Building Integration System

pl Instrukcja instalacji

Spis treści

1 Informacje prawne

1.1 Umowa licencyjna na oprogramowanie

Uwaga!
Niniejsze oprogramowanie służy do zarządzania bezpieczeństwem. Dostęp do niego należy zapewnić jedynie osobom upoważnionym. Oprogramowanie to zawiera mechanizmy do ustawiania haseł zabezpieczających. Przed zapewnieniem pracownikom operacyjnym dostępu do niniejszego oprogramowania należy określić odpowiednie poziomy bezpieczeństwa i ustawić hasła. Trzeba zabezpieczyć oryginalny dysk przed nieuprawnionym użyciem. Ponadto panele kontrole firmy Bosch Sicherheitssysteme GmbH zawierają hasła zapobiegające nieuprawnionemu dostępowi. Należy ustawić również te hasła i starannie je zabezpieczyć. Niniejszego programu ani licencji na jego użytkowanie nie można przekazać żadnej innej stronie bez wyraźnej pisemnej zgody firmy Bosch.

1.1.1 Ograniczona gwarancja

Firma Bosch Sicherheitssysteme GmbH gwarantuje, że niniejsze oprogramowanie jest zasadniczo zgodne z opublikowanymi specyfikacjami i dokumentacją, przy założeniu że jest użytkowane na sprzęcie komputerowym i z systemem operacyjnym, z myślą o których zostało zaprojektowane. Firma Bosch gwarantuje również, że nośniki magnetyczne, na których program jest dystrybuowany, oraz dokumentacja są wolne od wad materiałowych i produkcyjnych. Żaden ze sprzedawców, dystrybutorów, przedstawicieli ani pracowników firmy Bosch nie ma uprawnień do modyfikowania ani uzupełniania niniejszej gwarancji, ustnie ani na piśmie. O ile powyżej nie stwierdzono inaczej, firma Bosch nie udziela żadnych gwarancji ani nie składa żadnych oświadczeń, wyraźnych ani dorozumianych, w odniesieniu do niniejszego programu ani dokumentacji, w tym w odniesieniu do ich jakości, właściwego działania, przydatności handlowej ani przydatności do określonego celu.

1.1.2 Środki prawne

Firma Bosch dokona bezpłatnej wymiany uszkodzonych nośników i dokumentacji oraz poprawi bezpłatnie poważne błędy w oprogramowaniu, o ile Użytkownik zwróci dany produkt firmie Bosch wraz z dowodem zakupu w ciągu 90 dni od daty dostawy. Jeśli firma Bosch nie będzie w stanie dokonać wymiany uszkodzonych nośników lub dokumentacji bądź poprawić poważnych błędów w oprogramowaniu, zwróci Użytkownikowi pobraną opłatę licencyjną. Są to jedyne formy zadośćuczynienia przysługujące Użytkownikowi z tytułu naruszenia gwarancji. Z uwagi na fakt, że programy są z natury rzeczy złożone i nie można zapewnić ich całkowitej bezbłędności, zaleca się Użytkownikowi weryfikację wykonywanych prac. Firma Bosch nie ponosi w żadnym wypadku odpowiedzialności za żadne szkody bezpośrednie, pośrednie lub wtórne wynikłe z użytkowania lub braku możliwości użytkowania programu lub dokumentacji, nawet jeśli została poinformowana o możliwości takich szkód. W szczególności firma Bosch nie ponosi odpowiedzialności za żadne koszty, w tym za koszty poniesione w wyniku utraty zysków lub przychodów bądź utraty możliwości korzystania z programów komputerowych lub danych, za koszty jakiegokolwiek oprogramowania zastępczego bądź związane z roszczeniami osób trzecich ani za żadne inne podobne koszty. Firma Bosch nie twierdzi, że nie da się naruszyć ani obejść zabezpieczeń programów licencyjnych. W żadnym przypadku odpowiedzialność firmy Bosch nie może przekroczyć wysokości opłaty licencyjnej. Ponieważ prawo niektórych krajów nie dopuszcza wyłączenia lub ograniczenia odpowiedzialności z tytułu gwarancji dorozumianych lub ograniczenia odpowiedzialności za szkody przypadkowe lub wtórne, powyższe ograniczenia bądź wyłączenia mogą w przypadku Użytkownika nie mieć zastosowania.

Firma Bosch Security Systems GmbH zachowuje wszelkie prawa, które nie zostały przyznane wprost. Żaden zapis niniejszej licencji nie może być interpretowany jako zrzeczenie się przez firmę Bosch praw przysługujących jej na mocy amerykańskich przepisów o prawie autorskim bądź innych przepisów federalnych czy stanowych.
Wszelkie pytania odnośnie do niniejszej licencji można wysyłać na adres: Bosch Sicherheitssysteme GmbH, Postfach 1111, 85626 Grasbrunn, NIEMCY.

2 Ogólne informacje o systemie

2.1 Informacje o niniejszym podręczniku

W podręczniku tym omówiono kwestie instalacji oprogramowania i sprzętu, początkowego logowania oraz podstawowej konserwacji. Po zakończeniu procedury instalacji oprogramowania należy również wykonać obowiązkowe procedury poinstalacyjne. Procedury te są wymienione w oknie dokumentu wyświetlonym bezpośrednio po dokonaniu instalacji. Można je również znaleźć pod adresem <installation drive>:\MgtS\Platform\Mandatory post installation BIS.pdf.

2.2 Docelowi odbiorcy

Osoba instalująca system BIS powinna mieć wiedzę na temat następujących zagadnień:
– instalowanie na serwerze systemu operacyjnego Windows i aplikacji,
– praca w sieci.

2.3 Jednoserwerowe systemy BIS

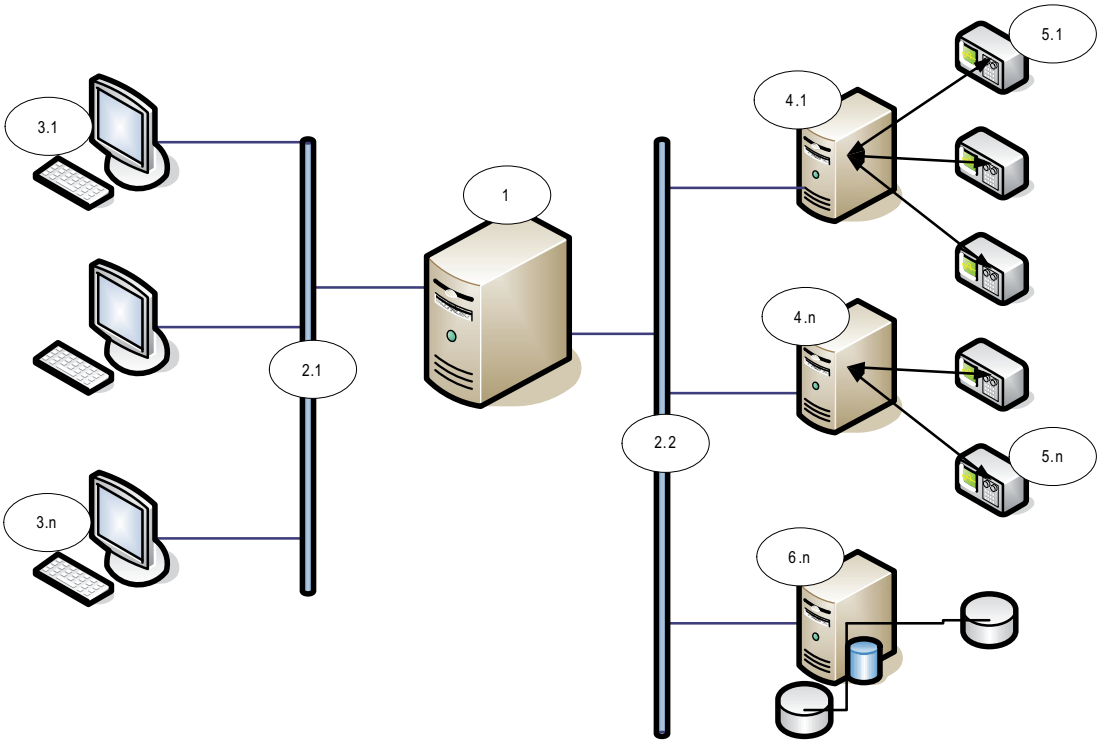
Definicja

Jednoserwerowy system BIS zawiera tylko jeden serwer logowania systemu BIS (zwany też serwerem systemu BIS). Może sam obsługiwać serwery OPC, może też zawierać zero lub więcej serwerów połączeń i komputerowych serwerów baz danych.

Ilustracja

Instalacje systemu BIS różnią się znacznie pod względem rozmiarów i złożoności. Poniżej przedstawiono przykłady małej i złożonej jednoserwerowej instalacji systemu BIS.

Rysunek 2.1: Mały jednoserwerowy system BIS



Rysunek 2.2: Złożony jednoserwerowy system BIS

Nr	Nazwa	Funkcja
1	Serwer (logowania) systemu BIS	Wykonuje aplikację BIS. Serwer systemu BIS funkcjonuje jako klient OPC.
Od 2.1 do 2.n	Sieć (sieci)	Przenosi sygnały.
Od 3.1 do 3.n	Stacja robocza (stacje robocze) klienta systemu BIS	Obsługuje interfejs użytkownika systemu BIS.
Od 4.1 do 4.n	Serwer połączeń (serwery połączeń)	Obsługuje procesy serwera OPC.
Od 5.1 do 5.n	Urządzenie (urządzenia) OPC	Obsługuje interakcje ze światem zewnętrznym.
Od 6.1 do 6.n	Serwer baz danych	Zapewnia hosting danych systemu BIS na potrzeby dziennika zdarzeń i różnych modułów.

2.4 Wieloserwerowe systemy BIS

Definicja

Wieloserwerowy system BIS to system, w którym wymienia między sobą informacje dwa lub więcej jednoserwerowych systemów BIS. Wieloserwerowe systemy BIS mogą mieć postać sieci hierarchicznych lub równorzędnych (peer-to-peer).

Ogólne informacje o wdrożeniu

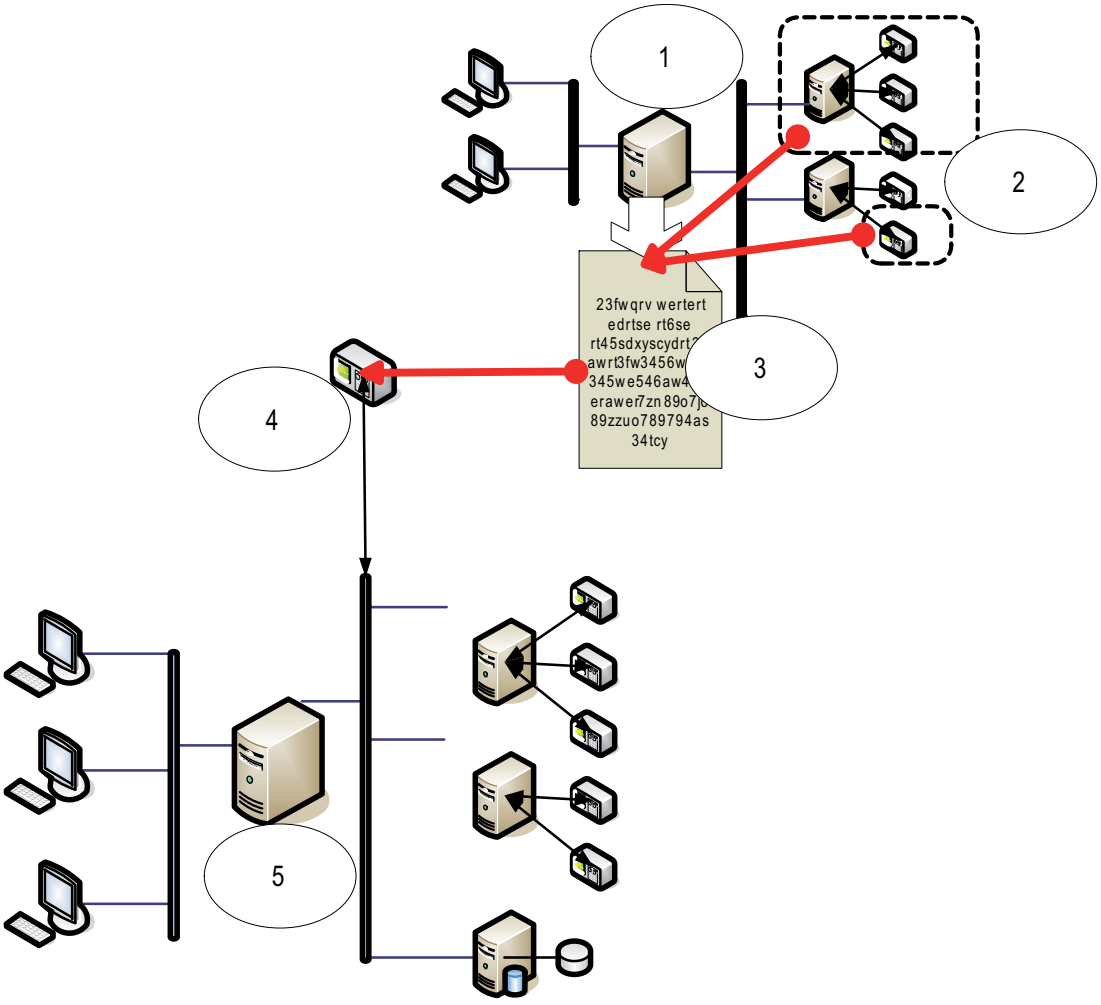
Jednoserwerowe systemy BIS wchodzące w skład konfiguracji mogą dostarczać informacje, odbierać je lub pełnić równocześnie obie te funkcje.

