilen sollte.	
3	Die vom Anbieter-Server generierte verschlüsselte Konfigurationsdatei.	Beschreibt die Untermenge von Informationen, die der Anbieter-Server teilen sollte.

<b>Nr.</b>	<b>Name</b>	<b>Funktion</b>
4	Ein OPC-Server vom Typ BIS Remote-System.	Dient als Schnittstelle zwischen dem Anbieter- und dem Verbraucher-Server. Er wird auf dem Verbraucher-Server mithilfe der verschlüsselten Konfigurationsdatei konfiguriert und dann wie ein gewöhnlicher Anschalte-Server durchsucht.
5	Verbraucher-Server	Dieser BIS Server empfängt und verarbeitet die Informationen seiner eigenen Geräte und der angeschlossenen Anbieter-Server.

### 3 Informationen zur Planung

#### 3.1 Systemvoraussetzungen für den BIS-Server

<b>Server</b>	
<p>Unterstützte Betriebssysteme (eigenständiger Modus oder Client/Server-Modus). BIS kann möglicherweise auch auf anderen Betriebssystemen installiert werden, hierfür besteht jedoch keinerlei Garantie.</p>	<ul style="list-style-type: none"> <li>- Windows Server 2016 (64 Bit, Standard, Datacenter)</li> <li>- Windows Server 2019 (64 Bit, Standard, Datacenter)</li> <li>- Windows 10 Enterprise LTSB (64 Bit)</li> <li>- <b>Hinweis:</b> Die mit dieser BIS-Version ausgelieferte Standard-Datenbank ist SQL Server 2017 Express Edition mit Advanced Services.</li> </ul>
<p>Weitere Software</p>	<p><b>Installieren Sie immer aktuelle Treiber und Betriebssystem-Aktualisierungen.</b></p> <ul style="list-style-type: none"> <li>- IIS 10.0 für Windows 10, Windows Server 2016 und Windows Server 2019</li> <li><b>Hinweis:</b> IIS ist auf BIS-Anschaltesservern nicht erforderlich.</li> <li>- Internet Explorer 9, 10 oder 11 im Kompatibilitätsmodus</li> <li>- .NET:                         <ul style="list-style-type: none"> <li>- Unter Windows 10, Windows Server 2016 und Windows Server 2019: .NET 3.51 und .NET 4.8 (enthält .NET 4.0)</li> </ul> </li> </ul>
<p>Hardware-Mindestanforderungen</p>	<ul style="list-style-type: none"> <li>- Intel i5 Prozessor mit mindestens 4 Kernen</li> <li>- 8 GB RAM (32 GB empfohlen)</li> <li>- 200 GB freier Festplattenspeicher</li> <li>- Grafikkarte mit                         <ul style="list-style-type: none"> <li>- 256 MB RAM</li> <li>- einer Auflösung von 1280x1024</li> <li>- mindestens 32K Farben</li> <li>- OpenGL® 2.1 und DirectX® 11</li> </ul> </li> <li>- Ethernet-Karte mit 1 Gbit/s</li> <li>- Ein freier USB-Anschluss oder Netzwerkfreigabe für Installationsdateien</li> </ul>

**Weitere allgemeine Anforderungen**

- Ein TCP/IP-Netzwerk, das eine Verbindung mit BIS und Datenbankservern herstellt.
- Ein eindeutiger Name für jeden Computer mit max. 15 lateinischen Zeichen ohne diakritische Zeichen.
- US-amerikanische oder standardmäßige europäische Datums-/Uhrzeit-Formate: *MM/dd/yyyy* oder *dd.MM.yyyy*
- Ein Benutzerkonto mit unbeschränkten lokalen Windows-Administratorrechten und Passwort
- Legen Sie ein Passwort für den *MgtS-Service* Benutzer entsprechend Ihrer Passworrichtlinie fest.
- Eine Antivirensoftware sollte installiert sein, darf aber während der BIS-Installation nicht ausgeführt werden.

**Allgemeine Empfehlungen**

- Verwenden Sie die regionalen Einstellungen für die USA, auch wenn die Sprache Ihres Betriebssystems nicht US-Englisch ist.
- Kopieren Sie die BIS-Installationsdateien in ein Unterverzeichnis auf der Hauptfestplatte und führen Sie die Installation von dort aus, statt vom Windows-Desktop.



**Hinweis!**

Hyper-Threading

Auf Systemen mit I5 / I7 / Xenon Prozessoren wird die BIS-Leistung verbessert, wenn Hyper-Threading deaktiviert ist.



**Hinweis!**

Primary Domain Controller (PDCs) und Backup Domain Controller (BDCs) werden nicht unterstützt, da sie keine Administration lokaler Benutzerkonten zulassen, die für Managementsysteme erforderlich sind.



**Hinweis!**

Die Leistungsfähigkeit der Systemkomponenten hängt hauptsächlich von der Größe des Systems ab, also von der Anzahl der vom BIS gesteuerten Objekte. Zur Leistungssteigerung sollte BIS stets als eigenständige Anwendung auf einem aktuellen Rechner in einem Subnetz ausgeführt werden, auf dem kein anderer geschäftskritischer Datenverkehr stattfindet. Dennoch empfiehlt Bosch, die vorhandene Netzwerkhardware unter den geplanten Netzwerkbedingungen zu testen, insbesondere wenn der umfassende Einsatz von IP-Kameras und Bildarchivierung vorgesehen ist.

**3.2 Systemvoraussetzungen für BIS-Clients**

<b>Clients</b>	
<p>Unterstützte Betriebssysteme (eigenständiger Modus oder Client/Server-Modus). BIS kann möglicherweise auch auf anderen Betriebssystemen installiert werden, hierfür besteht jedoch keinerlei Garantie.</p>	<ul style="list-style-type: none"> <li>- Windows 8.1 (64 Bit, Pro, Enterprise)</li> <li>- Windows Server 2016 (64 Bit, Standard, Datacenter)</li> <li>- Windows Server 2019 (64 Bit, Standard, Datacenter)</li> <li>- Windows 10 (32 oder 64 Bit, Pro oder Enterprise LTSB)                             <ul style="list-style-type: none"> <li>- <b>Hinweis:</b> Bei einer Pro-Edition müssen Aktualisierungen bis 8 Monate nach der Einführung der BIS-Version aufgeschoben werden. Weitere Informationen finden Sie auf der Microsoft TechNet-Seite unter <a href="https://technet.microsoft.com/en-us/itpro/windows/manage/introduction-to-windows-10-servicing">https://technet.microsoft.com/en-us/itpro/windows/manage/introduction-to-windows-10-servicing</a></li> </ul> </li> </ul>

<b>Clients</b>	
Weitere Software	<ul style="list-style-type: none"> <li>- ASP.NET</li> <li>- Internet Explorer 9, 10 oder 11 im Kompatibilitätsmodus <b>(Hinweis:</b> Der SEE-Client erfordert IE 9.0)</li> <li>- .NET:                             <ul style="list-style-type: none"> <li>- Unter Windows 10, Windows Server 2016 und Windows Server 2019: .NET 3.51 und .NET 4.8 (enthält .NET 4.0)</li> </ul> </li> </ul>
Hardware-Mindestanforderungen	<ul style="list-style-type: none"> <li>- Intel i5 oder höher</li> <li>- 8 GB RAM (16 GB empfohlen)</li> <li>- 20 GB freier Festplattenspeicher</li> <li>- Grafikkarte mit                             <ul style="list-style-type: none"> <li>- 256 MB RAM</li> <li>- einer Auflösung von 1280x1024</li> <li>- mindestens 32K Farben</li> <li>- OpenGL® 2.1 und DirectX® 11</li> </ul> </li> <li>- Ethernet-Karte mit 100 Mbit/s</li> </ul>
Zusätzliche Mindestanforderungen für VIE-Clients (Video Engine)	<ul style="list-style-type: none"> <li>- Kein Windows Server Betriebssystem</li> <li>- Intel i5 Prozessor oder höher</li> <li>- Für Kamerasequenzierung, virtuelle Matrix oder Multiview sind zusätzliche 4 GB RAM erforderlich</li> <li>- Neueste Videotreiber und Betriebssystem-Aktualisierungen sind dringend empfohlen. Verwenden Sie das DxDiag Diagnoseprogramm von Windows, um sicherzustellen, dass die Treiber maximal 1 Jahr alt sind.</li> </ul>



**Hinweis!**

Es wird empfohlen, weder BIS-Einwahl-Server noch Anschalte-Server als VIE-Client zu verwenden, damit Konflikte mit anderen Videokomponenten ausgeschlossen werden.

### 3.3

### Hardware für zusätzliche Serverfunktionen

<b>Serverfunktion</b>	<b>Erforderliche Hardware</b>
Systemvernetzung (zusätzliche Remote-Computer, Netzwerkdrucker, Bedienrechner im lokalen Netzwerk)	Eine Ethernet-Netzwerkkarte pro Netzwerk (OPC-Subsysteme und Client-Bedienplätze können separaten Netzwerken angehören)
Betrieb eines Monitors	VGA-Grafikkarte zur Unterstützung eines Monitors
Betrieb mehrerer Monitore (bis vier Monitore)	VGA-Grafikkarte(n) zur Unterstützung der gewünschten Anzahl Monitore
Subsysteme und externe Systeme wie Buskoppler (keine Netzwerkanschlüsse)	Eine serielle Schnittstelle (COM-Port) pro Anschluss (onboard oder an einer Schnittstellenerweiterungskarte)

Serverfunktion	Erforderliche Hardware
Zusätzliche Protokoll- oder Alarmdrucker	Je nach Drucker eine serielle oder parallele Schnittstelle (onboard oder an einer Schnittstellenerweiterungskarte). Netzwerkdruck ist ebenfalls möglich.
Externe Geräte wie Backup-Speichergeräte	Entsprechende Controller

### 3.4

## Übersicht des Installationsvorgangs

Die BIS-Installation umfasst im Allgemeinen die folgenden Schritte, welche in diesem Dokument später genauer beschrieben werden.

1. Einrichten des Netzwerks, Abschnitt *Einrichten des Netzwerks, Seite 15*
2. Einrichten des Datenbankservers, Abschnitt *Vorbereiten des Datenbankservers, Seite 18*
3. Installieren der BIS-Software auf dem BIS-Server,
  - Erstinstallation: Abschnitt *Durchführen der Erstinstallation, Seite 15* oder
  - Upgrade: Abschnitt *Durchführen einer Upgrade-Installation, Seite 35*
4. Installieren/Konfigurieren der Firewall, Abschnitt *Einrichten der Firewall, Seite 33*
5. Konfigurieren von DCOM und OPC-Server auf den Anschalteservern, Abschnitt *Konfigurieren von DCOM und OPC-Servern, Seite 34*
6. Konfigurieren der Webbrowser auf den Clients, Abschnitt *Konfigurieren von BIS-Clients und Tools, Seite 41*
7. Ggf. Installieren optionaler BIS-Tools, Abschnitt *Installieren optionaler BIS-Tools, Seite 45*
8. Lizenzierung, Abschnitt *Lizenzierung Ihrer BIS Installation, Seite 47*

## 4 Durchführen der Erstinstallation

Für die Erstinstallation (Hardware und Software) eines BIS-Systems wird die folgende Reihenfolge empfohlen (nicht alle Schritte sind in allen Fällen erforderlich):

1. Einrichten des Computernetzwerks, in dem BIS und die zugehörige(n) Datenbank(en) ausgeführt werden sollen
2. Vorbereiten des Datenbankservers
3. Installieren der BIS-Software auf dem BIS-Server
4. Installieren/Konfigurieren einer Firewall
5. Engine-spezifische Anpassungen bei der Installation

Die Konfiguration der DCOM-Einstellungen für Anschaltserver als Teil der BIS-Installation wird separat in Abschnitt *Konfigurieren von DCOM und OPC-Servern*, Seite 34 behandelt.

### 4.1 Einrichten des Netzwerks

BIS wird normalerweise in einem TCP/IP-Netzwerk ausgeführt. Dieses besteht üblicherweise aus:

- Einem **BIS-Einwahlserver**. Der Server, auf dem die Hauptsoftware der BIS-Anwendung läuft, wird auch als **Einwahlserver** oder **BIS-Server** bezeichnet.
  - Bitte beachten Sie, dass in BIS-Multi-Server-Systemen mehr als ein BIS-Server vorhanden sein kann.
- Null oder mehr Anschaltserver, die mit Peripheriegeräten wie Meldern, Alarmsignalgebern, Durchtritten und Videokameras kommunizieren.
- Null oder mehr **Bedienplätze**, auch als **BIS-Clients** bezeichnet. Dies sind normalerweise Computer, auf denen die BIS-Benutzeroberfläche in einem Webbrowser ausgeführt wird.
- Null oder mehr separate Datenbankserver.

Beachten Sie, dass der BIS-Server die Funktionen des Anschaltserver und der Bedienplätze übernehmen und auch seine eigenen Datenbanken hosten kann. Diese einfache Topologie ist allerdings nicht für große Systeme geeignet ist, da sie die Leistung beschränkt.

#### 4.1.1 Verbinden der Serverrechner mit dem Netzwerk

Zur Verwaltung der zahlreichen Systeme eines Gebäudes wird der BIS-Server normalerweise mit einem Netzwerk verbunden. Die unterschiedlichen Clients und Subsysteme müssen sich dabei nicht unbedingt im selben Netzwerk befinden. Zum Beispiel kann ein Netzwerk für die verbundenen Subsysteme und ein weiteres für die BIS-Clientrechner bestimmt sein.

##### Servernamen

Jeder Computer muss über einen eindeutigen Namen und eine eindeutige IP-Adresse verfügen. Die folgenden Einschränkungen gelten für Servernamen:

- Nicht länger als 15 Zeichen
- Keine Ziffer als erstes Zeichen im Namen
- Keine nicht-lateinischen Zeichen und keine Zeichen mit diakritischen Zeichen Der NetBIOS-Name wird empfohlen.

##### Verbindungen zu Remote-Servern

Die Netzwerkverbindung zu **Datenbankservern** (siehe *Vorbereiten des Datenbankservers*, Seite 18) muss vor der Installation der BIS-Software eingerichtet werden, da der Installationsassistent eine entsprechende Suche durchführt.

Die Einrichtung von **Anschalteservern** zum Ausführen von OPC-Serverprozessen kann dagegen nach der Installation der BIS-Software erfolgen (weitere Informationen hierzu finden Sie in der Dokumentation zur Hardware sowie im Abschnitt *Konfigurieren von DCOM und OPC-Servern*, Seite 34).