- Serwer nadawczy tworzy plik konfiguracyjny, w którym określa się dokładnie, jakie informacje powinien udostępniać innym serwerom.
- Serwer odbiorczy konfiguruje i przegląda zawartość serwera nadawczego jako zdalny serwer OPC.

Wybrane lub wszystkie informacje monitorowane przez serwer nadawczy mogą być przekazywane jednemu lub więcej serwerów odbiorczych. Zazwyczaj w skład takich informacji wchodzą adresy OPC, informacje o zmianach stanu, polecenia i alarmy.

Ilustracja

Dla uproszczenia na poniższej ilustracji przedstawiono interakcje pomiędzy jednym serwerem nadawczym i jednym serwerem odbiorczym. Rozmiar i złożoność wieloserwerowego systemu BIS są ograniczone przez ruch sieciowy i zdolność serwerów odbiorczych do przetwarzania danych przychodzących.



Nr	Nazwa	Funkcja
1	Serwer nadawczy	Rodzaj serwera systemu BIS, który dostarcza informacje innym jednoserwerowym systemom BIS.
2	Podzbiór adresów, które powinien udostępniać serwer nadawczy.	
3	Zaszyfrowany plik konfiguracyjny wygenerowany przez serwer nadawczy.	Opisuje podzbiór informacji, które powinien udostępniać serwer nadawczy.
4	Serwer OPC typu „zdalny system BIS”.	Pełni funkcję interfejsu pomiędzy serwerem nadawczym i serwerem odbiorczym. Jest skonfigurowany na serwerze odbiorczym za pomocą zaszyfrowanego pliku konfiguracyjnego i potem przeglądany, jak każdy inny serwer połączeń.
5	Serwer odbiorczy	Serwer BIS otrzymuje i przetwarza informacje od urządzeń własnych oraz od urządzeń połączonych z nim serwerów nadawczych.

3 Informacje na potrzeby planowania

3.1 Wymagania systemowe dotyczące serwera systemu BIS

Serwery	
Obsługiwane systemy operacyjne (w trybie standalone lub klient/serwer). Instalacja systemu BIS na innym systemie operacyjnym może zakończyć się powodzeniem, ale nie jest objęta gwarancją.	– Windows Server 2016 (64-bitowy, Standard lub Datacenter) – Windows Server 2019 (64-bitowy, Standard lub Datacenter) – Windows 10 Enterprise LTSB (64-bitowy) – **Uwaga:** domyślny system bazodanowy dostarczany z tą wersją systemu BIS to SQL Server 2017 Express z usługami zaawansowanymi
Inne oprogramowanie	**Należy zawsze instalować najnowsze sterowniki i aktualizacje systemu operacyjnego.** – IIS 10.0 dla systemów Windows 10, Windows Server 2016 i Windows Server 2019 **Uwaga:** program IIS nie jest konieczny w przypadku serwerów połączeń BIS – Internet Explorer 9, 10 lub 11 działający w trybie zgodności – .NET: – W systemach Windows 10, Windows Server 2016 i Windows Server 2019: .NET 3.51 i .NET 4.8 (obejmuje .NET 4.0)
Minimalne wymagania sprzętowe	– Procesor Intel i5 z co najmniej 4 rdzeniami fizycznymi – 8 GB RAM (32 GB — zalecane) – 200 GB wolnego miejsca na dysku twardym – Karta graficzna – 256 MB pamięci RAM, – Rozdzielczość 1280x1024 – Co najmniej 32 tys. kolorów – OpenGL® 2.1 i DirectX® 11 – Karta Ethernet 1 Gbit/s – Wolny port USB lub udział sieciowy na pliki instalacyjne

Inne wymagania ogólne

- Sieć TCP/IP łącząca serwery BIS z serwerami baz danych
- Niepowtarzalna nazwa dla każdego komputera, nie dłuższa niż 15 znaków łacińskich bez znaków diakrytycznych.
- Amerykański lub standardowy europejski format daty/godziny: *MM/dd/yyyy* lub *dd.MM.yyyy*
- Konto użytkownika z nieograniczonymi uprawnieniami administratora systemu Windows oraz hasłem
- Ustaw hasło dla użytkownika *MgtS-Service* zgodnie z zasadami haseł.
- W trakcie instalacji systemu BIS powinno być zainstalowane oprogramowanie antywirusowe, ale nie może ono być uruchomione w tym czasie.

Zalecenia ogólne

- Używaj ustawień regionalnych dla Stanów Zjednoczonych, nawet jeśli Twój system operacyjny nie jest w języku angielskim.
- Skopiuj pliki instalacyjne systemu BIS do podfolderu na dysku głównym i zainstaluj z tego miejsca, a nie z pulpitu systemu Windows.

Uwaga!
Hiperwątkowość
W systemach z procesorami I5/I7/Xenon wydajność systemu BIS będzie większa, gdy wyłączy się opcję hiperwątkowości.

Uwaga!
Podstawowe kontrolery domeny (PDC) oraz zapasowe kontrolery domeny (BDC) nie są obsługiwane, ponieważ nie umożliwiają administracji lokalnymi kontami użytkowników, która jest konieczna w przypadku systemów zarządzania.

Uwaga!
Wydajność składników systemu zależy w znacznym stopniu od jego rozmiarów, tzn. od liczby obiektów pod kontrolą systemu BIS. Aby maksymalnie zwiększyć wydajność tego systemu, należy go zawsze uruchamiać jako autonomiczną aplikację na nowoczesnym komputerze pracującym w sieci, w której nie ma innego ruchu o znaczeniu krytycznym dla działalności biznesowej. Niemniej jednak firma Bosch zaleca przetestowanie istniejącego sprzętu sieciowego w przewidywanych warunkach sieciowych, zwłaszcza jeśli planuje się intensywne korzystanie z kamer sieciowych i częstą archiwizację obrazów.

3.2 Wymagania systemowe dotyczące klientów systemu BIS

Stacje klienckie	
Obsługiwane systemy operacyjne (w trybie standalone lub klient/serwer). Instalacja systemu BIS na innym systemie operacyjnym może zakończyć się powodzeniem, ale nie jest objęta gwarancją.	– Windows 8.1 (64-bitowy, Pro lub Enterprise) – Windows Server 2016 (64-bitowy, Standard lub Datacenter) – Windows Server 2019 (64-bitowy, Standard lub Datacenter) – Windows 10 (32- lub 64-bitowy, Pro lub Enterprise LTSB) – **Uwaga:** w przypadku wersji Pro aktualizacje należy odłożyć na 8 miesięcy po wydaniu wersji systemu BIS. Więcej informacji można znaleźć w witrynie Microsoft TechNet pod adresem https://technet.microsoft.com/en-us/itpro/windows/manage/introduction-to-windows-10-servicing
Inne oprogramowanie:	– ASP.NET

Stacje klienckie	
	– Przeglądarka Internet Explorer 9, 10 lub 11 działająca w trybie zgodności (**Uwaga:** klient SEE wymaga przeglądarki IE 9.0) – .NET: – W systemach Windows 10, Windows Server 2016 i Windows Server 2019: .NET 3.51 i .NET 4.8 (obejmuje .NET 4.0)

Minimalne wymagania sprzętowe	– Intel i5 lub nowszy
	– 8 GB RAM (16 GB — zalecane)
	– 20 GB wolnego miejsca na dysku twardym
	– Karta graficzna
	  – 256 MB pamięci RAM,
	  – Rozdzielczość 1280x1024
	  – at least 32 k colors
	  – OpenGL® 2.1 i DirectX® 11
	– Karta Ethernet 100 Mbit

Dodatkowe wymagania minimalne dla klientów VIE (Video Engine)	– System operacyjny inny niż Windows Server – Procesor Intel i5 lub nowszy – Dodaj 4 GB RAM-u na potrzeby sekwencjonowania kamery, matrycy wirtualnej lub układu wielowidokowego – Zaleca się korzystanie z najnowszych sterowników wideo. Użyj narzędzia diagnostycznego DxDiag systemu Windows, aby się upewnić, czy sterowniki nie są stare (tzn. mają więcej niż 1 rok).

Uwaga!
Zaleca się, aby nie używać serwera logowania systemu BIS ani serwerów połączeń jako klientów VIE, aby wykluczyć możliwe konflikty z innymi komponentami wideo.

3.3 Sprzęt do obsługi specjalnych funkcji serwera

Funkcja serwera	Wymagany sprzęt
Praca sieciowa systemu (dodatkowe komputery zdalne, drukarki sieciowe, komputery sterujące w sieci lokalnej)	Jedna karta sieciowa Ethernet na sieć (podsystemy OPC i stacje robocze mogą funkcjonować w oddzielnych sieciach).
Obsługa jednego monitora	Karta graficzna VGA do obsługi jednego monitora
Obsługa wielu monitorów (maks. czterech)	Karta graficzna (karty graficzne) VGA do obsługi pożądanej liczby monitorów
Podsystemy i systemy zewnętrzne, takie jak sprzęgacze magistrali (połączenia pozasieciowe)	Jeden port COM interfejsu szeregowego na połączenie (na płycie lub na karcie rozszerzeń)

Funkcja serwera	Wymagany sprzęt
Dodatkowe drukarki raportów lub alarmów	Jeden interfejs szeregowy lub równoległy, zależnie od drukarki (na płycie lub na karcie rozszerzeń). Możliwe jest również drukowanie sieciowe.
Urządzenia zewnętrzne, np. urządzenie pamięci masowej do tworzenia kopii zapasowych	Odpowiednie kontrolery

3.4 Przegląd procesu instalacji

Instalacja systemu BIS składa się na ogół z następujących etapów, które opisano w dalszej części dokumentu.

1. Konfigurowanie sieci — rozdział *Konfigurowanie sieci, Strona 15*
2. Konfigurowanie serwera bazy danych — rozdział *Przygotowywanie serwera bazy danych, Strona 18*
3. Instalowanie oprogramowania BIS na serwerze systemu BIS:
   - po raz pierwszy — rozdział *Realizacja pierwszej instalacji, Strona 15* lub
   - uaktualnianie — rozdział *Realizacja instalacji uaktualniającej, Strona 35*.
4. Instalowanie/konfigurowanie zapory — rozdział *Konfigurowanie zapory, Strona 33*.
5. Konfigurowanie serwerów DCOM i OPC na serwerze (serwerach) połączeń — rozdział *Konfigurowanie serwerów DCOM i OPC, Strona 34*.
6. Konfigurowanie przeglądarek internetowych na klientach — rozdział *Konfigurowanie klientów systemu BIS oraz narzędzi, Strona 41*.
7. Instalowanie w razie potrzeby dodatkowych narzędzi systemu BIS — rozdział *Instalowanie dodatkowych narzędzi systemu BIS, Strona 45*.
8. Licencjonowanie — rozdział *Licencjonowanie instalacji systemu BIS, Strona 47*.