Für die Ethernet-Verbindung kann 10, 100 oder 1000BaseT (Twisted Pair) genutzt werden. Wird ein Netzwerkadapter direkt an einen anderen Netzwerkadapter angeschlossen, sollte ein Crossover-Kabel (Null-Modem-Kabel) verwendet werden.



**Hinweis!**

Deaktivieren Sie für die Installation alle energiesparenden Optionen wie „Standby“ oder „Ruhezustand“ auf allen Computern, die Teil des BIS-Systems sind (BIS-Einwahlserver, Datenbankserver, Anschalteserver, BIS-Clients).

**Siehe**

- *Konfigurieren von DCOM und OPC-Servern*, Seite 34

**4.1.2**

**Installieren der erforderlichen Software für Internetinformationsdienste (IIS)**

IIS muss auf dem BIS-Server installiert werden, bevor die BIS-Anwendung installiert wird. IIS ist eine optionale Windows-Komponente, für die möglicherweise das Windows-Installationsmedium erforderlich ist.

Ein neues IIS-Installationskript *InstallIISForBIS.exe* ist auf dem BIS Installationsmedium im Verzeichnis *Tools\InstallIISForBIS\* enthalten. Mit diesem Skript werden alle in der folgenden Tabelle aufgeführten erforderlichen Einstellungen vorgenommen. Bitte beachten Sie, dass das Script .NET 4.0 erfordert.

**WICHTIG:** Wenn Sie IIS nicht über das Skript installieren, lassen Sie die CGI-Funktion aus. Vergewissern Sie sich andernfalls, dass für die IIS-Installation die folgenden Einstellungen unter Windows 10 bzw. Windows Server 2016 oder 2019 festgelegt sind.

<b>Windows 10</b>	<b>Windows Server 2016 und Windows Server 2019</b>
<p><b>Internetinformationsdienste</b>  <b>Webverwaltungstools:</b>  <b>Kompatibilität mit der IIS 6-Verwaltung</b></p> <ul style="list-style-type: none"> <li>- [die Einstellungen]                             <ul style="list-style-type: none"> <li>- IIS 6-Verwaltungskonsole</li> <li>- IIS 6-Skripttools</li> <li>- Kompatibilität mit WMI für IIS 6</li> <li>- IIS 6-Metabasis und IIS 6-Konfigurationskompatibilität</li> </ul> </li> <li>- IIS-Verwaltungskonsole</li> <li>- IIS-Verwaltungsskripts und -tools</li> <li>- IIS-Verwaltungsdienst</li> </ul>	<p><b>Webserver</b>  <b>Allgemeine HTTP-Features:</b></p> <ul style="list-style-type: none"> <li>- Statischer Inhalt</li> <li>- Standarddokument</li> <li>- Suche in Verzeichnissen</li> <li>- HTTP-Fehler</li> </ul>
<p><b>WWW-Dienste:</b>  <b>Anwendungsentwicklungsfeatures:</b></p> <ul style="list-style-type: none"> <li>- [Auf Windows 10-Systemen]</li> </ul>	<p><b>Anwendungsentwicklung:</b></p> <ul style="list-style-type: none"> <li>- ISAPI-Erweiterungen</li> </ul>



<b>Windows 10</b>		<b>Windows Server 2016 und Windows Server 2019</b>
<ul style="list-style-type: none"> <li>- ASP.NET 3.5 <b>und</b></li> <li>- ASP.NET 4.6</li> <li>- .NET-Erweiterbarkeit 3.5 <b>und</b></li> <li>- .NET-Erweiterbarkeit 4.6</li> <li>- ISAPI-Erweiterungen</li> <li>- ISAPI-Filter</li> </ul>		<ul style="list-style-type: none"> <li>- ISAPI-Filter</li> </ul>
<b>Allgemeine HTTP-Features:</b>		<b>Systemzustand und Diagnose:</b>
<ul style="list-style-type: none"> <li>- Standarddokument</li> <li>- Suche in Verzeichnissen</li> <li>- HTTP-Fehler</li> <li>- Statischer Inhalt</li> </ul>		<ul style="list-style-type: none"> <li>- HTTP-Protokollierung</li> <li>- Anforderungsüberwachung</li> </ul>
<b>Systemzustand und Diagnose:</b>		<b>Sicherheit:</b>
<ul style="list-style-type: none"> <li>- HTTP-Protokollierung</li> <li>- Anforderungsüberwachung</li> </ul>		<ul style="list-style-type: none"> <li>- Windows-Authentifizierung</li> <li>- Anforderungsfilterung</li> <li>- Einschränkungen für IP-Adressen und Domänen</li> </ul>
<b>Leistungsfeatures:</b>		<b>Leistung:</b>
<ul style="list-style-type: none"> <li>- Komprimierung statischer Inhalte</li> </ul>		<ul style="list-style-type: none"> <li>- Komprimierung statischer Inhalte</li> </ul>
<b>Sicherheit:</b>		<b>Verwaltungstools:</b>
<ul style="list-style-type: none"> <li>- IP-Sicherheit</li> <li>- Anforderungsfilterung</li> <li>- Windows-Authentifizierung</li> </ul>		<ul style="list-style-type: none"> <li>- IIS-Verwaltungskonsole</li> <li>- IIS-Verwaltungsskripts und -tools</li> <li>- Verwaltungsdienst</li> </ul>
		<b>Verwaltungskompatibilität:</b>
		<ul style="list-style-type: none"> <li>-</li> <li>- IIS 6-Metabasiskompatibilität</li> <li>- Kompatibilität mit WMI für IIS 6</li> <li>- IIS 6-Skripttools</li> <li>- IIS 6-Verwaltungskonsole</li> </ul>

<b>Windows 10</b>		<b>Nur Windows Server 2016 und Windows Server 2019</b>
<b>.NET Framework 3.5</b>		<b>.NET Framework 3.5 Funktionen</b>
<ul style="list-style-type: none"> <li>- Windows Communication Foundation (WCF) HTTP-Aktivierung</li> <li>- Windows Communication Foundation (WCF) Ohne HTTP-Aktivierung</li> </ul>		<ul style="list-style-type: none"> <li>- HTTP Aktivierung</li> <li>- Ohne HTTP Aktivierung</li> </ul>
<b>.NET Framework 4.5 (4.6 für Windows 10) Advanced Services, WCF-Webservices</b>		<b>.NET Framework 4.5 Funktionen, WCF-Webservices</b>
<ul style="list-style-type: none"> <li>- HTTP Aktivierung</li> </ul>		<ul style="list-style-type: none"> <li>- HTTP Aktivierung</li> </ul>

**Deaktivieren der IIS-CGI-Funktion**

Falls IIS bereits mit CGI installiert ist, deaktivieren Sie die Funktion wie folgt für Windows 10:

- Windows 10: **Start > Systemsteuerung > Programme > Windows-Features aktivieren oder deaktivieren > Internetinformationsdienste > WWW-Dienste > Anwendungsentwicklungsfeatures > CGI**

## 4.2

### Vorbereiten des Datenbankservers

#### Einführung

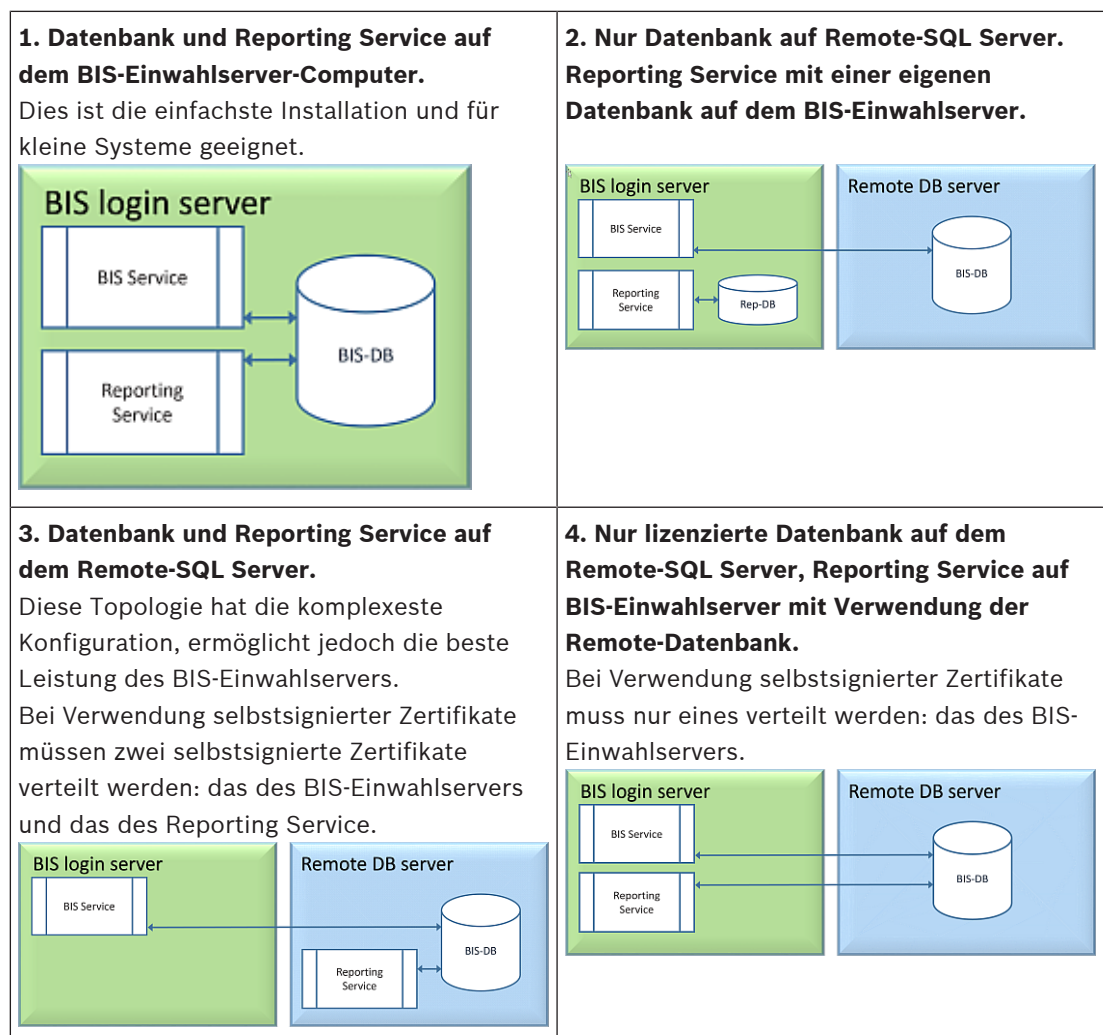
Das BIS-System erfordert eine Microsoft SQL Server-Datenbank und den Reporting Service.

- Sie können die **SQL Server-Datenbank** entweder auf dem BIS-Einwahlserver oder einem separaten Computer installieren. Dieser separate Computer wird als Remote-Datenbankserver bezeichnet.
- Sie können den **Reporting Service** entweder auf dem BIS-Einwahlserver oder auf dem Remote-Datenbankserver installieren.

#### Übersicht der Datenbankserver-Topologien

Da jede dieser beiden Komponenten remote oder lokal (auf dem BIS-Einwahlserver) installiert werden kann, gibt es  $2 \times 2 = 4$  mögliche Datenbankserver-Topologien.

Wählen Sie zum Fortfahren eine der vier Datenbankserver-Topologien aus.



In diesem Kapitel werden die folgenden Verfahren beschrieben:

- Installieren und Veröffentlichen der SQL Server-Datenbank
- Installieren und Konfigurieren des SQL Server Reporting Service

- Vorbereiten des Remote-Datenbankservers auf den Zugriff von BIS
- Sichern des Remote Reporting Service

Ihre Wahl der Datenbankserver-Topologie (1-4) bestimmt, welche der Vorgehensweisen Sie ausführen müssen.



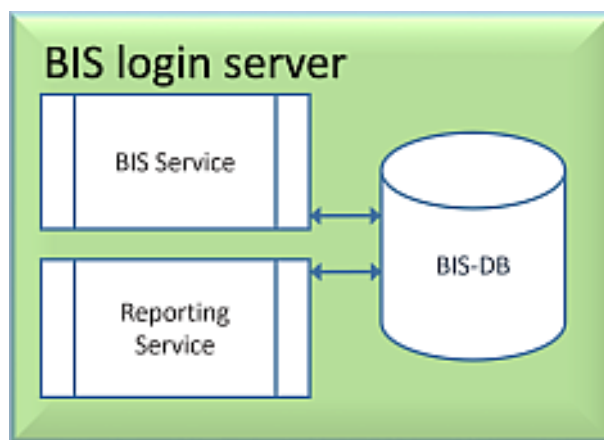
#### Hinweis!

Führen Sie die erforderlichen Verfahren für die gewählte Topologie aus, **BEVOR** Sie das BIS-Setup auf dem BIS-Einwahlserver ausführen.

### 4.2.1

#### Verfahren zum Einrichten von Datenbankserver-Topologien

**Topologie 1: Datenbank und Reporting Service werden auf dem BIS-Einwahlserver-Computer ausgeführt.**



Wenn Sie die kostenlose Express Edition von SQL Server verwenden möchten, die von BIS bereitgestellt wird, ist keine zusätzliche Vorbereitung erforderlich. Bei der BIS-Installation werden die erforderlichen SQL Server-Instanzen erstellt. Sie können mit *Installieren der BIS Software auf dem BIS-Einwahlserver*, Seite 28 fortfahren.