4 Realizacja pierwszej instalacji

Poniżej przedstawiono zalecaną ogólną kolejność działań podczas pierwszej instalacji (sprzętu i oprogramowania) systemu BIS, choć nie wszystkie kroki będą konieczne w każdym przypadku:

1. konfigurowanie sieci komputerów, na których ma działać system BIS i jego baza (bazy) danych;
2. Przygotowywanie serwera bazy danych
3. instalowanie oprogramowania BIS na serwerze systemu BIS;
4. instalowanie/konfigurowanie zapory;
5. dostosowanie instalacji do specyfiki zastosowanych modułów.

Konfigurację ustawień DCOM dla wszelkich serwerów połączeń wchodzących w skład instalacji systemu BIS omówiono oddzielnie w rozdziale *Konfigurowanie serwerów DCOM i OPC, Strona 34*.

4.1 Konfigurowanie sieci

System BIS działa zazwyczaj w sieci TCP/IP składającej się z następujących elementów:

- **Serwer logowania systemu BIS.** Serwer obsługujący główną aplikację BIS jest również często określanym mianem **serwera logowania** lub **serwera systemu BIS**.
  - Należy pamiętać, że w skład wieloserwerowych systemów BIS może wchodzić więcej niż jeden serwer systemu BIS.
- Zero lub więcej serwerów połączeń**,** które komunikują się z urządzeniami peryferyjnymi, takimi jak detektory, przyzywowe wskaźniki alarmowe, wejścia i kamery wideo.
- Zero lub więcej **operatorskich stacji roboczych**, zwanych również **klientami systemu BIS**. Są to zazwyczaj komputery, na których uruchomiono w przeglądarce internetowej interfejs użytkownika systemu BIS.
- Zero lub więcej oddzielnych serwerów baz danych.

Należy pamiętać, że serwer systemu BIS może wykonywać funkcje serwera połączeń i stacji roboczej operatora, a także obsługiwać własne bazy danych, ale prosta topologia jest nieodpowiednia w przypadku dużych systemów, gdyż ogranicza to wydajność.

4.1.1 Podłączanie serwerów do sieci

Aby móc zarządzać wieloma systemami budynku, serwer systemu BIS jest na ogół podłączony do sieci. Urządzenia klienckie i podsystemy nie muszą być koniecznie podłączone do tej samej sieci, tzn. można jedną sieć przeznaczyć do obsługi podłączonych podsystemów, a drugą do obsługi komputerów klienckich systemu BIS.

Nazwy serwerów

Każdy komputer musi posiadać unikatową nazwę i unikatowy adres IP. W przypadku nazw serwerów obowiązują następujące ograniczenia:

- Nie więcej niż 15 znaków
- Pierwszym znakiem w nazwie nie może być cyfra
- Nie można używać znaków innych niż łacińskie oraz znaków diakrytycznych. Rekomendowana jest nazwa NetBIOS.

Połączenia z serwerami zdalnymi
Przed zainstalowaniem oprogramowania BIS muszą istnieć połączenia sieciowe ze wszystkimi **serwerami baz danych** (patrz *Przygotowywanie serwera bazy danych, Strona 18*), gdyż kreator instalacji może wymagać ich przejrzenia.
Serwery połączeń do obsługi procesów serwerów OPC można natomiast skonfigurować po zainstalowaniu oprogramowania BIS (informacje na ten temat można znaleźć w firmowej dokumentacji sprzętu oraz w rozdziale *Konfigurowanie serwerów DCOM i OPC, Strona 34* niniejszego dokumentu).

Możliwe są połączenia Ethernet typu 10, 100 lub 1000BaseT (skrętka). Do bezpośredniego łączenia ze sobą kart sieciowych należy stosować kabel bezmodemowy „krosowany”.

Uwaga!
Do celów instalacji należy wyłączyć wszystkie opcje oszczędzania energii typu „Stan gotowości” i „Hibernacja” na wszystkich komputerach, które wchodzą w skład systemu BIS (serwer logowania systemu BIS, serwery bazy danych, serwery połączeń, klienty systemu BIS).

Patrz
– *Konfigurowanie serwerów DCOM i OPC, Strona 34*

4.1.2 Zainstalowanie wymaganego oprogramowania Internet Information Services (IIS)

Oprogramowanie IIS musi zostać zainstalowane na serwerze systemu BIS przed zainstalowaniem aplikacji BIS. IIS to opcjonalny składnik systemu Windows — aby go zainstalować, może być konieczne skorzystanie z nośnika instalacyjnego systemu Windows. Nowy skrypt instalacyjny oprogramowania IIS `InstallIISForBIS.exe` jest dostępny na nośniku instalacyjnym systemu BIS w katalogu `Tools\InstallIISForBIS\`. Skrypt ten dokonuje wszystkich niezbędnych ustawień wymienionych w tabeli poniżej. Należy pamiętać, że skrypt ten wymaga środowiska .NET 4.0.
UWAGA: Jeśli nie zamierza się skorzystać z tego skryptu w celu zainstalowania oprogramowania IIS, należy pominąć funkcję CGI. W przeciwnym wypadku należy zadbać o to, aby instalacja oprogramowania IIS zawierała odpowiednio następujące ustawienia systemu Windows 10 bądź Windows 2016 lub 2019 Server.

Windows 10		**Windows 2016 Server i Windows 2019 Server**

Internet Information Services
..Narzędzia zarządzania siecią Web:
....Zgodność z narzędziami zarządzania usługami IIS w wersji 6
– [ustawienia]
  – Konsola zarządzania usługami IIS w wersji 6.0
  – Narzędzia obsługi skryptów w usługach IIS
  – Zgodność z narzędziami WMI usług IIS w wersji 6
		Serwer sieci Web
		..Wspólne funkcje HTTP:
		– Zawartość statyczna
		– Dokument domyślny
		– Przeglądanie katalogów
		– Błędy HTTP

Windows 10		**Windows 2016 Server i Windows 2019 Server**
– Zgodność z metabazą usług IIS 6 i z konfiguracją usług IIS 6 – Konsola zarządzania usługami IIS – Narzędzia i skrypty zarządzania usługami IIS – Usługa zarządzania usługami IIS		
Usługi WWW: **..Funkcje tworzenia aplikacji:** – [W systemach Windows 10] – ASP.NET 3.5 **i** – ASP.NET 4.6 – Rozszerzenia architektury .NET 3.5 – Rozszerzenia architektury .NET 4.6 – Rozszerzenia ISAPI – Filtry ISAPI		**..Projektowanie aplikacji:** – Rozszerzenia ISAPI – Filtry ISAPI
..**Wspólne funkcje HTTP:** – Dokument domyślny – Przeglądanie katalogów – Błędy HTTP – Zawartość statyczna		**..Stan i diagnostyka:** – Rejestrowanie HTTP – Monitor żądań
..Stan i diagnostyka: – Rejestrowanie HTTP – Monitor żądań		**..Zabezpieczenia:** – Uwierzytelnianie systemu Windows – Filtrowanie żądań – Ograniczenia adresów IP i domen
..Funkcje wydajnościowe: – Kompresja zawartości statycznej		**..Wydajność:** – Kompresja zawartości statycznej
..Zabezpieczenia: – Protokół IPSec – Filtrowanie żądań – Uwierzytelnianie systemu Windows		**Narzędzia do zarządzania:** – Konsola zarządzania usługami IIS – Narzędzia i skrypty zarządzania usługami IIS – Usługa zarządzania **....Zgodność z narzędziami zarządzania:** – – Zgodność z metabazą usług IIS 6 – Zgodność z narzędziami WMI usług IIS w wersji 6 – Narzędzia obsługi skryptów w usługach IIS w wersji 6 – Konsola zarządzania usługami IIS w wersji 6.0

Windows 10		Tylko Windows 2016 Server i Windows 2019 Server
.NET Framework 3.5 – Aktywacja usługi Windows Communication Foundation (WCF) w oparciu o protokół HTTP – Aktywacja usługi Windows Communication Foundation (WCF) w oparciu o protokół inny niż HTTP **Zaawansowane usługi platformy .NET Framework 4.5** (**4.6** dla systemu Windows 10)**, usługi WCF** – Aktywacja HTTP		**Funkcje platformy .NET Framework 3.5** – Aktywacja HTTP – Aktywacja w oparciu o protokół inny niż HTTP **Funkcje platformy .NET Framework 4.5, usługi WCF** – Aktywacja HTTP

Wyłączenie funkcji CGI oprogramowania IIS

Jeśli usługi ISS są już zainstalowane z funkcją CGI, należy wyłączyć tę funkcję w przypadku systemu Windows 10:

– Windows 10: **Start > Panel sterowania > Programy > Włącz lub wyłącz funkcje systemu Windows > Internet Information Services > Usługi WWW > Funkcje tworzenia aplikacji > CGI**

4.2 Przygotowywanie serwera bazy danych

Wstęp

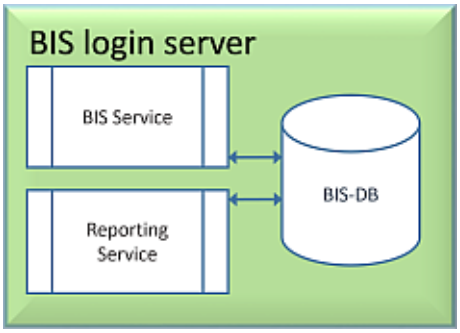
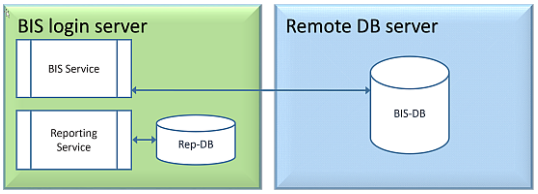
System BIS wymaga bazy danych Microsoft SQL Server i usługi raportowania.

– **Bazę danych SQL Server** można zainstalować na serwerze logowania systemu BIS lub na osobnym komputerze. Ten osobny komputer nosi nazwę zdalnego serwera bazy danych.
– **Usługę raportowania** można zainstalować na serwerze logowania systemu BIS lub na zdalnym serwerze bazy danych.

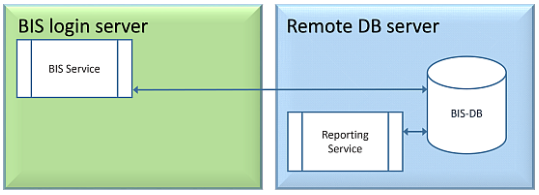
Omówienie topologii serwerów bazy danych

Ze względu na to, że każde z tych dwóch składników można zainstalować zdalnie lub lokalnie (na serwerze logowania systemu BIS), istnieją 2 x 2 = 4 możliwe topologie serwera bazy danych.

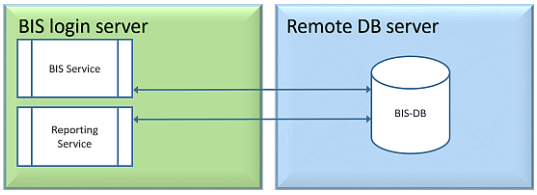
Aby kontynuować, należy wybrać jedną z 4 topologii serwera bazy danych.

1. Baza danych i usługa raportowania na komputerze serwera logowania systemu BIS Jest to najprostsza instalacja i odpowiednia dla małych systemów.  	**2. Sama baza danych na zdalnym serwerze SQL. Usługa raportowania wraz z własną bazą danych na serwerze logowania systemu BIS.** 

3. Baza danych i usługa raportowania na zdalnym serwerze SQL
Jest to najbardziej złożona topologia do skonfigurowania, ale pozwala na najlepszą wydajność serwera logowania systemu BIS. W przypadku korzystania z certyfikatów z podpisem własnym należy rozdzielić dwa certyfikaty z podpisem własnym: certyfikat serwera logowania systemu BIS i certyfikat usługi raportowania.



4. Licencjonowana sama baza danych na zdalnym serwerze SQL, usługa raportowania na serwerze logowania systemu BIS z użyciem zdalnej bazy danych.
W przypadku korzystania z certyfikatów z podpisem własnym należy przydzielić tylko jeden z nich: tj. certyfikat serwera logowania systemu BIS.



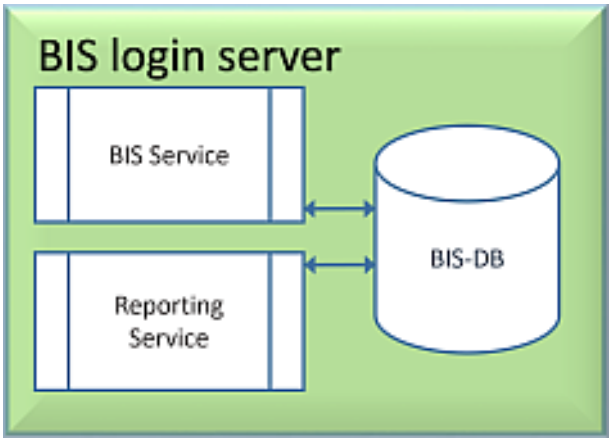
W tym rozdziale opisano następujące procedury:
- Instalowanie i publikowanie bazy danych SQL Server
- Instalowanie i konfigurowanie usługi SQL Server Reporting Service
- Przygotowanie zdalnego serwera baz danych do dostępu z systemu BIS.
- Zabezpieczanie zdalnej usługi raportowania

Wybór topologii serwerów baz danych (1-4) określa, które z procedur należy wykonać.

Uwaga!
PRZED uruchomieniem konfiguracji systemu BIS na serwerze logowania systemu BIS należy wykonać odpowiednie procedury dla wybranej topologii.

4.2.1 Procedury konfigurowania topologii serwera bazy danych

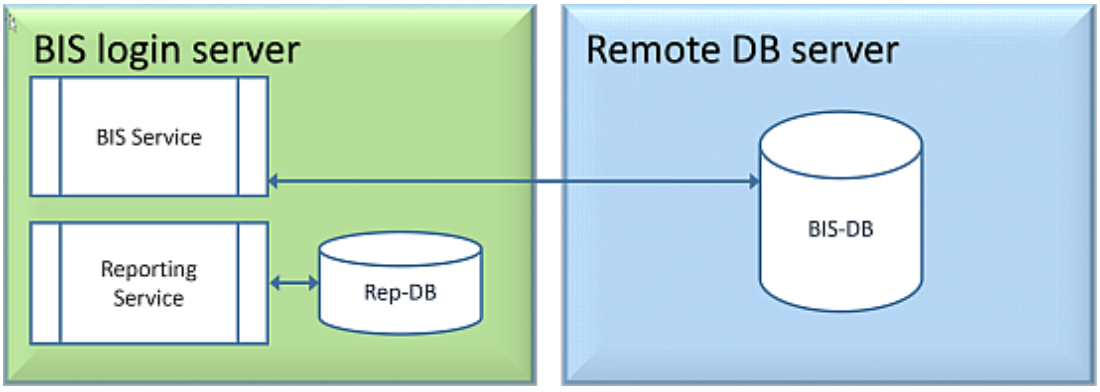
Topologia 1: baza danych i usługa raportowania uruchomione na komputerze serwera logowania systemu BIS



Aby korzystać z bezpłatnej wersji SQL Server Express Edition, która jest oferowana przez system BIS, nie trzeba stosować żadnych dodatkowych czynności przygotowawczych. Instalacja systemu BIS spowoduje utworzenie wymaganych instancji serwera SQL. Możesz przejść punktu *Instalowanie oprogramowania BIS na serwerze logowania systemu BIS, Strona 28*
Jeśli chcesz korzystać z licencjonowanej wersji SQL Server w celu zwiększenia pojemności, przed zainstalowaniem oprogramowania BIS wykonaj następujące procedury:
Procedura 1: *Instalowanie i publikowanie baz danych SQL Server na serwerach bazy danych, Strona 23*
Procedura 2: *Instalowanie i konfigurowanie usługi SQL Server Reporting Service, Strona 24*
Zakończenie: *Ostateczne kroki przed rozpoczęciem instalacji na serwerze logowania:, Strona 28*

Podczas instalacji oprogramowania BIS musisz przejrzeć instancje bazy danych i wybrać tę, która zostanie utworzona w ramach tych procedur.

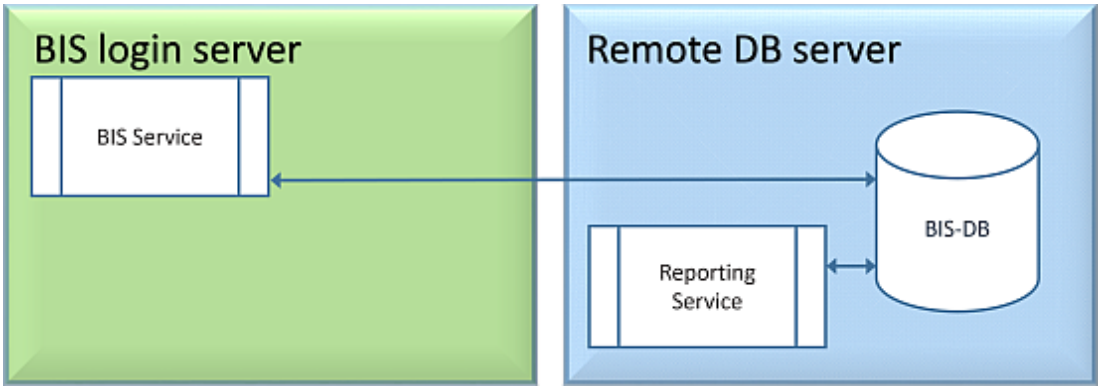
Topologia 2: pojedyncza baza danych na zdalnym serwerze SQL. Usługa raportowania wraz z własną bazą danych na serwerze logowania systemu BIS.



Na zdalnym komputerze SQL Server można korzystać z licencjonowanego serwera SQL lub wersji Express Edition.
Przed zainstalowaniem oprogramowania BIS należy wykonać następujące procedury:
Procedura 1: *Instalowanie i publikowanie baz danych SQL Server na serwerach bazy danych, Strona 23*
Procedura 2: *Przygotowanie zdalnego serwera baz danych do dostępu z systemu BIS, Strona 25*
Zakończenie: *Ostateczne kroki przed rozpoczęciem instalacji na serwerze logowania:, Strona 28*

Podczas instalacji oprogramowania BIS należy przejrzeć i wybrać wystąpienia bazy danych dla systemu BIS i ACE, które zostały utworzone w Procedurze 1.
W późniejszym kroku instalacji kliknij przycisk **Utwórz**, aby utworzyć nowe wystąpienie usługi raportowania na serwerze logowania systemu BIS.

Topologia 3: usługa baz danych i raportowania na zdalnym serwerze SQL

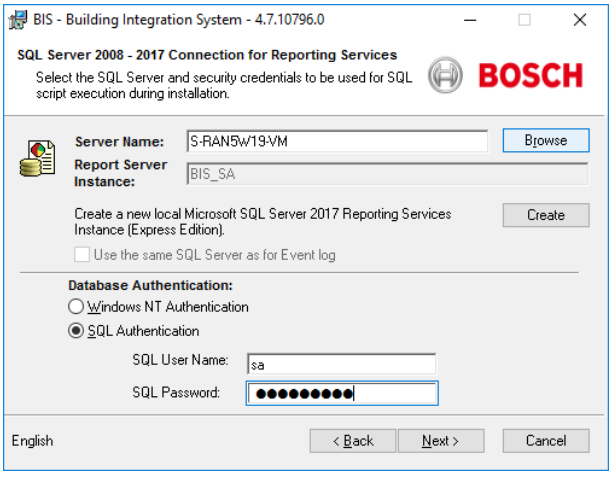


Na zdalnym komputerze SQL Server można korzystać z licencjonowanego serwera SQL lub wersji Express Edition.

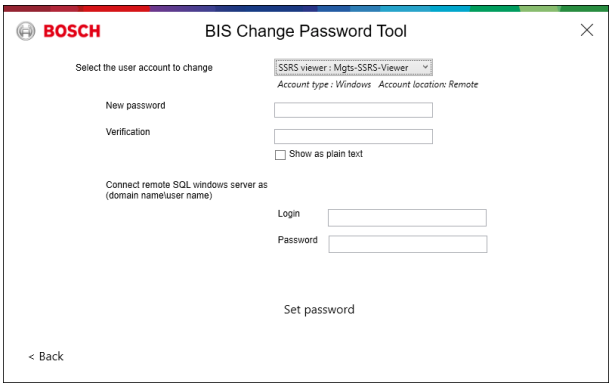
Przed zainstalowaniem oprogramowania BIS należy wykonać następujące procedury:
Procedura 1: *Instalowanie i publikowanie baz danych SQL Server na serwerach bazy danych, Strona 23*
Procedura 2: *Instalowanie i konfigurowanie usługi SQL Server Reporting Service, Strona 24*
Procedura 3: *Przygotowanie zdalnego serwera baz danych do dostępu z systemu BIS, Strona 25*
Procedura 4: *Zabezpieczenie usługi raportowania na zdalnym serwerze bazy danych, Strona 27*
Zakończenie: *Ostateczne kroki przed rozpoczęciem instalacji na serwerze logowania:, Strona 28*

Podczas instalacji oprogramowania BIS musisz przejrzeć instancje bazy danych i wybrać te, które zostaną utworzone w ramach tych procedur.

– W przypadku używania Access Engine należy wprowadzić nazwę zdalnego serwera bazy danych i kliknąć przycisk **Przeglądaj**, aby wybrać wystąpienie bazy danych ACE.
– W przypadku usług raportowania należy wprowadzić nazwę zdalnego serwera SQL, klikając go, a następnie kliknąć przycisk **Przeglądaj** i wybrać wymaganą instancję na potrzeby zdalnej usługi raportowania
  UWAGA: nie należy klikać przycisku **Utwórz** , ponieważ spowoduje to utworzenie nowego wystąpienia usługi raportowania.

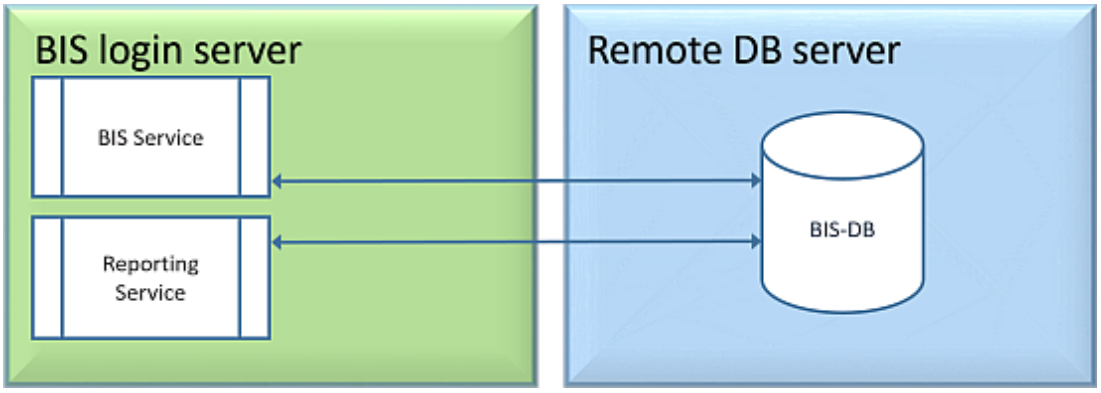


Ważna uwaga dotycząca topologii 3:
po pomyślnym zainstalowaniu na komputerze z serwerem logowania systemu BIS należy uruchomić narzędzie do zmiany hasła systemu BIS (`C:\MgtS\Tools\ChangePassword`), aby zmienić hasło do **przeglądarki Mgts-SSRS**. Nie jest wymagane stare hasło, jeśli narzędzie zostało uruchomione jako administrator.



Topologia 4: licencjonowana sama baza danych na zdalnym serwerze SQL, usługa raportowania na serwerze logowania systemu BIS z użyciem zdalnej bazy danych.

Topologia 4 jest zalecana, jeśli planujesz użycie certyfikatu z podpisem własnym, utworzonego przez system BIS, na potrzeby zdalnego wystąpienia SQL. Dzieje się tak, ponieważ musisz pobrać i zainstalować tylko jeden certyfikat z podpisem własnym. Jeden certyfikat obejmuje usługę BIS i usługę raportowania na serwerze logowania.