Wenn Sie eine lizenzierte Version von SQL Server für eine größere Kapazität verwenden möchten, gehen Sie vor der Installation der BIS-Software wie folgt vor:

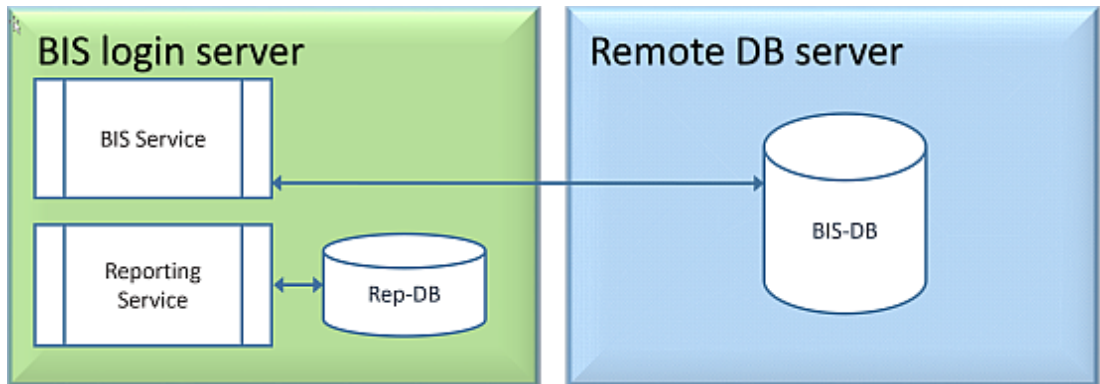
Verfahren 1: *Installieren und Veröffentlichen von SQL Server-Datenbanken auf Datenbankservern*, Seite 22

Verfahren 2: *Installieren und Konfigurieren des SQL Server Reporting Service*, Seite 24

Abschließen mit: *Letzte Schritte vor dem Starten der Installation auf dem Einwahlserver*., Seite 27

Während der Installation der BIS-Software müssen Sie die Datenbankinstanz auswählen, die Sie in diesen Verfahren erstellen.

**Topologie 2: Nur Datenbank auf Remote-SQL Server. Reporting Service mit einer eigenen Datenbank auf dem BIS-Einwahlserver.**



Auf dem Remote-SQL Server-Computer können Sie entweder einen lizenzierten SQL Server oder die Express Edition verwenden.

Führen Sie vor der Installation der BIS-Software die folgenden Schritte aus:

Verfahren 1: *Installieren und Veröffentlichen von SQL Server-Datenbanken auf Datenbankservern, Seite 22*

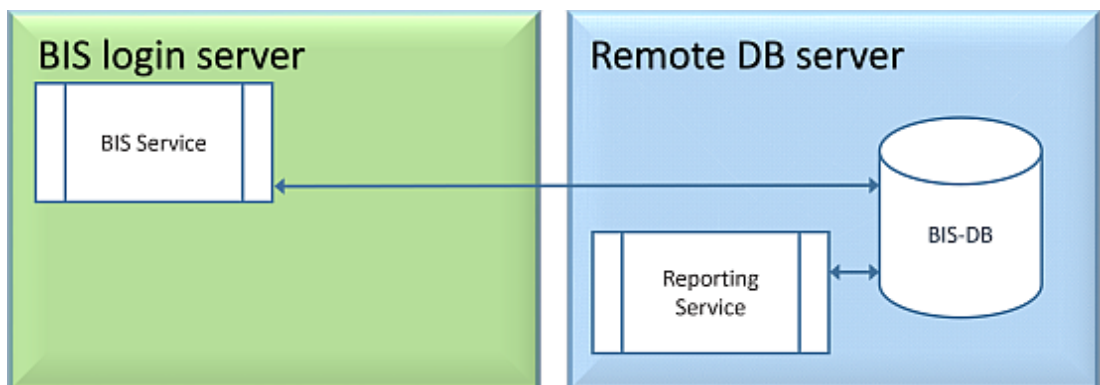
Verfahren 2: *Vorbereiten des Remote-Datenbankservers auf den Zugriff von BIS, Seite 25*

Abschließen mit: *Letzte Schritte vor dem Starten der Installation auf dem Einwahlserver., Seite 27*

Während der Installation der BIS-Software müssen Sie die Datenbankinstanzen für BIS und ACE auswählen, die Sie in Verfahren 1 erstellt haben.

Klicken Sie in einem späteren Schritt der Installation auf **Erstellen**, um eine neue Reporting Service-Instanz auf dem BIS-Einwahlserver zu erstellen.

**Topologie 3: Datenbank und Reporting Service auf dem Remote-SQL Server.**



Auf dem Remote-SQL Server-Computer können Sie entweder einen lizenzierten SQL Server oder die Express Edition verwenden.

Führen Sie vor der Installation der BIS-Software die folgenden Schritte aus:

Verfahren 1: *Installieren und Veröffentlichen von SQL Server-Datenbanken auf Datenbankservern, Seite 22*

Verfahren 2: *Installieren und Konfigurieren des SQL Server Reporting Service, Seite 24*

Verfahren 3: *Vorbereiten des Remote-Datenbankservers auf den Zugriff von BIS, Seite 25*

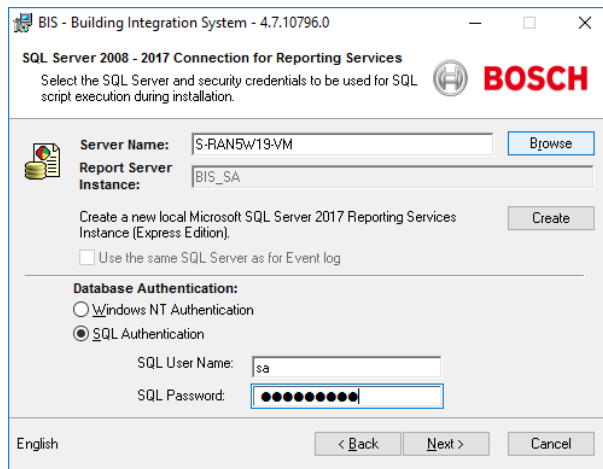
Verfahren 4: *Sichern des Reporting Service auf einem Remote-Datenbankserver, Seite 27*

Abschließen mit: *Letzte Schritte vor dem Starten der Installation auf dem Einwahlserver.*, Seite 27

Während der Installation der BIS-Software müssen Sie die Datenbankinstanzen auswählen, die Sie in diesen Verfahren erstellen.

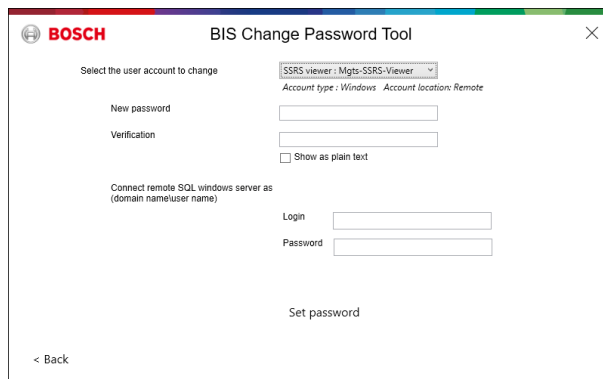
- Wenn Sie Access Engine verwenden, geben Sie den Namen des Remote-Datenbankservers ein und klicken Sie auf **Durchsuchen**, um die ACE-Datenbankinstanz auszuwählen.
- Geben Sie für Reporting Services den Computernamen des Remote-SQL Servers ein, klicken Sie auf **Durchsuchen** und wählen Sie die erforderliche Instanz für den Remote-Reporting Service aus.

**WICHTIG:** Sie dürfen nicht auf **Erstellen** klicken, da hierdurch eine neue Reporting Service-Instanz erstellt wird.



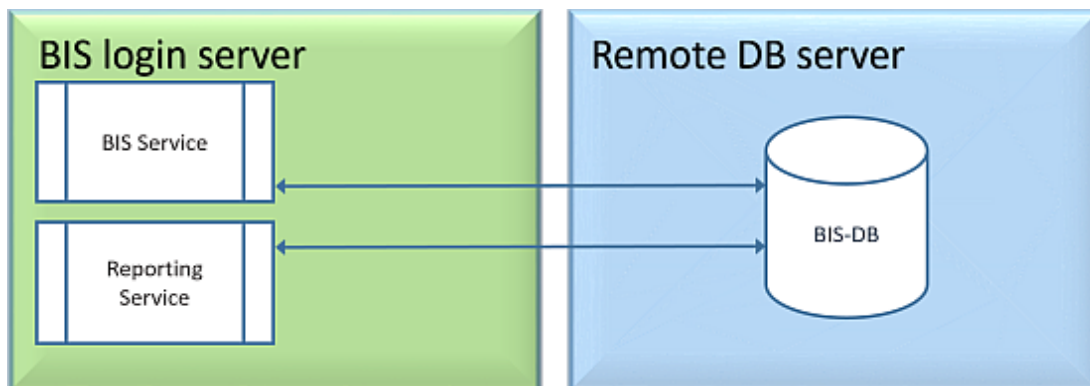
**Wichtiger Hinweis nur für Topologie 3:**

Nach der erfolgreichen Installation von BIS auf dem BIS-Einwahlserver-Computer müssen Sie das BIS Change Password Tool (Tool zur Kennwortänderung, *C:\MgtS\Tools\ChangePassword*) als Administrator ausführen, um das Kennwort von **Mgts-SSRS-Viewer** zu ändern. Wenn Sie das Tool als Administrator ausführen, ist das alte Kennwort nicht erforderlich.



**Topologie 4: Nur Datenbank auf dem Remote-SQL Server, Reporting Service auf BIS-Einwahlserver mit der Remote-Datenbank.**

Topologie 4 wird empfohlen, wenn Sie das selbstsignierte Zertifikat verwenden möchten, das von BIS für die Remote-SQL-Instanz erstellt wurde. Der Grund hierfür ist, dass Sie auf den Clients nur ein selbstsigniertes Zertifikat herunterladen und installieren müssen. Dieses eine Zertifikat umfasst sowohl den BIS-Service als auch den Reporting Service auf dem Einwahlserver.



- Auf dem Remote-Datenbankserver müssen Sie eine lizenzierte Version von SQL Server verwenden.
- Verwenden Sie auf dem BIS-Einwahlserver eine lizenzierte Version von Reporting Service.

Führen Sie vor der Installation der BIS-Software die folgenden Schritte aus:

Verfahren 1: *Installieren und Veröffentlichen von SQL Server-Datenbanken auf Datenbankservern, Seite 22*

Verfahren 2: *Vorbereiten des Remote-Datenbankservers auf den Zugriff von BIS, Seite 25*

Verfahren 3: **Auf dem BIS-Einwahlserver:** *Installieren und Konfigurieren des SQL Server Reporting Service, Seite 24*

Abschließen mit: *Letzte Schritte vor dem Starten der Installation auf dem Einwahlserver., Seite 27*

Während der Installation der BIS-Software müssen Sie die Remote-Instanz für den SQL Server auswählen und den lokalen Reporting Service (auf dem BIS-Einwahlserver) auswählen.

#### Siehe

- *Installieren der BIS Software auf dem BIS-Einwahlserver, Seite 28*
- *Installieren und Veröffentlichen von SQL Server-Datenbanken auf Datenbankservern, Seite 22*
- *Installieren und Konfigurieren des SQL Server Reporting Service, Seite 24*
- *Vorbereiten des Remote-Datenbankservers auf den Zugriff von BIS, Seite 25*
- *Sichern des Reporting Service auf einem Remote-Datenbankserver, Seite 27*
- *Installieren und Konfigurieren des SQL Server Reporting Service, Seite 24*

## 4.2.2

### Installieren und Veröffentlichen von SQL Server-Datenbanken auf Datenbankservern

Remote-Datenbankserver werden in den Topologien 2-4 verwendet.

#### Vorbereiten des Datenbankserver-Computers

Der Datenbankserver-Computer ist:

- In Topologie 1 der BIS-Einwahlserver.
- In Topologien 2-4 ein Remote-Datenbankserver.

**Hinweis!**

Verwenden Sie immer die neuesten Versionen und Service Packs für Ihre SQL Server-Version.

1. Stellen Sie sicher, dass der Hostname nicht länger als 15 Zeichen ist (gemäß Microsoft NetBIOS-Regeln).
2. Stellen Sie sicher, dass der Benutzer **Administrator** ein Kennwort hat.
3. Starten Sie den Datenbankserver-Computer neu und melden Sie sich als **Administrator** an.
4. Stellen Sie sicher, dass .NET 4.8 (oder höher) installiert ist. Sie dürfen NICHT mit einer früheren Version fortfahren.
5. Deaktivieren Sie alle automatischen Standby-Optionen zum Energiesparen.
6. Deaktivieren Sie die Firewall. Die Firewall muss während der Installation deaktiviert bleiben. Reaktivieren Sie sie nach Abschluss der Installation entsprechend der Beschreibung im Dokument *BIS\_Firewall\_Configuration.pdf*.

**Installieren von SQL Server auf dem Datenbankserver-Computer**

1. Entscheiden Sie, ob Sie die Express Edition von SQL 2017 (enthalten auf dem BIS-Installationsmedium <BIS-Installationsmedium>\3rd\_Party\SQL2017\1033\) oder Ihre eigene lizenzierte Version verwenden möchten.
2. Führen Sie die entsprechende *setup.exe* aus.
3. Klicken Sie auf **OK**, wenn Sie aufgefordert werden, die Core-Rolle zu einem neueren Framework und Installer zu ändern.  
Warten Sie, bis das **Installation Center** (Installationscenter) angezeigt wird.
4. Wählen Sie die Registerkarte **Installation** auf der linken Menüleiste aus.
5. Klicken Sie auf **New SQL Server stand-alone Installation or add features to an existing installation** (Neue eigenständige Installation von SQL Server oder Funktionen zu einer bestehenden Installation hinzufügen).
6. Durch den Klick auf **Next** (Weiter) werden die Installationsdateien überprüft und das Setup installiert die Unterstützungsdateien automatisch.
7. Wählen Sie **Perform a new installation of SQL Server 2017** (Neue Installation von SQL Server 2017 ausführen).
8. Akzeptieren Sie die Lizenzbedingungen und klicken Sie auf **Next** (Weiter).
9. Wählen Sie unter **Instance Features** (Instanzfunktionen) die Option *Database Engine Services* aus.
10. Geben Sie die benannte Instanz (Beispiel: *BIS* oder *BISACE*) an, aber geben Sie nicht den Computernamen selbst an und fahren Sie **nicht** mit dem Standard-Instanznamen *SQLExpress* fort.
11. Klicken Sie zum Fortfahren auf **Next** (Weiter).
12. Geben Sie bei **Account Name** (Kontoname) für das SQL Server-Datenbankmodul *NT AUTHORITY\SYSTEM* ein und lassen Sie das Kennwort leer.
13. Ändern Sie den **Startup Type** (Starttyp) zu *Automatic* für **SQL Server Database Engine** (SQL Server-Datenbankmodul) und **SQL Server Browser** (SQL Server-Browser).
14. Wählen Sie *Mixed Mode* für **Authentication Mode** (Authentifizierungsmodus) aus und geben Sie ein sicheres Kennwort für den Benutzer **sa** gemäß Ihrer Kennwortrichtlinie an.  
– Notieren Sie das Kennwort für **sa**, da es für die Installation von BIS erforderlich ist.