– Na zdalnym serwerze baz danych należy korzystać z licencjonowanej wersji SQL Server.
– Na komputerze serwera logowania systemu BIS użyj licencjonowanej wersji usługi raportowania

Przed zainstalowaniem oprogramowania BIS należy wykonać następujące procedury:
Procedura 1: *Instalowanie i publikowanie baz danych SQL Server na serwerach bazy danych, Strona 23*
Procedura 2: *Przygotowanie zdalnego serwera baz danych do dostępu z systemu BIS, Strona 25*
Procedura 3: **na serwerze logowania systemu BIS**: *Instalowanie i konfigurowanie usługi SQL Server Reporting Service, Strona 24*
Zakończenie: *Ostateczne kroki przed rozpoczęciem instalacji na serwerze logowania:, Strona 28*

Podczas instalacji oprogramowania BIS należy przejrzeć i wybrać zdalne wystąpienie serwera SQL, a następnie wybrać usługę raportowania, która jest lokalna (na serwerze logowania systemu BIS).

Patrz

- *Instalowanie oprogramowania BIS na serwerze logowania systemu BIS, Strona 28*
- *Instalowanie i publikowanie baz danych SQL Server na serwerach bazy danych, Strona 23*
- *Instalowanie i konfigurowanie usługi SQL Server Reporting Service, Strona 24*
- *Przygotowanie zdalnego serwera baz danych do dostępu z systemu BIS, Strona 25*
- *Zabezpieczenie usługi raportowania na zdalnym serwerze bazy danych, Strona 27*
- *Instalowanie i konfigurowanie usługi SQL Server Reporting Service, Strona 24*

4.2.2 Instalowanie i publikowanie baz danych SQL Server na serwerach bazy danych

Zdalne serwery bazy danych są używane w topologiach 2-4.

Przygotowanie komputera serwera bazy danych

Komputer serwera bazy danych:

- W topologii 1 jest to serwer logowania systemu BIS.
- W topologii 2-4 zdalny serwer bazy danych

Uwaga!

Zawsze należy używać najnowszych wersji i pakietów Service Pack w wersji SQL Server.

1. Upewnij się, że nazwa hosta jest dłuższa niż 15 znaków (zgodnie z regułami systemu Microsoft NETBIOS)
2. Upewnij się, że **administrator** użytkowników ma hasło.
3. Uruchom ponownie komputer z serwerem bazy danych i zaloguj się jako **administrator**.
4. Upewnij się, że zainstalowany jest system .NET 4.8 (lub nowszy). NIE należy próbować kontynuować pracy z wcześniejszą wersją.
5. Wyłącz dowolną opcję automatycznego oszczędzania energii.
6. Wyłącz zaporę sieciową. Zapora musi pozostać wyłączona podczas instalacji. Po zakończeniu instalacji należy ją ponownie aktywować zgodnie z opisem w dokumencie *BIS_Firewall_Configuration.pdf*

Instalowanie SQL Server na komputerze serwera bazy danych

1. Zdecyduj, czy chcesz używać wersji Express systemu SQL 2017 (dostarczonej na nośniku instalacyjnym systemu BIS <nośnik instalacyjny systemu BIS>*\3rd_Party \SQL2017\1033\)* czy własnej licencjonowanej wersji.
2. Uruchom odpowiedni plik *setup.exe*
3. Kliknij przycisk **OK** , gdy pojawi się monit o zmianę podstawowej roli na nowszą platformę i instalator.
   Poczekaj, aż pojawi się **Centrum instalacji**.
4. Wybierz kartę „**Instalacja**” na pasku menu z lewej strony
5. Kliknij „**Nowa autonomiczna instalacja SQL Server lub dodaj funkcje do istniejącej instalacji**”"

6. Kliknij **Dalej** , aby sprawdzić pliki instalacyjne, a proces konfiguracji zainstaluj pliki pomocnicze automatycznie
7. Wybierz „**Wykonaj nową instalację systemu SQL Server 2017**”
8. Zaakceptuj warunki umowy licencyjnej i kliknij **Dalej**
9. Wybierz „*Database Engine Services*" w obszarze **Funkcje instancji**
10. Podaj nazwaną instancję (na przykład: *BIS* lub *BISACE*), nie podawaj nazwy samego komputera ani **nie** podawaj domyślnej nazwy instancji „*SQLExpress*”.
11. Aby kontynuować, kliknij **Dalej**.
12. Jako „**Nazwę konta**” dla silnika bazy danych SQL Server wprowadź *NT AUTHORITY \SYSTEM* i zostaw hasło puste
13. Zmień „**Typ uruchomienia** ” na *Automatic* dla „**Silnik bazy danych SQL**” i „**Przeglądarka SQL Server**”
14. Wybierz *Mixed Mode* dla „**Authentication Mode**” i wprowadź silne hasło dla użytkownika „**sa**” zgodnie z zasadami dotyczącymi haseł.

– Dokładnie zanotuj hasło sobie **sa**, gdyż będzie ono wymagane przy instalacji systemu BIS.

15. W obszarze **Określ administratorów SQL Server**: dodaj co najmniej jednego użytkownika systemu Windows lub najlepiej grupę użytkowników, która będzie uprawniona do zarządzania SQL Server, np. Administrator lub Administratorzy
16. Aby rozpocząć instalację, kliknij przycisk **Dalej**.

– Po zakończeniu instalacji upewnij się, że pojawi się komunikat „**Instalacja udana**”

Opublikowanie instancji SQL, aby była widoczna w sieci podczas instalacji oprogramowania BIS.

1. Kliknij **Start** > **Microsoft SQL Server 2017** > **menedżer konfiguracji SQL server 2017**
2. Rozwiń „**SQL Server Network Configuration**” i wybierz Protokoły dla <INSTANCJI>, włącz „**Nazwane potoki**” i „**TCP/IP**”; <INSTANCJA> zostanie podana podczas konfiguracji SQL, na przykład: *BIS/BISACE*
3. Włącz „**Nazwane potoki**” i „**TCP/IP**” dla SQL Native Client, protokoły klienta.
4. Kliknij prawym przyciskiem myszy „**Protokoły dla** <INSTANCJI>**”,** wybierz **„Właściwości”** i wybierz kartę **„Flagi”.** W tym obszarze ustaw **„Wymuszaj szyfrowanie”** na **„***Yes***”,** aby włączyć szyfrowaną komunikację między serwerem systemu BIS a serwerem SQL.
5. W obszarze **Usługi SQL Server** > **Przeglądarka SQL Server** > **Właściwości** > **Usługa** upewnij się, że „**Tryb uruchamiania**” usługi „**Przeglądarka SQL Server**” jest *automatic*.
6. Uruchom ponownie komputer.

Instalowanie drugiego wystąpienia modułu ACE

– W razie potrzeby w przypadku innych modułów, np. systemu ACE, należy powtórzyć procedury opisane w tym rozdziale, aby zainstalować więcej instancji SQL.

4.2.3 Instalowanie i konfigurowanie usługi SQL Server Reporting Service

Na komputerze, na którym ma działać usługa raportowania, wykonaj następujące procedury:

Instalowanie usługi raportowania

1. Otwórz lokalizację pliku wykonywalnego usługi raportowania, albo wersję Express dostarczoną wraz z <nośnikiem instalacyjnym>*\3rd_Party\SQL2017*” systemu BIS lub lokalizację usługi raportowania z oddzielną licencją.
2. Z tej lokalizacji kliknij prawym przyciskiem myszy *SQLServerReportingServices.exe* i uruchom jako administrator

– Zostanie otwarte okno kreatora konfiguracji usługi **SQL Server Reporting Service**.
3. Wykonaj poszczególne etapy instalacji
4. Po instalacji uruchom ponownie komputer.

Konfigurowanie usługi raportowania
1. Otwórz okno poleceń systemu DOS jako administrator
2. Zmień katalog na jeden z następujących:
– <Nośnik instalacyjny systemu BIS>*\3rd_Party\SQL2017* lub
– lokalizacja usługi raportowania.
3. W tej lokalizacji należy wykonać następujące polecenie, a następnie zastąpić je nazwa komputera i instancji:

DOS> *RSConfig.exe -c -s [DBMachineName]\[InstanceName] -d ReportServer$[InstanceName] -a Windows -i SSRS*

– *DBMachineName* — komputer, na którym tworzona jest instancja SQL
– *InstanceName* — nazwa podawana podczas tworzenia instancji SQL
– Na przykład:
– Jeśli system SQL jest zainstalowany w komputerze „*SGPBISSQLSERVER*” i nazwą instancji jest „*BIS*”, to polecenie będzie brzmieć:
RSConfig.exe -c -s SGPBISSQLSERVER\BIS -d ReportServer$BIS -a Windows -i SSRS

Kończenie instalacji
1. Kreator wyświetla komunikat potwierdzający.
2. Uruchom *services.msc* i upewnij się, że *SQLServerReportingServices* działa na zainstalowanym komputerze. Jeśli nie, uruchom usługę ręcznie.

4.2.4 Przygotowanie zdalnego serwera baz danych do dostępu z systemu BIS

Tworzenie konta użytkownika na potrzeby tworzenia kopii zapasowych i przywracania
Na zdalnym serwerze bazy danych utwórz usługę **MgtS-Service** użytkownika z następującymi ustawieniami:
– **Nazwa użytkownika** (z uwzględnieniem wielkości liter): *MgtS-Service*
– **Hasło** : ustaw hasło zgodnie z zasadami bezpieczeństwa i zanotuj je dokładnie tak, jak będzie wymagane w konfiguracji systemu BIS na serwerze logowania.
– **Członek grupy**: *Administrators*
– Usuń zaznaczenie pola wyboru **Użytkownik musi zmienić hasło przy następnym logowaniu**
– Zaznacz pole wyboru **Użytkownik nie może zmienić hasła**
– Zaznacz pole wyboru **Hasło nigdy nie wygasa**
– Wyczyść pole wyboru **Konto jest wyłączone**

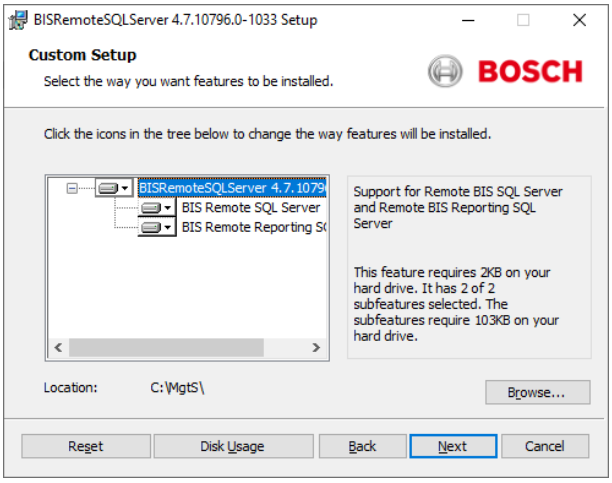
Usługa **MgtS-Service** użytkownika wymaga również uprawnień do logowania się w trybie usługi:
1. Uruchom *secpol.msc* z menu Start systemu Windows.
2. W narzędziu przejdź do **Ustawień zabezpieczeń** > **Zasady lokalne** > **Przypisanie praw użytkownika**
3. W okienku **Zasad** kliknij prawym przyciskiem myszy pozycję **Zaloguj się w trybie usługi** i wybierz **Właściwości**
4. W wyświetlonym oknie kliknij **Dodaj użytkownika lub grupę**

5. Dodaj <NameOfRemoteDBServer>*MgtS-Service*
6. Kliknij **OK**, aby potwierdzić i zamknąć program

Uruchomienie instalacji zdalnego serwera SQL

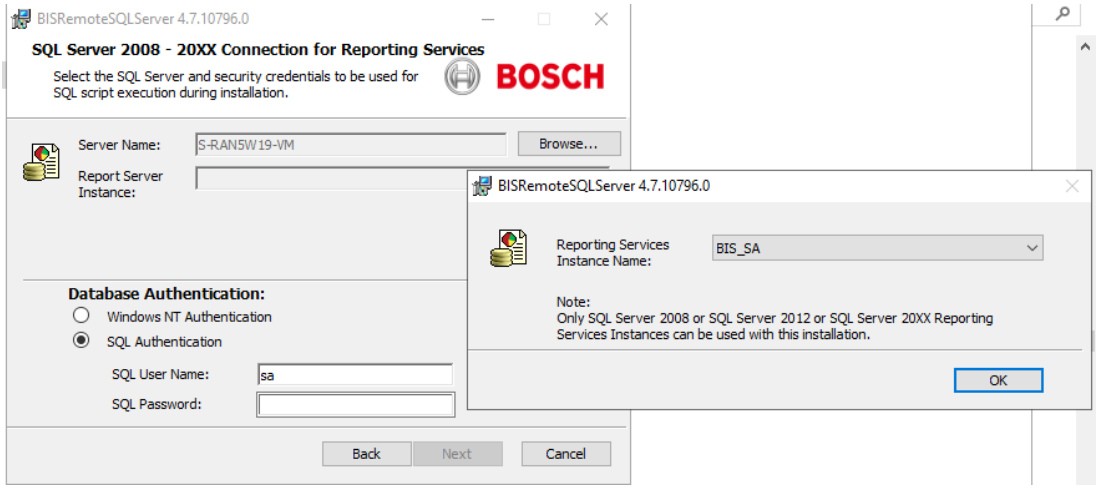
Na zdalnym serwerze bazy danych:

1. Zainstaluj następujące pakiety z nośnika instalacyjnego systemu BIS w obszarze <Nośnik instalacyjny>*3rd_Party\SQL2017\SMO*
   - *SQLSysClrTypes.msi*
   - *Sqlncli.msi*
2. Skopiuj zawartość z lokalizacji Nośnik instalacyjny>*3rd_Party\SQLSMO2017* do *C:\Windows\SysWOW64*
3. Kliknij prawym przyciskiem myszy i uruchom jako administrator plik instalacyjny *install.exe* w obszarze <Nośnik instalacyjny>*:*\<Language_ID>*\BIS\Tools\BISRemoteSQLServerSetup*
4. Podczas instalacji należy wybrać **jedną lub obie** funkcje „SQL Server” i „Reporting SQL Server”



- Aby używać zdalnego serwera SQL do jako **rejestru zdarzeń, DB9000, dziennika audytowego i/lub Access Engine**, wybierz funkcję *BIS Remote SQL Server*
- Ponadto, jeśli chcesz używać zdalnego serwera SQL do obsługi usług **Reporting Services**, wybierz funkcję *BIS Remote Reporting SQL Server*

5. Wyszukaj i wybierz wystąpienie usługi raportowania



6. Użyj uwierzytelniania SQL z nazwą użytkownika *sa* i hasłem zanotowanym w trakcie instalacji.

7. Kliknij przycisk **Dalej** i kliknij przycisk **Instaluj** na następnej stronie, aby wykonać instalację
8. Po zakończeniu instalacji uruchom ponownie zdalny komputer serwera bazy danych.

Uwaga!
Tylko jedna instalacja systemu BIS na zdalnym serwerze bazy danych
Komputer zdalnej bazy danych używany do obsługi usług Reporting Services może obsługiwać tylko jedną instalację systemu BIS.

Uwaga!
Nazwa instancji i nazwa komputera
Należy zadbać o to, aby nazwa instancji bazy danych nie przekraczała 15 znaków i nie pokrywała się z nazwą komputera.

4.2.5 Zabezpieczenie usługi raportowania na zdalnym serwerze bazy danych

Gdy usługa raportowania działa na zdalnym serwerze bazy danych, serwer logowania systemu BIS i klienci systemu BIS wymagają certyfikatu od usługi raportowania, aby umożliwić mu bezpieczne uzyskanie dostępu za pośrednictwem sieci.
Można używać zarówno certyfikatów z podpisem własnym, jak podpisane przez urząd certyfikacji. Poniższe procedury opisują sposób tworzenia i wdrażania:
– Certyfikaty z podpisem własnym
– Certyfikaty podpisane przez urząd certyfikacji

Certyfikaty z podpisem własnym

1. Na zdalnym serwerze baz danych uruchom następujący *.BAT* z nośnika instalacyjnego, aby utworzyć certyfikat z podpisem własnym i powiązać z adresem URL usługi raportowania
   _Install\3rd_Party\RemoteReportingService \create_remote_sql_certificate.bat
2. Wyeksportuj i zainstaluj ten certyfikat z podpisem własnym jako zaufany certyfikat główny na serwerze systemu BIS i wszystkich komputerach klienckich.
– Szczegółowe instrukcje można znaleźć w temacie *Konfigurowanie certyfikatu z podpisem własnym za pomocą usługi raportowania systemu BIS, Strona 42*.
3. Dodaj adres URL HTTPS zdalnego serwera bazy danych jako zaufaną witrynę na serwerze logowania systemu BIS oraz na wszystkich klientach, które będą korzystać z usługi raportowania.
– Na przykład, jeśli zdalny serwer bazy danych nazywa się *MyRemoteDBServer*, przejdź do menu ustawień Internet Explorer > **Opcje internetowe** > karta: **Zabezpieczenia** > **Zaufane witryny** > przycisk: **Witryny**
  i dodaj witrynę *HTTPS://MyRemoteDBServer*

Certyfikaty podpisane przez urząd certyfikacji

Jeśli masz certyfikat podpisany przez urząd certyfikacji, nie musisz tworzyć certyfikatu z podpisem własnym. Zamiast tego należy powiązać certyfikat podpisany przez urząd certyfikacji z adresem URL usługi raportowania.
Szczegółowe instrukcje można znaleźć w temacie *Aktualizowanie powiązania usługi raportowania, Strona 39*.

4.2.6 Ostateczne kroki przed rozpoczęciem instalacji na serwerze logowania:

- Aby umożliwić systemowi BIS wykonywanie kopii zapasowych i przywracanie ich baz danych, należy się upewnić, że serwer logowania systemu BIS ma tego samego użytkownika systemu Windows do administrowania bazami danych i takim samym hasłem.
- W oknach dialogowych instalacji systemu BIS wybierz odpowiednie instancje SQL Server dla dziennika zdarzeń, DB9000, dziennika audytowego i/lub Access Engine.
- Wprowadź wcześniej ustawione hasło **sa** zanotowane w trakcie serwera SQL na komputerze zdalnego serwera baz danych w korku *Instalowanie i publikowanie baz danych SQL Server na serwerach bazy danych, Strona 23*
- W oknie dialogowym, w którym wprowadza się instancję SQL Server dla usług Reporting Services, należy wprowadzić nazwę zdalnego serwera bazy danych i kliknąć przycisk „**Przeglądaj**”, aby wyświetlić wszystkie dostępne wystąpienia serwera SQL z usługami raportowania.
- Wybierz tę samą instancję, która została wybrana w trakcie wykonywania pliku `install.exe` w sekcji *Uruchomienie instalacji zdalnego serwera SQL, Strona 26*
- Uwaga: w przypadku topologii 2 wprowadź komputer serwera logowania systemu BIS i kliknij przycisk **Utwórz**, aby utworzyć nową usługę raportowania na komputerze lokalnym.

Patrz

- *Instalowanie i publikowanie baz danych SQL Server na serwerach bazy danych, Strona 23*
- *Przygotowanie zdalnego serwera baz danych do dostępu z systemu BIS, Strona 25*
- *Przygotowanie zdalnego serwera baz danych do dostępu z systemu BIS, Strona 25*

4.3 Instalowanie oprogramowania BIS na serwerze logowania systemu BIS

Zanim zaczniesz

Upewnij się, że ma zastosowanie jeden z poniższych warunków:

- Instalowane są wszystkie składniki systemu na serwerze logowania systemu BIS z bezpłatnym systemem MS SQL Server Express Edition.
- Skonfigurowano jedną z topologii bazy danych opisanych w poprzednim rozdziale *Przygotowywanie serwera bazy danych, Strona 18*

W celu dokonania instalacji skorzystaj z konta z uprawnieniami lokalnego administratora, najlepiej z samego konta **Administrator**. Sprawdź, czy serwer ma adres IP poprzez wpisanie w wierszu polecenia słowa **ipconfig**. Należy też mieć pod ręką nośnik instalacyjny systemu MS Windows, na wypadek gdyby kreator instalacji systemu BIS wymagał dodatkowych funkcji. Systemu BIS nie da się zainstalować, jeśli zapora jest aktywna. Kreator instalacji systemu BIS jest w stanie wyłączyć zaporę systemu Windows, jednak wszystkie inne zapory trzeba przed rozpoczęciem procedury instalacji systemu BIS wyłączyć ręcznie.

Uwaga!

Instalacja tylko na lokalnym komputerze

Zestaw instalacyjny systemu BIS może się znajdować na oddzielnym komputerze sieciowym, jednak plik setup.exe może zainstalować system BIS tylko na tym komputerze, z którego ten plik wywołano.

Uwaga!
Unikaj znaków specjalnych
W systemie BIS nie należy używać żadnych znaków specjalnych ani innych niż łacińskie (np. chińskich, rosyjskich, ä, é, ô, /, #, %, $, |, !, ~, ‘). Wolno używać jedynie innych niż znaki diakrytyczne znaków alfanumerycznych [A-z] i [0-9] (o 7-bitowym kodzie ASCII) oraz znaku podkreślenia.
Ta zasada dotyczy wszelkich znaków wpisywanych w kreatorze instalacji systemu BIS lub przeglądarce konfiguracji, w tym haseł.

Krok	Działanie	Efekt (efekty), uwagi, wyjaśnienia
1	Kliknij prawym przyciskiem myszy plik **setup.exe** i wybierz opcję **Run as administrator (Uruchom jako administrator)**.	Spowoduje to wyświetlenie okna dialogowego umożliwiającego dokonanie wyboru języka. **Uwagi:** – Oprócz języka niemieckiego i rosyjskiego, wszystkie instalacje wykonuje się obecnie w języku angielskim. – Aby prawidłowo wyświetlić znaki rosyjskie w innym niż rosyjski systemie operacyjnym, należy zmienić ustawienie regionalne systemu na rosyjski. – Po zainstalowaniu systemu BIS w określonym języku nie można już zmienić tego języka na inny w kolejnej instalacji uaktualniającej na tym samym komputerze.
2	Wybierz język interfejsu w swoim nowym systemie BIS i kliknij przycisk **Next (Dalej)**.	Spowoduje to wyświetlenie okna kreatora instalacji systemu BIS. Kreator przegląda zawartość komputera w poszukiwaniu oprogramowania wymaganego przez system BIS i odpowiednio dostosowuje plan instalacji. W zależności od tego, co jest już dostępne, kreator zaznaczy następujące wymagane oprogramowanie, które należy zainstalować wraz z systemem BIS: – Instalator Windows – Wymagane wersje platformy Microsoft .NET Framework. Należy pamiętać, że niezależnie od nośnika instalacyjnego systemu operacyjnego pojawi się monit o zainstalowanie platformy .NET Framework 3.5. – Obsługa obiektów SQL DMO/SMO
3	Kliknij przycisk **Next (Dalej)**.	Jeśli kreator instalacji wykryje aktywną zaporę Windows, kliknij opcję**Yes, I want to disable the Windows Firewall (Tak, chcę wyłączyć zaporę Windows)** i następnie kliknij przycisk **Next (Dalej)>**, aby ją wyłączyć. Aby móc kontynuować, trzeba ręcznie wyłączyć inne zapory poza procedurą instalacji systemu BIS.
		Domyślnie kreator instalacji instaluje na poziomie głównym lokalnego dysku C: katalog **MgtS**. Jeśli taka lokalizacja jest do przyjęcia, kliknij przycisk **Next (Dalej)**. Jeśli chcesz wybrać inną ścieżkę instalacji (tylko na dyskach lokalnych), kliknij przycisk **Browse (Przeglądaj)**.
		Spowoduje to wyświetlenie okna dialogowego Select Features (Wybierz funkcje).