15. Fügen Sie bei **Specify SQL Server administrators** (SQL Server-Administratoren angeben) mindestens einen Windows-Benutzer oder vorzugsweise eine Benutzergruppe hinzu, der bzw. die zur Verwaltung des SQL Server berechtigt ist, z. B. „Administrator“ oder „Administratoren“.
16. Klicken Sie auf **Next** (Weiter), um die Installation zu starten.
  - Prüfen Sie anhand der Meldung **Install successful** (Installation erfolgreich), ob die Installation abgeschlossen ist.

#### **Veröffentlichen der SQL-Instanz, damit sie während der Installation der BIS-Software im Netzwerk sichtbar ist**

1. Navigieren Sie zu **Start > Microsoft SQL Server 2017 > SQL Server 2017 Configuration Manager**.
2. Erweitern Sie **SQL Server Network Configuration** (SQL Server-Netzwerkkonfiguration) und wählen Sie Protokolle für <INSTANCE>. Aktivieren Sie **Named Pipes** und **TCP/IP**. <INSTANCE> wird beim SQL-Setup bereitgestellt, z. B.: *BIS/BISACE*
3. Aktivieren Sie **Named Pipes** und **TCP/IP** für die Client-Protokolle des SQL Native Client.
4. Klicken Sie mit der rechten Maustaste auf **Protocols for <INSTANCE>** (Protokolle für <INSTANCE>), wählen Sie **Properties** (Eigenschaften) und dann die Registerkarte **Flags** (Kennzeichnungen) aus. Wählen Sie dort für **Force Encryption** (Verschlüsselung erzwingen) die Option *Yes* aus, um die verschlüsselte Kommunikation zwischen BIS-Server und SQL Server zu aktivieren.
5. Stellen Sie unter **SQL Server services > SQL Server Browser > Properties > Service** (SQL Server-Dienste > SQL Server-Browser > Eigenschaften > Dienst) sicher, dass **Start Mode** (Startmodus) des Diensts **SQL Server Browser** auf *automatic* festgelegt ist.
6. Starten Sie den Computer neu.

#### **Installieren einer zweiten Instanz für ACE**

- Falls für andere Engines (z. B. ACE) erforderlich, wiederholen Sie die Verfahren in diesem Kapitel, um weitere SQL-Instanzen zu installieren.

### **4.2.3**

#### **Installieren und Konfigurieren des SQL Server Reporting Service**

Führen Sie auf dem Computer, auf dem der Reporting Service ausgeführt werden soll, die folgenden Schritte aus:

##### **Installieren des Reporting Service**

1. Öffnen Sie den Speicherort der Reporting Service-Programmdatei, entweder von der Express-Version (Lieferung mit BIS, <BIS-Installationsmedium>\3rd\_Party\SQL2017\) oder den Speicherort des separat lizenzierten Reporting Service.
2. Klicken Sie an diesem Speicherort mit der rechten Maustaste auf *SQLServerReportingServices.exe* und führen Sie es als Administrator aus.
  - Der Setup-Assistent für den **SQL Server Reporting Service** wird geöffnet.
3. Fahren Sie mit der Einrichtung fort.
4. Starten Sie den Computer nach der Installation neu.

##### **Konfigurieren des Reporting Service**

1. Öffnen Sie ein DOS-Befehlsfenster als Administrator.
2. Wechseln Sie zu einem der folgenden Verzeichnisse:
  - <BIS-Installationsmedium>\3rd\_Party\SQL2017\ oder



- Speicherort des lizenzierten Reporting Service.
- 3. Führen Sie von diesem Speicherort den folgenden Befehl aus und ersetzen Sie dabei die Namen von Computer und Instanz:  
DOS> *RSConfig.exe -c -s [DBMachineName]\[InstanceName]*  
*-d ReportServer\$[InstanceName] -a Windows -i SSRS*
- *DBMachineName*: der Computer, auf dem die SQL-Instanz erstellt wird
- *InstanceName*: der Name, der während der Erstellung der SQL-Instanz angegeben wird
- Beispiele:
- Wenn SQL auf dem Computer *SGPBISSQLSERVER* installiert wird und der Instanzname *BIS* ist, lautet der Befehl wie folgt:  
*RSConfig.exe -c -s SGPBISSQLSERVER\BIS -d ReportServer\$BIS -a Windows -i SSRS*

#### Abschluss der Installation

1. Der Assistent zeigt eine Bestätigungsmeldung an.
2. Führen Sie *services.msc* aus und stellen Sie sicher, dass *SQLServerReportingServices* auf dem installierten Computer ausgeführt wird. Starten Sie den Dienst andernfalls manuell.

## 4.2.4

### Vorbereiten des Remote-Datenbankservers auf den Zugriff von BIS

#### Erstellen eines Benutzerkontos für Backup und Wiederherstellung

Erstellen Sie auf dem Remote-Datenbankserver den Benutzer **MgtS-Service** mit den folgenden Einstellungen:

- **Benutzername** (Groß- und Kleinschreibung wird berücksichtigt): *MgtS-Service*
- **Kennwort**: Legen Sie das Kennwort entsprechend Ihren Sicherheitsrichtlinien fest und notieren Sie es, da es für das BIS-Setup auf dem Einwahlservers erforderlich ist.
- **Mitglied von Gruppe**: *Administrators*
- Deaktivieren Sie das Kontrollkästchen **Benutzer muss Kennwort bei der nächsten Anmeldung ändern**.
- Aktivieren Sie das Kontrollkästchen **Benutzer kann Kennwort nicht ändern**.
- Aktivieren Sie das Kontrollkästchen **Kennwort läuft nie ab**.
- Deaktivieren Sie das Kontrollkästchen **Konto ist deaktiviert**.

Der Benutzer **MgtS-Service** benötigt außerdem die Berechtigung zum Anmelden als Dienst:

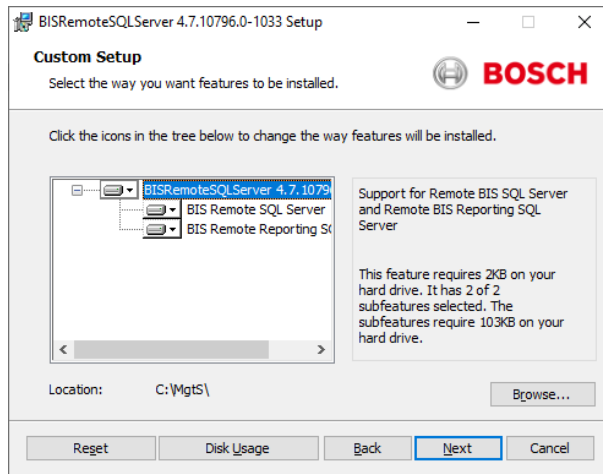
1. Starten Sie *secpol.msc* aus dem Windows-Startmenü.
2. Navigieren Sie im Tool zu **Sicherheitseinstellungen > Lokale Richtlinien > Zuweisen von Benutzerrechten**.
3. Klicken Sie im Bereich **Richtlinie** mit der rechten Maustaste auf **Anmelden als Dienst** und wählen Sie **Eigenschaften** aus.
4. Klicken Sie im Popup-Fenster auf **Benutzer oder Gruppe hinzufügen**.
5. Fügen Sie *<NameOfRemoteDBServer>\MgtS-Service* hinzu.
6. Klicken Sie auf **OK**, um den Vorgang zu bestätigen und das Programm zu schließen.

#### Ausführen des Setups für Remote-SQL Server

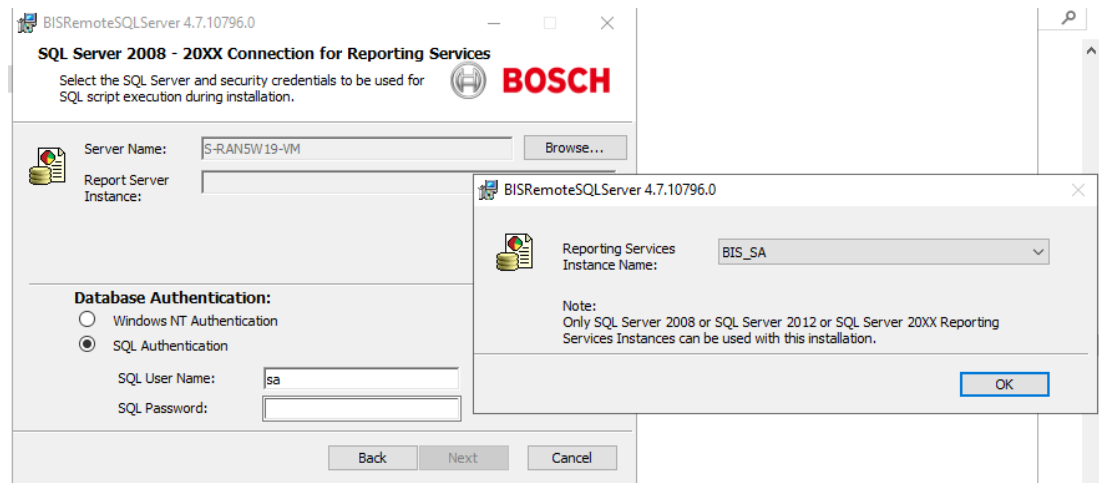
Auf dem Remote-Datenbankserver:

1. Installieren Sie die folgenden Pakete vom BIS-Installationsmedium unter:  
*<Installationsmedium>>\3rd\_Party\SQL2017\SMO\*
- *SQLSysClrTypes.msi*
- *Sqlncli.msi*

2. Kopieren Sie den Inhalt von Speicherort <Installationsmedium>\3rd\_Party\SQLSMO2017\ zu C:\Windows\SysWOW64\.
3. Klicken Sie mit der rechten Maustaste auf die Installationsdatei und führen Sie sie als Administrator aus: *install.exe* unter <Installationsmedium>:\<Sprache\_ID>\BIS\Tools\BISRemoteSQLServerSetup\
4. Während der Installation müssen Sie **eine oder beide** der Funktionen „SQL Server“ und „Berichterstellung für SQL Server“ auswählen.



- Wenn Sie einen Remote-SQL Server für **Logbuch, DB9000, Änderungsverfolgung und/oder Access Engine** verwenden möchten, wählen Sie Funktion *BIS Remote SQL Server* aus.
  - Wenn Sie außerdem einen Remote-SQL Server für **Reporting Services** verwenden möchten, wählen Sie die Funktion *BIS Remote Reporting SQL Server* aus.
5. Suchen und Auswählen der Instanz für Reporting Service



6. Verwenden Sie die SQL-Authentifizierung mit dem Benutzernamen *sa* und dem Kennwort, das Sie während der oben genannten Installation notiert haben.
7. Klicken Sie auf **Weiter** und klicken Sie auf der nächsten Seite auf **Installieren**, um die Installation auszuführen.
8. Starten Sie nach Abschluss der Installation den Remote-Datenbankserver-Computer neu.

**Hinweis!**

Nur eine BIS-Installation pro Remote-Datenbankserver-Computer  
Ein Remote-Datenbank-Computer, der für Reporting Services verwendet wird, unterstützt nur eine BIS-Installation.

**Hinweis!**

Instanzname und Computername  
Achten Sie darauf, dass der Name der Datenbankinstanz aus maximal 15 Zeichen besteht und nicht identisch mit dem Computernamen ist.

#### 4.2.5

#### Sichern des Reporting Service auf einem Remote-Datenbankserver

Wenn der Reporting Service auf einem Remote-Datenbankserver ausgeführt wird, benötigen der BIS-Einwahlserver und BIS-Clients ein Zertifikat vom Reporting Service, um über das Netzwerk sicher darauf zugreifen zu können.

Es können sowohl selbstsignierte als auch von einer Zertifizierungsstelle signierte Zertifikate verwendet werden. In den folgenden Verfahren wird das Erstellen und Bereitstellen dieser Zertifikate beschrieben:

- Selbstsignierte Zertifikate
- Von einer Zertifizierungsstelle signierte Zertifikate

##### Selbstsignierte Zertifikate

1. Führen Sie auf dem Remote-Datenbankserver die folgende *.BAT*-Datei vom Installationsmedium aus, um ein selbstsigniertes Zertifikat zu erstellen und an die Reporting Service-Webadresse zu binden:  

```
_Install\3rd_Party\RemoteReportingService  
\create_remote_sql_certificate.bat
```
2. Exportieren und installieren Sie dieses selbstsignierte Zertifikat als vertrauenswürdiges Stammzertifikat auf dem BIS-Server und allen Client-Computern.
  - Detaillierte Anweisungen finden Sie unter *Konfigurieren eines selbstsignierten Zertifikats vom BIS Reporting Service, Seite 42*.
3. Fügen Sie die HTTPS-URL des Remote-Datenbankservers als vertrauenswürdige Site auf dem BIS-Einwahlserver und allen Clients hinzu, die den Reporting Service verwenden werden.
  - Wenn Ihr Remote-Datenbankserver beispielsweise *MyRemoteDBServer* heißt, navigieren Sie im Einstellungsmenü von Internet Explorer zu **Internetoptionen** > Registerkarte **Sicherheit** > **Vertrauenswürdige Sites** > Schaltfläche **Sites** und fügen Sie *HTTPS://MyRemoteDBServer* hinzu.

##### Von einer Zertifizierungsstelle signierte Zertifikate

Wenn Sie über ein von einer Zertifizierungsstelle signiertes Zertifikat verfügen, muss kein selbstsigniertes Zertifikat erstellt werden. Binden Sie dieses von einer Zertifizierungsstelle signierte Zertifikat stattdessen an die Reporting Service-Webadresse.

Detaillierte Anweisungen finden Sie unter *Aktualisieren der Reporting Service-Bindung, Seite 39*.

#### 4.2.6

#### Letzte Schritte vor dem Starten der Installation auf dem Einwahlserver:

- Damit BIS Sicherungen seiner Datenbanken erstellen und diese wiederherstellen kann, müssen Sie sicherstellen, dass der BIS-Einwahlserver denselben Windows-Benutzer mit demselben Kennwort für die Datenbankadministration hat.

- Wählen Sie in den Dialogen der BIS-Installation die entsprechenden SQL Server-Instanzen für Logbuch, DB9000, Änderungsverfolgung und/oder Access Engine.
- Geben Sie das Kennwort für **sa** ein, das Sie bei der Installation von SQL Server auf dem Remote-Datenbankserver-Computer in *Installieren und Veröffentlichen von SQL Server-Datenbanken auf Datenbankservern*, Seite 22 festgelegt und notiert haben.
- Geben Sie im Dialogfeld, in dem Sie die SQL Server-Instanz für Reporting Services eingeben, den Namen des Remote-Datenbankserver-Computers ein und klicken Sie auf **Durchsuchen**, um alle verfügbaren SQL Server-Instanzen mit Reporting Services anzuzeigen.
- Wählen Sie dieselbe Instanz aus, die Sie während der Ausführung von *install.exe* im Abschnitt *Ausführen des Setups für Remote-SQL Server*, Seite 25 ausgewählt haben.
- Hinweis: Geben Sie für Topologie 2 den BIS-Einwahlserver-Computer ein und klicken Sie auf **Erstellen**, um einen neuen Reporting Service auf dem lokalen Computer zu erstellen.

#### Siehe

- *Installieren und Veröffentlichen von SQL Server-Datenbanken auf Datenbankservern*, Seite 22
- *Vorbereiten des Remote-Datenbankservers auf den Zugriff von BIS*, Seite 25
- *Vorbereiten des Remote-Datenbankservers auf den Zugriff von BIS*, Seite 25

## 4.3

### Installieren der BIS Software auf dem BIS-Einwahlserver

#### Bevor Sie beginnen

Stellen Sie sicher, dass eine der folgenden Voraussetzungen zutrifft:

- Sie installieren alle Systemkomponenten auf dem BIS-Einwahlserver mit einer kostenlosen MS SQL Server Express Edition.
- Sie haben eine der im vorherigen Kapitel *Vorbereiten des Datenbankservers*, Seite 18 beschriebenen Datenbank-Topologien konfiguriert.

Verwenden Sie für die Installation ein Konto mit lokalen Administratorrechten, vorzugsweise das **Administratorkonto**. Geben Sie **ipconfig** in der Eingabeaufforderung ein, um zu prüfen, ob der Server über eine IP-Adresse verfügt. Legen Sie das MS Windows-Installationsmedium bereit, falls der BIS Installation Wizard zusätzliche Funktionen erfordert.

BIS kann nicht installiert werden, wenn eine Firewall aktiv ist. Der BIS Installation Wizard kann zwar die Windows-Firewall deaktivieren, andere Firewalls müssen aber manuell vor dem Start des BIS-Installationsvorgangs deaktiviert werden.



#### Hinweis!

Installation nur auf lokalem Rechner

Das BIS-Installationspaket kann sich auf einem separaten Rechner im Netzwerk befinden, aber setup.exe wird BIS nur auf dem Rechner installieren, der es aufgerufen hat.



#### Hinweis!

Vermeiden Sie Sonderzeichen.

Verwenden Sie keine Sonderzeichen oder nicht lateinischen Zeichen in BIS (z. B. chinesische/russische Zeichen, ä, é, ô, /, #, %, \$, |, !, ~, ' ). Verwenden Sie nur nicht-diakritische Zeichen (7-Bit-ASCII), alphanumerische Zeichen [A-z] [0-9] und Unterstriche.

Dies gilt für die Eingabe von Zeichen (einschließlich Passwörtern) beim BIS Installation Wizard oder Configuration Browser.

Schritt	Vorgang	Ergebnis, Hinweise, Erläuterungen
1	Klicken Sie mit der rechten Maustaste auf <b>setup.exe</b> und wählen Sie <b>Als Administrator ausführen</b> .	Der Dialog für die Sprachauswahl wird geöffnet. <b>Hinweise:</b> <ul style="list-style-type: none"> <li>- Neben Deutsch und Russisch werden derzeit alle Installationen in Englisch durchgeführt.</li> <li>- Um russische Zeichen auf einem nicht russischen Betriebssystem ordnungsgemäß darstellen zu können, müssen Sie das Eingabegebietsschema auf Russisch umstellen.</li> <li>- Sobald BIS in einer bestimmten Sprache installiert wurde, kann diese Sprache auf dem gleichen Computer nicht durch ein nachfolgendes Update geändert werden.</li> </ul>
2	Wählen Sie die Sprache Ihres neuen BIS Systems aus und klicken Sie auf <b>Weiter &gt;</b> .	Der BIS Preparation Wizard wird geöffnet. Der Assistent durchsucht den Rechner nach vorhandener für BIS erforderlicher Software und bereitet die Installation entsprechend vor. Je nach bereits verfügbarer Software markiert der Assistent die folgende erforderliche Software für die Installation zusammen mit BIS: <ul style="list-style-type: none"> <li>- Windows Installer</li> <li>- Erforderliche Versionen des Microsoft .NET Framework. Beachten Sie, dass Sie dazu aufgefordert werden, .NET Framework 3.5 separat vom Installationsmedium des Betriebssystems zu installieren.</li> <li>- SQL-DMO/SMO-Unterstützung</li> </ul>
3	Klicken Sie auf <b>Weiter &gt;</b> .	Wenn der Installationsassistent eine aktive Windows-Firewall ermittelt, klicken Sie auf <b>Ja, Windows-Firewall deaktivieren</b> und auf <b>Weiter &gt;</b> , um sie zu deaktivieren. Andere Firewalls müssen manuell außerhalb des BIS Installationsvorgangs deaktiviert werden, bevor die Installation fortgesetzt wird.
		Der Installationsassistent installiert das Verzeichnis <b>MgtS</b> standardmäßig im Stammverzeichnis des lokalen Laufwerks „C:“. Wenn Sie diesen Speicherort akzeptieren möchten, klicken Sie auf <b>Weiter &gt;</b> . Wenn Sie einen anderen Installationspfad auswählen möchten (nur lokale Laufwerke), klicken Sie auf <b>Durchsuchen</b> .
		Das Dialogfeld „Funktionen auswählen“ wird angezeigt
4	Wählen Sie die zu installierenden BIS Funktionen in der BIS Funktionsauswahl aus.	Wählen Sie nur die Engine(s) und Anschaltung(en) aus, die Sie von Bosch erworben haben. Ohne Lizenz können andere Funktionen nicht verwendet werden und verbrauchen daher unnötig Speicherplatz. Die Standardinstallation installiert alle BIS Funktionen. Verwenden Sie die Dropdown-Menüs, um nicht erforderliche Funktionen von der Installation auszuschließen.

Schritt	Vorgang	Ergebnis, Hinweise, Erläuterungen
5	Klicken Sie auf <b>Weiter &gt;</b> .	<p>Die nächste Stufe des Installationsvorgangs ist die Einrichtung von Datenbankinstanzen für ausgewählte Engines und Funktionen, die diese erfordern (Logbuch/Security Engine, Access Engine sowie im nächsten Schritt Reporting Services).</p> <p>Wenn Sie bereits über SQL Server-Lizenzen mit hoher Kapazität verfügen, können Sie diese für BIS verwenden. Andernfalls kann BIS neue Instanzen mit begrenzter Kapazität für Sie installieren (siehe <i>Kompatibilitätsprobleme mit SQL Server, Seite 31</i> unten).</p> <p>Hinsichtlich der Verfügbarkeit geeigneter SQL Server-Instanzen gibt es im Wesentlichen drei Möglichkeiten, die unten als <b>A</b>, <b>B</b> und <b>C</b> beschrieben werden:</p>

	Verfügbarkeit geeigneter SQL Server-Instanzen		Aktion
<b>A</b>	Auf dem Einwahlserver oder im Netzwerk ist keine geeignete (*) SQL Server-Instanz vorhanden.	>	Klicken Sie auf die Schaltfläche <b>Erstellen</b> . BIS richtet für die folgenden Komponenten separate Instanzen seiner aktuellen Standardversion von SQL Server Express Edition mit Advanced Services ein: <ul style="list-style-type: none"> <li>– Logbuch/Security Engine (SEE nur sofern erforderlich)</li> <li>– Reporting Services</li> <li>– Access Engine (sofern erforderlich)</li> </ul>
<b>B</b>	Eine geeignete (*) SQL Server-Instanz kann durch Durchsuchen des Einwahlserver oder des Netzwerks ermittelt werden.	>	Klicken Sie auf die Schaltfläche <b>Durchsuchen</b> , um das Netzwerk zu durchsuchen und eine Instanz auszuwählen.
<b>C</b>	Eine geeignete (*) SQL Server-Instanz ist vorhanden, kann aber nicht durch Durchsuchen des Einwahlserver oder des Netzwerks ermittelt werden.	>	Geben Sie die Instanz manuell in das Textfeld für den Namen des SQL Servers ein. Verwenden Sie dabei die folgende Syntax: <b>&lt;Rechnername&gt;\&lt;Instanzname&gt;</b> , z. B. MEINSERVER\MEINEINSTANZ.
<p><b>(*)</b> Eine Definition des Begriffs „geeignet“ finden Sie im Warnhinweis <i>Kompatibilitätsprobleme mit SQL Server, Seite 31</i> unten.</p>			

**Kompatibilitätsprobleme mit SQL Server**



**Hinweis!**

**Kompatibilitätsprobleme mit SQL Server bei den obigen Optionen B (Durchsuchen) und C (manuelle Eingabe):**

Die folgenden Kombinationen sind nicht kompatibel:

**Access Engine (ACE)** mit der unbenannten Instanz (LOCAL) sämtlicher SQL Server

**Access Engine (ACE) mit Logbuch/Security Engine zusammen** in derselben Instanz sämtlicher SQL Server Express-Editionen.

**BIS Reporting Services** mit SQL Server-Versionen vor 2008.

**BIS allgemein** mit SQL Server-Versionen vor 2005 SP2. Solche Datenbanken müssen manuell aktualisiert werden, bevor sie mit BIS verwendet werden können.

**BIS**-Versionen vor 4.3 mit SQL Server-Versionen ab SQL Server 2012 (BIS auf Windows 10 Enterprise LTSB wird nur mit SQL 2014 unterstützt)

**Windows Server 2016** unterstützt die folgenden SQL Server-Versionen:

2012 SP2

2014 SP1

2016 SP2

2017

**Windows Server 2019** unterstützt die folgenden SQL Server-Versionen:

2014 SP1

2016 SP2

2017




**Hinweis!**

Für BIS SQL-Server-Instanzen zum Hosten von Access Engine (ACE) muss die **SQL-Authentifizierung** statt der Windows-Authentifizierung verwendet werden. Wenn Sie für ACE vorhandene Instanzen durch Durchsuchen auswählen oder manuell eingeben, geben Sie im Dialogfeld das Passwort „sa“ dieser Instanz ein.

SQL Server Express kann maximal 1 GB RAM verwenden und nur maximal 10 GB große Datenbanken verarbeiten.

Schritt	Vorgang	Ergebnis, Hinweise, Erläuterungen
6	Konfigurieren Sie anhand der oben beschriebenen Aktionen (A, B, C) die erforderlichen Instanzen für Logbuch/SEE und Access Engine.	<b>WICHTIG:</b> Gilt nur beim Erstellen einer <b>neuen</b> Datenbankinstanz: Verwenden Sie immer den <i>sa</i> -Benutzer für das Administratorkonto.  Der BIS Installation Wizard speichert Ihre Auswahl für die Datenbankinstallation.
7	Ermitteln Sie ebenfalls mithilfe des BIS Installation Wizard eine Instanz des Microsoft	<b>WICHTIGER HINWEIS:</b> Dieser Schritt ist nur für die oben beschriebenen Aktionen <b>B oder C</b> relevant, da nach dem Erstellen einer neuen Instanz für das Logbuch im vorherigen Schritt Reporting Services automatisch in dieser Instanz aktiviert wird.

Schritt	Vorgang	Ergebnis, Hinweise, Erläuterungen
	<p>SQL Servers für BIS Reporting Services im Netzwerk.</p>	<p>Diese Reporting Services-Datenbank kann eine separate benannte Instanz sein oder eine SQL Server 2012 SP2 oder höhere Instanz mit dem Logbuch/SEE teilen.</p> <ul style="list-style-type: none"> <li>- Um eine separate Instanz zu erstellen (z. B. wenn im Textfeld <b>Berichtsserver-Instanz</b> kein Name angezeigt wird), klicken Sie auf die Schaltfläche <b>Erstellen</b>. Ein Popup-Fenster wird angezeigt, in dem der Name <b>BISREPORTS</b> vorgegeben ist. Übernehmen (empfohlen) oder ändern Sie den Instanznamen, und klicken Sie auf <b>OK</b>, um zum vorherigen Fenster zurückzukehren und die Installation fortzusetzen.</li> <li>- Um Remote-Knoten nach SQL Server-Instanzen zu durchsuchen, geben Sie den Namen des Remote-Knotens manuell ein und klicken Sie auf die Schaltfläche <b>Durchsuchen</b>.</li> <li>- Um eine Instanz gemeinsam zu verwenden, aktivieren Sie das Kontrollkästchen <b>Denselben Server wie für Logbuch verwenden</b></li> </ul>
		
8	<p>Klicken Sie auf <b>Weiter &gt;</b>.</p>	<ul style="list-style-type: none"> <li>- SQL Server wird installiert.</li> <li>- Die BIS Anwendung wird installiert.</li> <li>- Alle angeforderten Datenbanken werden installiert.</li> <li>- Der BIS Installation Wizard schließt die Installation der Anwendung ab.</li> </ul>
9	<p>Klicken Sie auf <b>Ende</b>.</p>	<p>Die Datei <b>Mandatory Post Installation</b> wird geöffnet.</p>
10	<p>Lesen und befolgen Sie die Anweisungen in dieser Datei, und schließen Sie das Fenster.</p>	<p>Die Datei enthält wichtige Informationen und Anweisungen.</p>
11	<p>Sie müssen den Computer neu starten, um die BIS Installation</p>	<p>Die Erstinstallation der BIS Anwendung ist abgeschlossen. Ein Symbol für den BIS Manager wurde auf dem Desktop erstellt.</p>



Schritt	Vorgang	Ergebnis, Hinweise, Erläuterungen
	abzuschließen. Klicken Sie auf „Ja“, um den Computer neu zu starten.	
12	Klicken Sie nach Abschluss der Installation im BIS Konfigurations-Manager auf die Registerkarte <b>Lizenz</b> , um das Lizenzierungsverfahren zu starten.	Siehe <i>Lizenzierung Ihrer BIS Installation, Seite 47</i>
13	Erstellen Sie eine Erstkonfiguration im BIS Manager.	Entsprechende Anweisungen finden Sie in der Onlinehilfe „BIS Konfigurationsanleitung“. Drücken Sie im BIS Manager die Taste F1.