Krok	Działanie	Efekt (efekty), uwagi, wyjaśnienia
4	Skorzystaj z okna wyboru funkcji, aby określić, które funkcje systemu BIS chcesz zainstalować.	Zaznacz tylko te moduły i połączenia, które zostały zakupione w firmie Bosch. Z innych funkcji nie da się korzystać bez uzyskania na nie licencji i będą one jedynie zajmować miejsce na dysku. Instalacja domyślna obejmuje wszystkie funkcje systemu BIS. Skorzystaj z menu rozwijanych, aby wykluczyć funkcje, których nie chcesz zainstalować.
5	Kliknij przycisk **Next (Dalej)**.	Następny etap procesu instalacji polega na skonfigurowaniu instancji bazy danych dla tych wybranych modułów i funkcji, które ich wymagają (dziennik zdarzeń/Security Engine, Access Engine i — w następnym kroku — usługi raportowania). Jeśli posiadasz już licencje na oprogramowanie SQL Server o dużej pojemności, możesz je wykorzystać dla potrzeb systemu BIS. W przeciwnym wypadku system BIS może zainstalować na Twoje potrzeby nowe instancje o ograniczonej pojemności (patrz: *Problemy ze zgodnością systemu SQL Server, Strona 31* poniżej). Istnieją 3 podstawowe możliwości dotyczące dostępności odpowiednich instancji systemu SQL Server, opisane poniżej jako **A**, **B** i **C**:

	Dostępność odpowiednich instancji systemu SQL Server		Działanie
A	Na serwerze logowania i w sieci brak jest odpowiedniej instancji **(*)** systemu SQL Server.	>	Kliknij przycisk **Create (Utwórz)**. System BIS skonfiguruje oddzielne instancje swojego obecnego systemu SQL Server Express Edition z zaawansowanymi usługami dla modułów: – dziennik zdarzeń/Security Engine (SEE tylko w razie potrzeby), – usługi raportowania, – Access Engine (w razie potrzeby).
B	Odpowiednią instancję **(*)** systemu SQL Server można znaleźć poprzez przejrzenie serwera logowania lub sieci.	>	Kliknij przycisk **Browse (Przeglądaj)**, aby wybrać instancję poprzez przeglądanie sieci.
C	Odpowiednia instancja **(*)** systemu SQL Server istnieje, ale nie można jej znaleźć poprzez przejrzenie serwera logowania lub sieci.	>	Wprowadź instancję ręcznie w polu tekstowym przeznaczonym na nazwę systemu SQL Server (SQL Server Name), stosując następującą składnię: **<nazwakomputera>\<nazwainstancji>**, np. MOJSERWER\MOJAINSTANCJA.

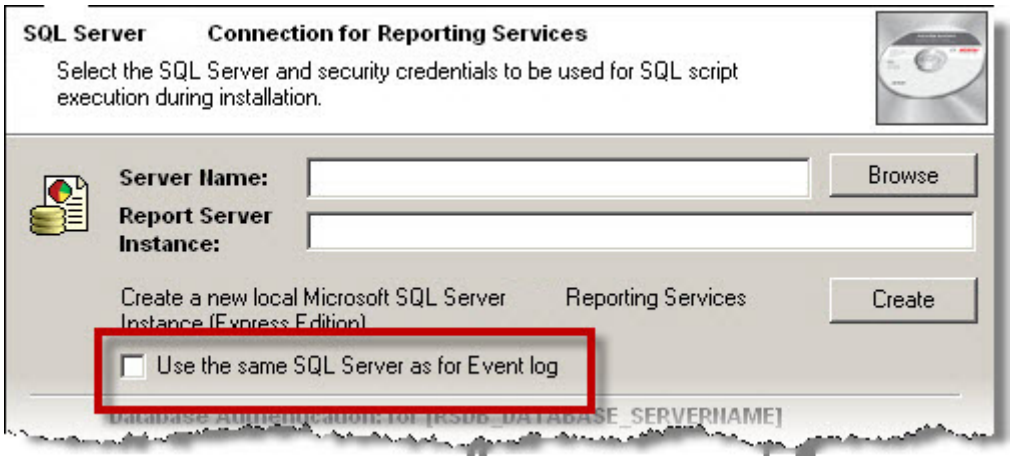
	Dostępność odpowiednich instancji systemu SQL Server		Działanie
	(*) Wyjaśnienie terminu „odpowiednia” można znaleźć w zastrzeżeniu *Problemy ze zgodnością systemu SQL Server, Strona 31* zamieszczonym poniżej.		

Problemy ze zgodnością systemu SQL Server

Uwaga!
Problemy ze zgodnością systemu SQL Server wywierające wpływ na wymienione powyżej opcje B (Browse (Przeglądaj)) i C (wprowadzanie ręczne) dotyczące tego systemu:
Niezgodne są następujące kombinacje:
Access Engine (ACE) z nienazwaną instancją (LOCAL) dowolnego systemu SQL Server.
Access Engine (ACE) z dziennikiem zdarzeń/Security Engine razem w tej samej instancji dowolnego systemu SQL Server Express Edition.
Usługi raportowania systemu BIS z wersjami systemu SQL Server poniżej wersji 2008.
Ogólnie system BIS z wersjami systemu SQL Server poniżej wersji 2005 SP2. Takie bazy danych trzeba uaktualnić ręcznie, zanim będzie można z nich korzystać z systemem BIS.
Wersje **systemu BIS** poniżej 4.3 z wersjami systemu SQL Server powyżej wersji SQL Server 2012 (system BIS pod kontrolą systemu Windows 10 Enterprise LTSB będzie obsługiwany jedynie z wersją SQL 2014).
Windows 2016 Server będzie obsługiwał następujące wersje systemu SQL Server:
2012 SP2,
2014 SP1
2016 SP2
2017
Windows 2019 Server będzie obsługiwał następujące wersje systemu SQL Server:
2014 SP1
2016 SP2
2017

Uwaga!
W przypadku instancji systemu BIS SQL Server zapewniających hosting modułu Access Engine (ACE) należy korzystać z **uwierzytelniania serwera SQL** a nie z uwierzytelniania systemu Windows. Jeśli przegląda się istniejące instancje ACE lub wchodzi do nich, w oknie dialogowym należy wprowadzić hasło „sa” tej instancji.
Wersja SQL Server Express Edition nie może wykorzystywać więcej niż 1 GB pamięci RAM i nie może obsługiwać baz danych zajmujących więcej niż 10 GB.

Krok	Działanie	Efekt (efekty), uwagi, wyjaśnienia
6	Podejmując opisane powyżej działania (A,B,C), skonfiguruj niezbędne instancje na potrzeby dziennika zdarzeń/SEE i modułu Access Engine.	**WAŻNE** — tylko podczas tworzenia **nowej** instancji bazy danych: jako konta administratora należy zawsze używać użytkownika `sa` . Kreator instalacji systemu BIS zachowa Twoje wybory dotyczące instalacji baz danych.

Krok	Działanie	Efekt (efekty), uwagi, wyjaśnienia
7	Podobnie wykorzystaj kreator instalacji systemu BIS do zlokalizowania w sieci instancji systemu Microsoft SQL Server na potrzeby usług raportowania systemu BIS.	**WAŻNA UWAGA**: Ten krok występuje tylko wtedy, gdy w kroku powyżej wybrano działanie **B lub C**, gdyż jeśli w poprzednim kroku utworzono nową instancję na potrzeby dziennika zdarzeń, wtedy w tej samej instancji zostaną automatycznie aktywowane usługi raportowania. Ta baza danych na potrzeby usług raportowania może stanowić oddzielną nazwaną instancję lub może współużytkować instancję wersji SQL 2012 SP2 lub nowszej z dziennikiem zdarzeń/SEE. – Aby utworzyć oddzielną instancję (np. jeśli w polu tekstowym z etykietą **Report Server Instance (Zgłoś instancję serwera)** nie pojawi się żadna nazwa), kliknij przycisk **Create (Utwórz)**. Wyświetlone wtedy zostanie wyskakujące okienko sugerujące nazwę **BISREPORTS**. Potwierdź (zalecane) lub zmień nazwę instancji i następnie kliknij przycisk **OK**, aby wrócić do poprzedniego okna i kontynuować instalację. – Aby szukać instancji systemu SQL Server w zdalnych węzłach, wprowadź ręcznie nazwę zdalnego węzła i kliknij przycisk **Browse (Przeglądaj)**. – Aby współużytkować instancję, zaznacz pole wyboru: **Use the same SQL Server as for Event Log (Użyj tej samej instancji systemu SQL Server, jak w przypadku dziennika zdarzeń)**.
		
8	Kliknij przycisk **Next (Dalej)**.	– Instalowany jest system SQL Server. – Instalowana jest aplikacja BIS. – Instalowane są wszystkie żądane bazy danych. – Kreator instalacji systemu BIS kończy instalowanie aplikacji.
9	Kliknij przycisk **Finish (Zakończ)**.	Spowoduje to otwarcie pliku **Mandatory Post Installation BIS.rtf**.

Krok	Działanie	Efekt (efekty), uwagi, wyjaśnienia
10	Przeczytaj zalecenia zamieszczone w tym pliku i postąp zgodnie z nimi, następnie zamknij okno.	Plik ten zawiera ważne informacje i instrukcje.
11	Aby zakończyć instalację systemu BIS, należy ponownie uruchomić komputer. W tym celu kliknij przycisk Yes (Tak).	Pierwsza instalacja aplikacji BIS została zakończona. Na pulpicie ukazała się ikona menedżera systemu BIS (BIS Manager).
12	Po zakończeniu instalacji kliknij kartę **License (Licencja)** w oknie BIS Configuration Manager (Menedżer konfiguracji systemu BIS), aby zainicjować procedurę licencjonowania.	Patrz *Licencjonowanie instalacji systemu BIS, Strona 47*.
13	Utwórz początkową konfigurację w menedżerze systemu BIS (BIS Manager).	Instrukcje można znaleźć w pomocy ekranowej konfiguracji systemu BIS. Aby uzyskać pomoc, kliknij klawisz F1 z poziomu menedżera systemu BIS (BIS Manager).

4.4 Konfigurowanie zapory

Różne wersje systemu Windows instalują własne zapory, które trzeba jedynie skonfigurować. Zainstaluj wszelkie inne zapory zgodnie z instrukcjami producenta. Skonfiguruj posiadaną zaporę (Windows lub innego producenta) pod kątem używania z systemem BIS, jak to opisano w pliku <installation_drive>:\MgtS\Platform\BIS_Firewall_Configuration.pdf.

4.5 Informacje poinstalacyjne dotyczące poszczególnych modułów

Różne moduły systemu BIS mogą wymagać dodatkowych ustawień, których trzeba dokonać po głównej instalacji systemu BIS. W tym celu skorzystaj z podręczników instalacji poszczególnych używanych modułów, zamieszczonych w odpowiednich podkatalogach katalogu <installation_drive>:\MgtS\.

5 Konfigurowanie serwerów DCOM i OPC

Z tym rozdziałem zapoznaj się tylko wtedy, gdy zamierzasz zainstalować serwery OPC, zwłaszcza innych producentów.

5.1 Informacje techniczne i wprowadzenie

Głównym zadanie aplikacji BIS na serwerze (logowania) systemu BIS jest gromadzenie informacji od procesów serwerów OPC i przekazywanie poleceń do tych procesów. Procesy te, zwane serwerami OPC, to standardowe interfejsy do szerokiej gamy urządzeń, np. do kontrolerów drzwi, alarmów pożarowych i kamer.
Procesy serwerów OPC są często realizowane nie na komputerze serwera systemu BIS, lecz na zdalnych komputerach zwanych **serwerami połączeń**. Komunikacja sieciowa pomiędzy serwerem systemu BIS a serwerem połączeń jest obsługiwana z wykorzystaniem protokołu DCOM (Distributed Common Object Model) oraz wspólnego konta użytkownika zwanego **MgtS-Service**. Serwer OPC przyjmuje więc tożsamość i dane uwierzytelniające konta użytkownika MgtS-Service.

Aby takie rozwiązanie mogło funkcjonować, należy poczynić następujące przygotowania:
- Na serwerze połączeń musi istnieć konto użytkownika MgtS-Service.
- Konto użytkownika MgtS-Service musi mieć wystarczające uprawnienia dostępowe, aby można było uruchamiać z jego poziomu różne programy i aktywować różne funkcje, zarówno lokalnie, jak i zdalnie.
- Należy wykonać procedurę instalacji serwera OPC, o ile jest dostępna. **Uwaga:** Procedury różnych producentów może cechować różny stopień złożoności. Wiele z nich będzie zawierać wymienione poniżej zadania, jednak niektóre z tych zadań trzeba będzie wykonać ręcznie (we wszystkich takich przypadkach należy skorzystać z dokumentacji danego serwera OPC):
  - zainstalowanie podstawowych składników serwera OPC;
  - przygotowanie protokołu DCOM do obsługi serwera OPC;
  - zainstalowanie serwera OPC;
  - skonfigurowanie z użyciem protokołu DCOM nowo zainstalowanego serwera OPC, np. tożsamości jego użytkownika (zazwyczaj ustawianej na MgtS-Service).