#### 4.4 Einrichten der Firewall

Bei Windows-Versionen wird eine eigene Firewall installiert, die nur noch konfiguriert werden muss. Bitte befolgen Sie bei der Installation anderer Firewalls die Anweisungen des Herstellers. Sie müssen die Firewall (Windows oder andere) anschließend für die Verwendung mit BIS konfigurieren. Befolgen Sie dazu die Anleitung in der Datei <installation\_drive>:\MgtS\Platform\BIS\_Firewall\_Configuration.pdf

#### 4.5 Engine-spezifische Informationen nach Installationsabschluss

Für verschiedene BIS-Engines müssen nach Abschluss der Hauptinstallation von BIS eventuell zusätzliche Einstellungen vorgenommen werden. Befolgen Sie dazu die entsprechende Installationsanleitung für Ihre Engine in dem jeweiligen Unterverzeichnis von <installation\_drive>:\MgtS\

## 5 Konfigurieren von DCOM und OPC-Servern

Dieser Abschnitt ist nur relevant, wenn Sie OPC-Server installieren möchten (insbesondere OPC-Server von Drittanbietern).

### 5.1 Technische Hintergrundinformationen und Einführung

Die Hauptaufgabe der BIS Anwendung auf dem BIS (Einwahl-)Server besteht darin, Informationen von OPC-Serverprozessen zu erfassen und Befehle an diese weiterzuleiten. Bei diesen Prozessen, die auch als OPC-Server bezeichnet werden, handelt es sich um standardisierte Schnittstellen für eine Vielzahl unterschiedlicher Geräte, darunter Türsteuerungen, Feuermelder und Kameras.

OPC-Serverprozesse werden häufig nicht auf dem BIS Serverrechner ausgeführt, sondern auf Remote-Rechnern, die als **Anschaltesserver** bezeichnet werden. Die Netzwerkkommunikation zwischen einem BIS Server und einem Anschaltesserver wird über DCOM (Distributed Common Object Model) und ein gemeinsames Benutzerkonto mit der Bezeichnung **MgtS-Service** realisiert. Der OPC-Server übernimmt dabei die Identität und Anmeldedaten des MgtS-Service-Benutzerkontos.

Die folgenden Voraussetzungen müssen erfüllt sein:

- Das MgtS-Service-Benutzerkonto muss auf dem Anschaltesserver eingerichtet worden sein.
- MgtS-Service muss über ausreichende Zugriffsrechte für Start und Aktivierung verfügen (lokaler und Remotezugriff).
- Die Installationsroutine für den OPC-Server muss ausgeführt werden (falls verfügbar).

**Hinweis:** Je nach Hersteller können diese Routinen mehr oder weniger komplex sein.

Viele Routinen decken die folgenden Aufgaben bereits ab, einige Aufgaben müssen jedoch möglicherweise manuell vorgenommen werden. Beachten Sie in jedem Fall die Dokumentation für den verwendeten OPC-Server:

- Installieren der OPC-Kernkomponenten.
- Vorbereiten von DCOM zur Unterstützung des OPC-Servers.
- Installieren des OPC-Servers.
- DCOM-Konfiguration des neu installierten OPC-Servers, z. B. der Benutzeridentität (wird normalerweise auf „MgtS-Service“ gesetzt).

Diese Schritte sind in einem separaten Dokument auf dem BIS Installationsmedium beschrieben: **DCOM Configuration.pdf**

#### Verbinden von OPC-Servern mit einer BIS-Installation

Die Komplexität von OPC-Servern und somit auch der Vorgehensweisen zum Verbinden mit einer BIS-Installation ist sehr unterschiedlich. Weitere Informationen zum Verbinden einzelner OPC-Server finden Sie in der Onlinehilfe **BIS-Konfigurationsanleitung**.

## 6 Durchführen einer Upgrade-Installation



### Hinweis!

Kompatibilität mit bestehenden Zentralen

Möglicherweise ergeben sich Versionskonflikte zwischen der neuen BIS-Version und den OPC-Servern von Brandmelde- und Einbruchmeldesystemen, die sich bereits in Ihrer Installation befinden (z. B. Bosch FPA- oder MAP-Zentralen). Um solche Konflikte zu vermeiden, empfiehlt Bosch eindringlich, dass Sie diese Zentralen auf die neueste Firmware aktualisieren, **bevor** Sie mit der Installation des BIS-Upgrades beginnen.

Im Folgenden sind die wesentlichen Schritte zum Upgrade eines BIS-Systems aufgeführt:

1. Wählen Sie einen geeigneten Upgrade-Pfad, abhängig von der Ausgangsversion, der Zielversion und davon, ob Sie die Access Engine verwenden oder nicht. Eine Übersicht über die Upgrade-Pfade finden Sie in den untenstehenden Tabellen.
2. Stellen Sie sicher, dass die Hardware, die erforderliche Software und die Lizenzdatei aktualisiert wurden und den Angaben in *Informationen zur Planung, Seite 11* entsprechen und dass keine Inkompatibilität mit Ihren bestehenden Datenbanken besteht; siehe Informationen zu Kompatibilitätsproblemen mit SQL Server im Abschnitt *Installieren der BIS Software auf dem BIS-Einwahlserver, Seite 28*.
3. Stoppen Sie das BIS-System (und ACE, falls installiert).
4. Führen Sie alle erforderlichen Upgrades von SQL Server durch.
5. Führen Sie das BIS-Setup auf dem BIS-Server aus.

Diese Schritte werden in den folgenden Abschnitten näher beschrieben.

### 6.1 Voraussetzungen

In den folgenden Tabellen sind die unterstützten Upgrade-Pfade für BIS-Versionen mit und ohne Access Engine (ACE) beschrieben. Führen Sie Upgrades nur durch, wenn der entsprechende Upgrade-Pfad unterstützt wird. Möglicherweise muss das Upgrade in mehreren Stufen durchgeführt werden, siehe *Deinstallation, Seite 49*.

Bitte beachten Sie, dass die Installation eines Updates auf die aktuelle BIS-Version immer die vorherigen Versionen entfernt, jedoch durch Beibehaltung der Konfigurationen und Umwandlung der Datenbanken inklusive deren Inhalten Konsistenz gewährleistet.

Beachten Sie dennoch die unten aufgeführten **Informationen** zu MS SQL Server 2000 und WCF-Anpassungen.

From/To	BIS 4.0	BIS 4.1	BIS 4.2	BIS 4.3	BIS 4.4	BIS 4.5	BIS 4.6	BIS 4.7	BIS 4.8
BIS 4.0		✓	✓	✓	✓	✓	✓	✓	✓
BIS 4.1			✓	✓	✓	✓	✓	✓	✓
BIS 4.2				✓	✓	✓	✓	✓	✓
BIS 4.3					✓	✓	✓	✓	✓
BIS 4.4						✓	✓	✓	✓
BIS 4.5							✓	✓	✓
BIS 4.6								✓	✓
BIS 4.7									✓

**Hinweis!**

\*) MS SQL Server 2005

Microsoft SQL Server 2014 SP1 oder höher kann Backup-Datenbanken nicht direkt von einer SQL Server-Version vor 2005 SP3 konvertieren. Wenn Sie noch Backup-Datenbanken vor SQL Server 2005 SP3 verwenden, müssen Sie zunächst ein Zwischen-Upgrade auf Version BIS 2.5 (mit SQL Server 2008) durchführen, bevor Sie mit dem Upgrade auf BIS-Versionen 4.x (mit SQL Server 2012) fortfahren können.

Microsoft SQL Server 2005 SP3 ist die Mindestversion für ein Upgrade auf Microsoft SQL Server 2014.



**Hinweis!**

Multi-Server-BIS und angepasste WCF-Konfigurationen

Wenn Sie manuelle Änderungen an der WCF-Konfigurationsdatei vorgenommen haben:

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

werden diese in BIS 4.0 auch zu BIS 4.1 und neueren Versionen übertragen. Lesen Sie vor der Anpassung dieser Datei zuerst die Fachdokumentation in `\MgtS\Platform\WCF`

`Configuration.pdf`



From/To	BIS 4.1	BIS 4.2	BIS 4.3	BIS 4.4	BIS 4.5	BIS 4.6	BIS 4.7	BIS 4.8
BIS 4.0	✓	✓	✓	✓	✓	✓	✓	✓
BIS 4.1		✓	✓	✓	✓	✓	✓	✓
BIS 4.2			✓	✓	✓	✓	✓	✓
BIS 4.3				✓	✓	✓	✓	✓
BIS 4.4					✓	✓	✓	✓
BIS 4.5						✓	✓	✓
BIS 4.6							✓	✓
BIS 4.7								✓

## 6.2 Starten des BIS Installation Wizard auf dem BIS-Server

Gehen Sie wie folgt vor, um eine vorhandene BIS Installation ohne Verlust der aktuellen Daten und Konfigurationsdateien zu aktualisieren. Diese Beschreibung einer Upgrade-Installation setzt voraus, dass ein Upgrade für eine funktionsfähige BIS Konfiguration durchgeführt wird und das entsprechende Rechnernetzwerk bereits gestartet wurde.

Schritt	Vorgang	Ergebnis, Hinweise, Erläuterungen
1	Sichern Sie Ihre BIS-Installationsdateien oder erstellen Sie eine Image-Kopie der Festplatte, auf der die BIS-Installation gespeichert ist.	
2	Schließen Sie alle BIS-Fenster und stoppen Sie den BIS-Server.	

Schritt	Vorgang	Ergebnis, Hinweise, Erläuterungen
	<p><b>Falls Sie eine Aktualisierung von BIS 4.7 durchführen UND einen Remote-Datenbankserver verwenden</b>, führen Sie die folgende Batchdatei auf dem Remote-Datenbankserver aus:</p>	
3	<p>Legen Sie das BIS-Installationsmedium in den Server ein und führen Sie das Installationsverfahren wie unter <i>Installieren der BIS Software auf dem BIS-Einwahlserver, Seite 28</i> beschrieben durch.</p>	<p><b>Hinweise:</b>                      Bei Installationen von BIS Updates und bei der Wiederverwendung von Datenbankinstanzen muss der Datenbank-Administrator den Benutzernamen <i>sa</i> nicht mehr haben.                      Bei einer BIS Upgrade-Installation wird automatisch auch die Logbuch-Datenbank aktualisiert. Datenbank-Backups aus älteren BIS Versionen können im BIS Manager auf der Registerkarte <b>Logbuch</b> über die Schaltfläche <b>DB-Migration</b> aktualisiert werden. Weitere Informationen finden Sie in der Onlinehilfe „BIS Konfigurationsanleitung“.</p>
4	<p>Wenn der Bildschirm mit der BIS Funktionsauswahl angezeigt wird, wählen Sie die neu zu installierenden BIS Funktionen aus, und schließen Sie die Installation wie unter <i>Installieren der BIS Software auf dem BIS-Einwahlserver, Seite 28</i> beschrieben ab.</p>	
5	<p>Die Datei <b>Mandatory post installation BIS.pdf</b> wird geöffnet. Lesen und befolgen Sie die Anweisungen in dieser Datei aufmerksam, da sie für die neue Version besonders relevant sind.</p>	
6	<p>Klicken Sie nach Abschluss der Installation im BIS Konfigurations-Manager auf die Registerkarte <b>Lizenz</b>, um das Lizenzierungsverfahren zu starten.</p>	<p>Siehe <i>Lizenzierung Ihrer BIS Installation, Seite 47</i></p>

Schritt	Vorgang	Ergebnis, Hinweise, Erläuterungen
7	Erstellen Sie eine neue Konfiguration oder importieren Sie eine vorhandene Konfiguration in den BIS Manager.	Entsprechende Anweisungen finden Sie in der Onlinehilfe. Drücken Sie hierfür im BIS Manager die Taste F1.

### 6.3 Aktualisieren von durch Zertifizierungsstellen signierte Zertifikate

#### Einführung

Die folgenden drei Verfahren sind nur erforderlich, wenn Sie ein aktualisiertes, von einer Zertifizierungsstelle signiertes Zertifikat erworben haben.

- Aktualisieren Sie die IIS-SSL-Bindung (Internet Information Services Secure Socket Layer) mit dem neuen Zertifizierungsstellenzertifikat.
- Aktualisieren Sie die Reporting Service-Bindungen.
- Aktualisieren Sie den „Fingerabdruck“ des von der Zertifizierungsstelle signierten Zertifikats in der Konfigurationsdatei **BISIdservice**.

Alle drei Verfahren werden im Folgenden beschrieben.

#### 6.3.1 Aktualisieren der IIS-SSL-Bindung

##### Vorgehensweise

1. Starten Sie den **Internetinformationsdienste (IIS)-Manager** über das Windows-Startmenü.
2. Wählen Sie unter **Verbindungen** die Option **Standardwebsite** aus.
3. Wählen Sie im Hauptfenster **SSL-Einstellungen** aus.
4. Wählen Sie unter **Aktionen** die Option **Bindungen...** aus.
5. Wählen Sie im Popup **Sitebindungen** die Option **https** aus und klicken Sie auf **Bearbeiten....**
6. Wählen Sie im Popup **Sitebindung bearbeiten** unter **SSL-Zertifikat** Ihr von der Zertifizierungsstelle signiertes Zertifikat aus der Liste aus.
7. Klicken Sie zum Bestätigen auf **OK**.
8. Schließen Sie die Popups und beenden Sie den IIS-Manager.
9. Starten Sie den IIS-Dienst neu, damit die Änderungen wirksam werden.

#### 6.3.2 Aktualisieren der Reporting Service-Bindung

##### Vorgehensweise

1. Starten Sie den **Reporting Services-Konfigurations-Manager** im Windows-Startmenü.
2. Geben Sie unter **Servername** den Namen des Servers ein, auf dem der Reporting Service ausgeführt wird, und klicken Sie auf **Suchen**.
3. Wählen Sie unter **Berichtsserver-Instanz** die richtige Instanz aus der Liste aus.
4. Klicken Sie auf **Verbinden**.
5. Wählen Sie das Menü **Webdienst-URL** aus.
6. Wählen Sie in der Anzeige **Webdienst-URL** unter **HTTPS-Zertifikat** das von der Zertifizierungsstelle signierte Zertifikat aus und klicken Sie auf **Übernehmen**.
7. Starten Sie den Reporting Service neu, damit die Änderungen wirksam werden.

### 6.3.3

#### Aktualisieren des Zertifikat-Fingerabdrucks

**Hinweis:** Sie können entweder das unten beschriebene Verfahren oder das Tool BWC Certificate Configuration (BWC-Zertifikatkonfiguration) verwenden, wie in *BIS\_Data\_Security.PDF* beschrieben.

##### Vorgehensweise

1. Führen Sie *certlm.msc* über die Windows Start- oder Suchen-Symbole aus.
2. Wählen Sie das für Sie ausgestellte Zertifizierungsstellenzertifikat aus und öffnen Sie es.
3. Wählen Sie die Registerkarte **Details** und das Feld **Fingerabdruck** aus.
4. Kopieren Sie den Wert für **Fingerabdruck** (nur die alphanumerischen Zeichen).
5. Öffnen Sie auf dem BIS Installationslaufwerk die Datei *\MgtS\SmartClient\BISIdService\appsettings.json* in einem Texteditor.
6. Ersetzen Sie den vorherigen Fingerabdruckwert zwischen den doppelten Anführungszeichen mit dem neu kopierten Fingerabdruckwert.
7. Öffnen Sie den Internetinformationsdienst und starten Sie den Anwendungspool **BIS IdService** neu, damit diese Änderungen wirksam werden.

### 6.4

#### Mögliche weitere Aktionen

Wenn Sie im Rahmen des Upgrades das System erweitern (z. B. durch Hinzufügen neuer OPC-Server), sind möglicherweise weitere Aktionen erforderlich; siehe *Durchführen der Erstinstallation, Seite 15* beginnend mit *Einrichten der Firewall, Seite 33* und anschließend weiter mit *Konfigurieren von DCOM und OPC-Servern, Seite 34*.



## 7 Konfigurieren von BIS-Clients und Tools

Nach der Installation der BIS-Anwendung können die Client-Software und Software-Tools konfiguriert werden.

### 7.1 Konfigurieren selbstsignierter Zertifikate vom BIS-Server

#### Einführung

Ab BIS 4.7 erfolgt die gesamte Kommunikation zwischen BIS-Clients und BIS-Server über HTTPS. Der BIS Server erstellt selbstsignierte Zertifikate sowohl für Neuinstallationen als auch für Upgrades früherer Versionen, die kein HTTPS hatten. Selbstsignierte Zertifikate sind 30 Jahre gültig.

- Sie müssen das selbstsignierte BIS-Zertifikat von einem Browser herunterladen und auf allen lokalen Computern oder Geräten installieren.
- Nur wenn Sie Access Engine (ACE) verwenden, müssen Sie die Zertifikatsdatei auf dem Installationslaufwerk suchen und auf allen ACE-Clientcomputern auf dieselbe Weise installieren.

#### Herunterladen des selbstsignierten BIS-Zertifikats von einem Browser

1. Öffnen Sie auf dem Clientgerät die Zertifikat-URL in einem Browser. Wenn der Name des BIS Servers beispielsweise *MYBISSERVER* lautet, ist die URL *http://MYBISSERVER/MYCERT.CER*



#### Hinweis!

HTTPS ist zu diesem Zeitpunkt noch nicht konfiguriert, daher müssen Sie das Zertifikat über HTTP herunterladen.

Wenn auf die BIS Server-Webseite bereits über HTTPS zugegriffen wird, können Sie das Zertifikat nicht herunterladen. Löschen Sie in diesem Fall den Browserverlauf, und laden Sie die URL über HTTP erneut.

2. Speichern Sie die Zertifikatsdatei im lokalen Speicher auf dem Clientgerät.

#### Suchen des Zertifikats für Access Engine (ACE)

Das Zertifikat befindet sich am folgenden Speicherort:

```
<installation drive>:\MgtS\Certificates\  
Access Management System Internal CA.cer.
```

#### Installieren selbstsignierter Zertifikate auf einem Client-Computer oder auf dem BIS-Einwahlserver

1. Doppelklicken Sie auf die *.CER* -Datei des Zertifikats, um es zu öffnen.
2. Klicken Sie auf der Registerkarte **General** (Allgemein) auf **Install Certificate** (Zertifikat installieren).
3. Wählen Sie **Local machine** (Lokaler Computer) als den **Speicherort** und klicken Sie auf **Next** (Weiter).
4. Wählen Sie **Place all certificates in the following store** (Alle Zertifikate im folgenden Speicher platzieren) aus, und klicken Sie auf **Browse** (Durchsuchen).
5. Wählen Sie **Trusted Root Certification Authorities** (Vertrauenswürdige Root-Zertifizierungsstellen) aus, und klicken Sie auf **OK**.
6. Klicken Sie auf **Next** (Weiter) und anschließend auf **Finish** (Fertigstellen), um die Installation des Zertifikats abzuschließen.

### Installieren von selbstsignierten Zertifikaten auf einem mobilen Clientgerät

1. Öffnen Sie auf dem mobilen Gerät die Geräteeinstellungen und geben Sie *certificate* ein, um nach dem Installationsmenü für Zertifikate zu suchen.
2. Wählen Sie **Install certificate from storage** (Zertifikat aus dem Speicher installieren) oder – je nach Betriebssystem – ein Menüelement mit einem ähnlichen Namen aus.
3. Wählen Sie das importierte Zertifikat aus, und installieren Sie es. Beachten Sie, dass einige Geräte Zertifikate automatisch installieren, wenn Sie das Zertifikat öffnen.

**Hinweis:** Zertifikate werden für einen bestimmten Hostnamen erstellt, daher schlagen Versuche, sich mit `https://localhost` anzumelden, fehl. Verwenden Sie immer den Hostnamen in der URL, `https://<hostname>`.

#### 7.1.1

### Einstellungen für vertrauenswürdige Sites

Wie in der BIS-Installationsanleitung beschrieben (Abschnitt **Konfigurieren von BIS-Clients und optionalen Tools**) ist die einfachste Methode zum Konfigurieren der erforderlichen vertrauenswürdigen Sites für Internet Explorer auf BIS-Clients die Verwendung der von BIS bereitgestellten *.REG*-Datei.

HTTPS erfordert, dass zusätzliche Sites manuell hinzugefügt werden.

1. Öffnen Sie auf dem Clientgerät die Zertifikat-URL in einem Browser. Wenn der Name des BIS-Servers beispielsweise *MYBISSERVER* lautet, ist die URL `http://MYBISSERVER/MYCERT.CER`.
2. Speichern Sie die Zertifikatdatei im lokalen Speicher auf dem Clientgerät.
3. Öffnen Sie diese URL im Internet Explorer auf dem BIS-Server: `https://localhost/ClientDeploy/tools.aspx`
4. Laden Sie von der aspx-Seite die folgende Datei herunter:  
*IE\_InternetSettings\_Zone2\_TrustedSites\_BIS.zip*
5. Entpacken Sie die *.REG*-Datei aus der *.ZIP*-Datei.
6. Führen Sie die *.REG*-Datei auf jedem der BIS-Clientcomputer von Benutzerkonten mit Administratorrechten aus.

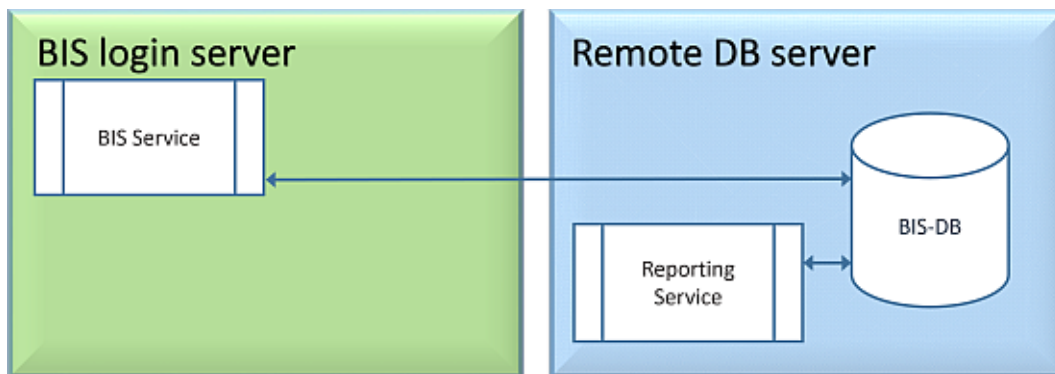
Die IE-Einstellungen werden über die Windows-Registrierung global vorgenommen.

## 7.2

### Konfigurieren eines selbstsignierten Zertifikats vom BIS Reporting Service

#### Einführung

Dieser Abschnitt gilt nur für eine Servertopologie, in der der BIS Reporting Service auf dem Remote-Datenbankserver und **nicht** auf dem BIS-Einwahlserver ausgeführt wird. In allen anderen Topologien benötigt der BIS Reporting Service kein eigenes Zertifikat.



Es sind drei Schritte erforderlich:

1. Exportieren des Zertifikats aus der Zertifikatverwaltung auf dem Remote-Datenbankserver

2. Kopieren der `.CER`-Datei zum BIS-Einwahlserver und den BIS-Clients
3. Installieren des Zertifikats auf dem BIS-Einwahlserver und den BIS-Clients

#### Exportieren des Zertifikats

1. Führen Sie auf dem Remote-Datenbankserver, auf dem der Reporting Service ausgeführt wird, das Windows-Zertifikat-Snap-In `Certlm.msc` im Windows-Startmenü aus.
2. Navigieren Sie in der Zertifikatverwaltung zu **Zertifikate - Lokaler Computer > Eigene Zertifikate > Zertifikate**.
3. Klicken Sie mit der rechten Maustaste auf das Zertifikat für **Reporting Service** und wählen Sie **Alle Aufgaben > Exportieren...** aus.
4. Klicken Sie auf **Weiter**, um mit dem Assistenten fortzufahren. Verwenden Sie nur die Standardwerte.
5. Speichern Sie die `.CER`-Datei (das Zertifikat) an einem geeigneten Speicherort, von dem aus Sie sie einfach auf den BIS-Einwahlserver und die BIS-Clients kopieren können.
6. Wenn Sie die Datei gespeichert haben, schließen Sie `Certlm.msc`.

#### Kopieren des Zertifikats

1. Kopieren Sie die `.CER`-Datei, die Sie auf den BIS-Einwahlserver und alle BIS-Clients exportiert haben.
2. Gehen Sie wie folgt vor, um das Zertifikat auf jedem dieser Computer zu installieren.

#### Installieren selbstsignierter Zertifikate auf einem Client-Computer oder auf dem BIS-Einwahlserver

1. Doppelklicken Sie auf die `.CER`-Datei des Zertifikats, um es zu öffnen.
2. Klicken Sie auf der Registerkarte **General** (Allgemein) auf **Install Certificate** (Zertifikat installieren).
3. Wählen Sie **Local machine** (Lokaler Computer) als den **Speicherort** und klicken Sie auf **Next** (Weiter).
4. Wählen Sie **Place all certificates in the following store** (Alle Zertifikate im folgenden Speicher platzieren) aus, und klicken Sie auf **Browse** (Durchsuchen).
5. Wählen Sie **Trusted Root Certification Authorities** (Vertrauenswürdige Root-Zertifizierungsstellen) aus, und klicken Sie auf **OK**.
6. Klicken Sie auf **Next** (Weiter) und anschließend auf **Finish** (Fertigstellen), um die Installation des Zertifikats abzuschließen.

## 7.3 Konfigurieren der Webbrowser für die Clients

Der BIS Client arbeitet mit dem Webbrowser MS Internet Explorer. Die URL entspricht entweder der des BIS Servers oder `https://<Name_of_BIS_Server>`, wenn der Client auf dem BIS Server selbst ausgeführt werden soll.

Um eine einwandfreie Kommunikation der unterschiedlichen Komponenten des BIS Systems sicherzustellen, ist eine Anpassung der Sicherheitseinstellungen des Browsers erforderlich. Diese Änderungen müssen für alle Browser vorgenommen werden, die den BIS Client ausführen, unabhängig von Benutzer und Betriebssystem.

### 7.3.1 Einstellungen für Internet Explorer (IE)

### Festlegen von Browsereinstellungen mit einer .REG-Datei

Die einfachste Art, Browsereinstellungen zu ändern, ist die Verwendung der vorbereiteten Registrierungs-Befehlsdatei. Führen Sie nach der Installation der BIS-Serversoftware folgendes durch.

1. Öffnen Sie diese URL im Internet Explorer auf dem BIS-Server: `https://<Name_of_BIS_server>/ClientDeploy/tools.aspx`
2. Laden Sie von der aspx-Seite die folgende Datei herunter:  
`IE_InternetSettings_Zone2_TrustedSites_BIS.zip`
3. Entpacken Sie die .REG-Datei aus der .ZIP-Datei.
4. Führen Sie die .REG-Datei auf jedem der BIS-Clientcomputer von Benutzerkonten mit Administratorrechten aus.
  - **Ergebnis:** Die IE-Einstellungen werden über die Windows-Registrierung global vorgenommen.

### Importieren von Zertifikaten für Dienste

Für die HTTPS-Kommunikation zwischen dem Client und den BIS-Komponenten müssen Sie die entsprechenden Zertifikate auf jedem Client installieren:

- BIS-Dienst (in jedem Fall)
- Reporting Service (wenn Reporting Services auf einem Remote-Datenbankserver ausgeführt werden)
- ACE-Dienst (wenn Access Engine installiert ist)

Weitere Informationen finden Sie in der BIS-Hauptinstallationsanleitung.

### Manuelles Durchführen von Browsereinstellungen

Es ist möglich, wenn auch Fehler anfälliger und deshalb nicht empfohlen, die Browsereinstellungen manuell zu erstellen oder anzupassen. Gehen Sie wie folgt vor.

1. Öffnen Sie den Internet Explorer und gehen Sie zur Seite **Internet-Optionen** für diese Browser-Version, d. h. wählen Sie **Tools** (oder das entsprechende Symbol) > **Internet-Optionen**.
2. Wenn der Anmeldebildschirm für den BIS Administrator automatisch beim Starten des Internet Explorers geladen werden soll, geben Sie auf der Registerkarte „General“ (Allgemein) in das Feld für die Startseite die Adresse `https://<Name_of_Bis_Server>` (d.h. die URL Ihres BIS Servers) ein.
3. Klicken Sie auf die Registerkarte **Security** (Sicherheit) > Symbol **Trusted Sites** (Vertrauenswürdige Sites) > Schaltfläche **Sites**.
4. Geben Sie die Adresse `https://<Name_of_Bis_Server>` (<Name\_of\_Bis\_Server> mit dem Namen Ihres BIS Servers ersetzen) ein, und klicken Sie auf die Schaltfläche **Add** (Hinzufügen), um die Adresse zur Liste der vertrauenswürdigen Sites hinzuzufügen. Wenn Sie diesen Client auf dem BIS Server konfigurieren, fügen Sie auch die Adresse `https://localhost` hinzu.
5. Klicken Sie auf die Schaltfläche **Close** (Schließen).
6. Klicken Sie ebenfalls auf der Registerkarte **Security** (Sicherheit) unter **Trusted Sites** (Vertrauenswürdige Sites) auf die Schaltfläche **Custom Level...** (Stufe anpassen...).
7. Suchen Sie auf dem BIS Installationsträger die Datei `<language_folder>\Documents\BIS_platform\IE-Settings.xls` und öffnen Sie diese.
8. Unter **IE-Settings.xls** öffnen Sie die Registerkarte, die Ihre Browserversion betrifft.

9. Abhängig davon, ob Ihrer Standardsicherheitsstufe **Mittel, Hoch** oder **Benutzerspezifisch** ist, aktivieren bzw. deaktivieren Sie die Steuerelemente gemäß der entsprechenden Spalte unter **IE-Settings.xls**. Klicken Sie anschließend auf **OK**.  
**HINWEIS:** Wenn Ihre Sicherheitsstufe keiner der oben genannten entspricht, sollten Sie die Standardstufe **Mittel** festlegen.
10. Starten Sie den Internet Explorer neu, damit die Einstellungen wirksam werden.



#### Hinweis!

Wenn die Windows-Option **Aktualisierung von Stammzertifikaten** aktiviert ist, prüft das Betriebssystem sämtliche Zertifikate über den Microsoft Windows Update-Server und erstellt einen Eintrag im Ereignisprotokoll. Um dies zu verhindern, deaktivieren Sie das Kontrollkästchen **Aktualisierung von Stammzertifikaten** im folgenden Dialogfeld:

**Start > Systemsteuerung > Programme hinzufügen oder entfernen > Windows-Komponenten hinzufügen/entfernen**

## 7.4 Verwenden sicherer Passwörter

Für eine gesteigerte Sicherheit zwingt das System alle Benutzer, ein sicheres Kennwort festzulegen, wenn sie sich an einem Windows-Client mit einem Standardkennwort anmelden, das mit dem Benutzernamen identisch ist.

Befolgen Sie die Anweisungen im Dialogfeld **Kennwort ändern**, um das Kennwort entsprechend der Kennwortrichtlinie zurückzusetzen.



#### Hinweis!

Die Systeme lehnen alle Anmeldungen in mobilen Webclients ab, bis Sie ein sicheres Kennwort in einem Windows-Client festgelegt haben.

## 7.5 Einrichten der Firewall

Befolgen Sie zur Einrichtung einer Firewall für Clients die Anweisungen für den BIS-Server im Abschnitt *Einrichten der Firewall, Seite 33*

## 7.6 Installieren optionaler BIS-Tools

BIS stellt optionale Tools für die folgenden Aufgaben zur Verfügung:

- Begrenzung der von BIS genutzten Netzwerkbandbreite
- Prüfung detaillierter Daten zu einem BIS Client-PC
- Erstellen und Ändern von SQL Server-Berichten für das BIS Logbuch
- Ausführen von Anwendungen für .NET Framework 2.0, 3.5, 4.0 und 4.8

Die Verwendung dieser Tools wird in der Onlinehilfe „BIS Konfigurationsanleitung“ beschrieben. Sie können über eine aktive Serverseite des BIS Servers auf dem BIS Server selbst und/oder auf den BIS Clients installiert werden. Gehen Sie für die Installation wie folgt vor:

1. Starten Sie den Internet Explorer.
2. Geben Sie die folgende URL ein: `https://<Name_of_Bis_Server>/ClientDeploy/Tools.aspx` (Ersetzen Sie den Namen Ihres eigenen BIS Servers). **Hinweis:** Wenn im Internet Explorer keine Adresszeile angezeigt wird, können Sie ebenso auf **Start > Ausführen** klicken und **ieexplore** `https://<Name_of_Bis_Server>/ClientDeploy/Tools.aspx` eingeben.
3. Die Download-Seite wird angezeigt. Klicken Sie für das gewünschte Tool auf die Schaltfläche **Download** (Herunterladen).

4. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Ausführen**.
5. Das Ergebnis ist vom ausgewählten Tool abhängig:
  - Das Programm „NetLimiter“ wird installiert und erfordert einen Neustart.
  - Das Tool „Client-Info“ wird sofort gestartet.
  - Das Tool „Report Builder“ kann direkt nach Klicken auf **Herunterladen** installiert werden.
  - .NET Framework (2.0, 3.5 oder 4.0) kann direkt nach Klicken auf **Download... (Herunterladen...) installiert werden**. Beachten Sie, dass bei Windows 8.1- und Server 2012-Systemen der Microsoft-Installationsträger erforderlich ist.

#### **ChangePassword-Tool**

Ab BIS 4.6 wurde ein neues Tool hinzugefügt, um die Passwörter von BIS-Systembenutzern zu verwalten, d. h. für Benutzer von Windows-Betriebssystemen und SQL.

Weitere Informationen finden Sie in der Hilfe zu BIS Konfiguration.

## 7.7

### **Installieren von Software eines Drittanbieters neben BIS**

#### **Hintergrund**

BIS ist ein geschäftskritisches Sicherheitssystem und sollte immer auf dedizierten Computern ausgeführt werden. Sollte die Installation von zusätzlicher Software eines Drittanbieters unvermeidbar sein, muss dies gut überlegt und geplant werden.



#### **Hinweis!**

Bosch empfiehlt eindringlich, Software eines Drittanbieters zunächst auf einem Offline-Testsystem zu installieren, bevor sie auf einem laufenden System installiert wird.

#### **Vorgehensweise**

Führen Sie immer die folgenden Schritte durch und dokumentieren Sie diese Schritte gründlich, falls später technische Unterstützung erforderlich sein sollte.

1. Vor der Installation von Software eines Drittanbieters auf dem laufenden System:
  - Stellen Sie sicher, dass die Einschränkungen und Anforderungen der Software des Drittanbieters nicht in Konflikt mit denen der BIS stehen.
  - Erstellen Sie einen Wiederherstellungspunkt.
  - Erstellen Sie eine Sicherung des BIS-Systems.
2. Nach der Installation von Software eines Drittanbieters auf dem laufenden System:
  - Stellen Sie sicher, dass BIS voll funktionsfähig ist.

## 8 Lizenzierung Ihrer BIS Installation

Lizenzen für BIS 4.0 und darüber können online bestellt und elektronisch geliefert werden. Gehen Sie wie folgt vor:

1. Bestellen Sie Ihre benötigten Lizenzen bei Ihrem lokalen Bosch Order Desk oder Ihrer Verkaufsorganisation. Sie erhalten daraufhin eine E-Mail mit Ihrer Autorisierungsnummer.



### Hinweis!

#### Notlizenzierung

Lizenzen sind streng an Hardware gebunden. Wenn Sie aufgrund eines Notfalls die Server-Hardware austauschen müssen, wenden Sie sich an einen Bosch Partner oder Kundenberater vor Ort. Bosch kann Ihre Lizenz dann entweder auf die neuen Hardware-IDs übertragen oder eine zeitlich begrenzte Notlizenz ausstellen.

2. Starten Sie den BIS Manager.
3. Klicken Sie in der Registerkarte **License** (Lizenz) auf die Schaltfläche **Start License Manager** (Lizenzmanager starten).
  - **Ergebnis:** Das Dialogfenster „License Manager“ (Lizenzmanager) wird angezeigt.
4. Wählen Sie die Kontrollkästchen für das Softwarepaket, die Funktionen und Erweiterungen aus, die Sie bestellt haben. Geben Sie für die Erweiterungen auch die Anzahl der benötigten Einheiten an.
5. Klicken Sie auf die Schaltfläche **Activate...** (Aktivieren...).
  - **Ergebnis:** Das Dialogfenster **Lizenzaktivierung** mit Ihrer Computersignatur wird angezeigt.
6. Notieren Sie sich die Computersignatur, oder fügen Sie sie per Copy & Paste in eine Textdatei ein.
7. Geben Sie auf einem Rechner mit Internetzugang folgende URL im Browser ein:  
<https://activation.boschsecurity.com>  
Wenn Sie nicht über ein Konto für den Zugriff auf das Bosch License Activation Center verfügen, erstellen Sie entweder ein neues Konto (empfohlen) und melden Sie sich an oder klicken Sie auf den Link, um eine neue Lizenz ohne Anmeldung zu aktivieren. Bitte beachten Sie, dass für SMA-Lizenzen (Softwarewartungsvertrag) immer ein Konto erforderlich ist. Ein Konto hat weiter den Vorteil, das Sie für künftige Angaben einen Überblick über sämtliche Aktivierungen haben.  
  
Folgen Sie den Angaben auf der Website, um den Lizenzaktivierungsschlüssel zu erhalten.
8. Kehren Sie zur Software zurück. Tippen Sie im Dialogfenster **License Activation** (Lizenzaktivierung) den vom Bosch License Activation Center erhaltenen Lizenzaktivierungsschlüssel (oder fügen Sie ihn per Copy & Paste ein) und klicken Sie auf die Schaltfläche **Activate** (Aktivieren).
  - **Ergebnis:** Die Softwarepakete werden für den Rechner aktiviert.
9. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die Änderungen bei den aktivierten Lizenzen anzuzeigen.

**Hinweis!**

Auswirkungen von Hardware- und Softwareänderungen

Änderungen an der Hardware Ihres Servers können dazu führen, dass die Lizenz ungültig wird und die Software nicht mehr funktioniert. Wenden Sie sich an den technischen Support, bevor Sie Änderungen am Server vornehmen.

---



## 9 Wartung und Deinstallation

In diesem Kapitel werden die wichtigsten Schritte beschrieben, die Sie ausführen sollten, damit das BIS-System auf Dauer einwandfrei funktioniert. Auch die Vorgehensweise zur ordnungsgemäßen Deinstallation wird erläutert.

### 9.1 Wartung

Bei BIS-Systemen handelt es sich oft um geschäftskritische Systeme – sowohl in Bezug auf die gespeicherten Daten als auch ihre Funktionen. Bosch empfiehlt daher nachdrücklich die Verwendung eines RAID-Systems oder SAN (Storage Area Network), das jeweils ordnungsgemäß gewartet werden muss. Stellen Sie sicher, dass Sie die Systemfestplatten regelmäßig auf Schreib-/Lesefehler, fehlenden Speicherplatz und erforderliche Fragmentierung prüfen.

Das BIS-Fehlerprotokoll (**BIS Manager** > Registerkarte: **Fehlerprotokoll**) bietet nützliche Informationen zu Problemen, die das System möglicherweise festgestellt hat.

Bosch bietet bei Bedarf über die üblichen Kanäle technische Unterstützung an. Wenden Sie sich hierzu an Ihren Händler. Sollten Sie dabei nähere Informationen zu Ihrer Konfiguration bereitstellen müssen, finden Sie diese im **BIS Manager** in der Registerkarte: **Fehlerprotokoll** > Schaltfläche: **Starte Configuration Collector**. Der Configuration Collector ist Teil jedes BIS-Systems und verfügt über eine eigene Onlinehilfe.

### 9.2 Sichern und Wiederherstellen von Konfigurationen

Die verwendeten BIS-Konfigurationen sollten regelmäßig gesichert werden, insbesondere wenn Sie wichtige Veränderungen vorgenommen haben. Dazu haben Sie zwei Möglichkeiten:

- Manuelle Sicherung im BIS Manager: Stellen Sie sicher, dass das System **gestartet** wurde, und klicken Sie anschließend auf die Registerkarte: **Backup / Restore Konfiguration** > Schaltfläche: **Sichern**.
- Automatische Sicherung als geplante Aufgabe in BIS selbst: Entsprechende Anweisungen finden Sie in der Onlinehilfe zur BIS-Konfiguration.

Das Standardverzeichnis für die Sicherung von Konfigurationen lautet **<installation\_drive>:\Backup**.

Zur Wiederherstellung eines Konfigurations-Backups stellen Sie zunächst sicher, dass die BIS-Anwendung **gestoppt** wurde. Gehen Sie dann zur selben Registerkarte im BIS Manager: **Backup / Restore Konfiguration** > Schaltfläche: **Wiederherstellen**. Wenn Sie eine Konfiguration von einer älteren BIS-Version wiederherstellen, werden alle erforderlichen Konvertierungen automatisch ausgeführt, wenn die neue BIS-Version die alte Konfiguration lädt.

### 9.3 Deinstallation

Eine Deinstallation kann beispielsweise erforderlich sein, wenn ein Upgrade von einer BIS-Version auf eine andere vorgenommen werden soll und der Upgrade-Pfad nicht unterstützt wird. Siehe *Voraussetzungen, Seite 35*



#### Hinweis!

Produkte von Drittanbietern wie Microsoft SQL Server werden vom BIS Installation Wizard nicht entfernt, da diese eventuell von anderen Anwendungen auf Ihrem Rechner benötigt werden. Wenn Sie BIS zu einem späteren Zeitpunkt neu installieren, ohne Microsoft SQL Server zuvor manuell zu deinstallieren, nimmt der Assistent die Installation von BIS in den vorhandenen Datenbanken vor.

1. Stoppen Sie zunächst den BIS-Server. Klicken Sie dazu in BIS Manager auf die Registerkarte **Systemstart/-stop** > Schaltfläche **Stop Server component (Stop Serverkomponente)** .
2. Deinstallieren Sie die BIS Software über die Microsoft Windows-Softwareverwaltung. Klicken Sie beispielsweise unter Windows 7 auf **Start > Control Panel (Systemsteuerung) > Programs and Features (Programme und Funktionen)**. Alle auf dem Rechner installierten Softwarepakete werden aufgelistet. Wählen Sie in dieser Liste den Eintrag **BIS – Building Integration System** aus, klicken Sie auf die Schaltfläche **Entfernen**, und befolgen Sie die Anweisungen des Konfigurationsprogramms.
3. Entfernen Sie ebenso alle weiteren Pakete, deren Namen mit „BIS“ beginnen.
4. Starten Sie den Computer nach der Deinstallation neu.









**Bosch Security Systems B.V.**

Torenallee 49

5617 BA Eindhoven

Netherlands

**[www.boschsecurity.com](http://www.boschsecurity.com)**

© Bosch Security Systems B.V., 2020