Procedury te są opisane w oddzielnym dokumencie zamieszczonym na nośniku instalacyjnym systemu BIS w pliku: **DCOM Configuration.pdf**

Łączenie serwerów OPC z instalacją systemu BIS
Serwery OPC różnią się znacznie pod względem złożoności, a w konsekwencji pod względem złożoności procedur ich łączenia z instalacją systemu BIS. Szczegółowe informacje na temat łączenia poszczególnych serwerów OPC można znaleźć w pomocy ekranowej **BIS Configuration Guide (Podręcznik konfiguracji systemu BIS)**.

6 Realizacja instalacji uaktualniającej

Uwaga!
Zgodność z istniejącymi panelami
Mogą występować konflikty wersji pomiędzy nową wersją systemu BIS a serwerami OPC różnych paneli przeciwpożarowych lub antywłamaniowych istniejących już w Twojej instalacji (np. paneli Bosch FPA lub MAP). Aby uniknąć takich konfliktów, firma Bosch zdecydowanie zaleca dokonanie uaktualnienia tych paneli do najnowszej wersji oprogramowania układowego jeszcze **przed** rozpoczęciem instalacji uaktualniającej system BIS.

Poniżej wymieniono istotne czynności, które należy wykonać podczas aktualizacji systemu BIS:

1. Zaplanuj ścieżkę uaktualnienia w zależności od posiadanej wersji początkowej, wersji docelowej i tego, czy korzystasz z modułu Access Engine. Zapoznaj się z tabelami ścieżek uaktualnienia przedstawionymi poniżej.
2. Zadbaj o uaktualnienie sprzętu, wymaganego oprogramowania i pliku licencji zgodnie ze specyfikacjami zamieszczonymi w sekcji *Informacje na potrzeby planowania, Strona 11* oraz o to, aby nie było żadnych niezgodności z Twoimi już istniejącymi bazami danych — patrz panel informacyjny „Problemy ze zgodnością systemu SQL Server” w sekcji *Instalowanie oprogramowania BIS na serwerze logowania systemu BIS, Strona 28*.
3. Zatrzymaj system BIS (i moduł ACE, jeśli jest zainstalowany)
4. Dokonaj wszelkich niezbędnych aktualizacji systemu SQL Server.
5. Uruchom program konfiguracji systemu BIS na serwerze systemu BIS.

Kroki te opisano bardziej szczegółowo w poniższych sekcjach.

6.1 Wymagania wstępne

W poniższych tabelach opisano obsługiwane ścieżki uaktualniania dla różnych wersji systemu BIS, zarówno z modułem Access Engine (ACE), jak i bez niego. Dalsze działania można podjąć tylko wtedy, gdy proponowana ścieżka uaktualniania jest obsługiwana. Uaktualnienie może wymagać realizacji w wielu krokach, patrz *Deinstalacja, Strona 49*.
Należy pamiętać, że instalacja uaktualniająca do najnowszej wersji systemu BIS zawsze usuwa poprzednie wersje, ale zapewnia ciągłość poprzez zachowanie konfiguracji oraz konwersję baz danych i zachowanie ich zawartości.
Niemniej jednak zapoznaj się z zamieszczonymi poniżej panelami **Uwag** dotyczącymi dostosowywania systemu MS SQL Server 2000 i usługi WCF.

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									✓

Uwaga!

*) MS SQL Server 2005

System Microsoft SQL Server 2014 z dodatkiem SP1 lub nowszy nie może dokonywać konwersji kopii zapasowych bazy danych bezpośrednio z wersji SQL Server sprzed wersji 2005 z dodatkiem SP3. Jeśli wciąż posiadasz kopie zapasowe bazy danych z przed wersji SQL Server 2005 z dodatkiem SP3, musisz najpierw dokonać wewnętrznego uaktualnienia do wersji BIS 2.5 (z systemem SQL Server 2008) i dopiero potem możesz uaktualnić to wersji BIS 4.x (z systemem SQL Server 2012).

Microsoft SQL Server 2005 z dodatkiem SP3 jest minimalną wersją wymaganą do uaktualnienia systemu do wersji Microsoft SQL Server 2014.

Uwaga!

Wieloserwerowy system BIS i dostosowane konfiguracje usługi WCF

Jeśli wprowadzasz ręcznie zmiany w pliku konfiguracji usługi WCF *\MgtS\Platform\BisClientProxyWcfServer\BisClientProxyWcfServer.exe.config* w wersji BIS 4.0, zostaną one również przeniesione do wersji BIS 4.1 i nowszych. Przed dostosowaniem tego pliku zapoznaj się ze specjalistyczną dokumentacją dostępną w pliku *\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 Uruchomienie kreatora instalacji systemu BIS na serwerze systemu BIS

Wykonać poniższą procedurę, aby uaktualnić istniejącą instalację systemu BIS bez utraty obecnych danych i plików konfiguracyjnych. W niniejszym opisie instalacji uaktualniającej zakłada się, że uaktualnia się działającą konfigurację systemu BIS oraz że sieć związanych z nią komputerów istnieje i prawidłowo funkcjonuje.

Krok	Działanie	Efekt (efekty), uwagi, wyjaśnienia
1	Utwórz kopię zapasową plików instalacyjnych systemu BIS lub utwórz obraz dysku twardego zawierającego instalację systemu BIS.	
2	Zamknij wszystkie okna systemu BIS i wyłącz serwer tego systemu.	

Krok	Działanie	Efekt (efekty), uwagi, wyjaśnienia
	Jeśli i tylko wtedy, gdy uaktualniasz system BIS 4.7 ORAZ używasz zdalnego serwera bazy danych, uruchom następujący plik wsadowy na zdalnym serwerze bazy danych:	
3	Włóż do serwera nośnik instalacyjny systemu BIS i wykonaj procedurę instalacyjną zgodnie z opisem zamieszczonym pod adresem *Instalowanie oprogramowania BIS na serwerze logowania systemu BIS, Strona 28*.	**Uwagi**: Aby zainstalować aktualizacje systemu BIS oraz podczas ponownego wykorzystywania instancji baz danych, administrator bazy danych nie musi już używać nazwy `sa` Instalacja uaktualniająca systemu BIS automatycznie aktualizuje również bazę danych dziennika zdarzeń. Kopie zapasowe baz danych z poprzednich wersji systemu BIS można zaktualizować poprzez naciśnięcie przycisku **DB Migration (Migracja bazy danych)** na karcie **Event Log (Dziennik zdarzeń)** menedżera systemu BIS (BIS Manager). Szczegółowe informacje na ten temat można znaleźć w pomocy ekranowej konfiguracji systemu BIS.
4	Po wyświetleniu w systemie BIS ekranu Select Features (Wybór funkcji) wybierz nowe funkcje systemu BIS, które chcesz zainstalować, a następnie zakończ instalację zgodnie z opisem zamieszczonym pod adresem *Instalowanie oprogramowania BIS na serwerze logowania systemu BIS, Strona 28*	
5	Spowoduje to otwarcie pliku **Mandatory post installation BIS.pdf**. Przeczytaj uważnie zalecenia zamieszczone w tym pliku, gdyż są one szczególnie ważne dla nowej wersji.	
6	Po zakończeniu instalacji kliknij kartę **License (Licencja)** w oknie BIS Configuration Manager (Menedżer konfiguracji systemu BIS), aby zainicjować procedurę licencjonowania.	Patrz *Licencjonowanie instalacji systemu BIS, Strona 47*.

Krok	Działanie	Efekt (efekty), uwagi, wyjaśnienia
7	Utwórz nową lub zaimportuj istniejącą konfigurację z poziomu menedżera systemu BIS (BIS Manager).	Szczegółowe instrukcje można znaleźć w pomocy ekranowej menedżera systemu BIS (BIS Manager) — w tym celu naciśnij klawisz F1 z poziomu tego menedżera.

6.3 Aktualizacja certyfikatu podpisanego przez urząd certyfikacji

Wstęp

Następujące 3 procedury są niezbędne tylko wtedy, gdy zakupiono zaktualizowany certyfikat urzędu certyfikacji.

- Zaktualizuj powiązanie IIS SSL (Internet Information Services Secure Sockets Layer) z nowym certyfikatem urzędu certyfikacji.
- Zaktualizuj powiązania usługi raportowania.
- Zaktualizuj „odcisk palca” certyfikatu podpisanego przez urząd certyfikacji w pliku konfiguracji **BISIdservice**.

Poniżej opisano wszystkie trzy procedury.

6.3.1 Aktualizowanie powiązania protokołu SSL usług IIS

Procedura

1. Uruchom **Menedżer usług Internet Information Services** z menu Start systemu Windows.
2. W obszarze **Połączenia** wybierz **Domyślna witryna serwera**
3. W okienku głównym wybierz **Ustawienia protokołu SSL**
4. W obszarze **Działania** wybierz **Powiązania...**
5. W wyskakującym oknie **Powiązania witryny** wybierz **https** i kliknij **Edytuj...**
6. W wyskakującym okienku **Edytowanie powiązania witryny** w obszarze **Certyfikat SSL** wybierz z listy certyfikat podpisany przez urząd certyfikacji.
7. Kliknij przycisk **OK**, aby zatwierdzić
8. Zamknij wyskakujące okna i zamknij Menedżera IIS.
9. Uruchom ponownie usługę IIS, aby zmiany zaczęły obowiązywać.

6.3.2 Aktualizowanie powiązania usługi raportowania

Procedura

1. Uruchom **Menedżera konfiguracji serwera raportowania** z menu Start systemu Windows.
2. W obszarze **Nazwa serwera** wprowadź nazwę serwera, gdzie działa usługa raportowania, i kliknij **Znajdź**.
3. W obszarze **Instancja serwera raportów** wybierz prawidłową instancję z listy
4. Kliknij **Połącz**
5. Wybierz menu **Adres URL usługi sieci Web**
6. Na ekranie **Adres URL usługi sieci Web** w sekcji **Certyfikat HTTPS** wybierz certyfikat podpisany przez urząd certyfikacyjny i kliknij **Zastosuj**
7. Uruchom ponownie usługę raportowania, aby zmiany zaczęły obowiązywać.

6.3.3 Aktualizowanie odcisku palca certyfikatu

Uwaga: możesz skorzystać z dowolnej z poniższych procedur lub użyć narzędzia konfigurowania certyfikatu BWC zgodnie z opisem w dokumencie *BIS_Data_Security.PDF*

Procedura

1. W oknie ikony uruchamiania lub wyszukiwania systemu Windows uruchom *certlm.msc*
2. Wybierz certyfikat urzędu certyfikacji, który został wystawiony i otwórz go

3. Wybierz kartę **Szczegóły** > pole **Odcisk palca**
4. Skopiuj wartość **Odcisku palca** (tylko znaki alfanumeryczne).
5. Na dysku instalacyjnym systemu BIS otwórz plik *\MgtS\SmartClient\BISIdService \appsettings.json*w edytorze tekstów.
6. Zastąp poprzednią wartość odcisku palca między podwójnymi cudzysłowami skopiowaną nową, wartością.
7. Aby wprowadzić te zmiany w życie, otwórz Internet Information Service i uruchom ponownie pulę aplikacji **BIS IdService**.

6.4 Możliwe dalsze działania

W ramach uaktualnienia możesz rozbudować swój system, np. poprzez dodanie nowych serwerów OPC. Potem mogą się okazać konieczne dalsze działania, takie jak te opisane pod adresem *Realizacja pierwszej instalacji, Strona 15*, począwszy od *Konfigurowanie zapory, Strona 33* aż po *Konfigurowanie serwerów DCOM i OPC, Strona 34*.

7 Konfigurowanie klientów systemu BIS oraz narzędzi

Po zainstalowaniu aplikacji BIS należy przejść do konfigurowania oprogramowania klienckiego i oprogramowania narzędziowego.

7.1 Konfigurowanie certyfikatów z podpisem własnym z serwera systemu BIS

Wstęp

W przypadku systemu BIS 4,7 cała komunikacja między klientami systemu BIS a serwerem BIS odbywa się za pośrednictwem protokołu HTTPS. Serwer systemu BIS tworzy certyfikaty z podpisem własnym zarówno dla nowych instalacji, jak i do uaktualnień z poprzednich wersji, które nie mają protokołu HTTPS. Certyfikaty z podpisem własnym są ważne przez 30 lat.

– Certyfikat systemu BIS z podpisem własnym należy pobrać z przeglądarki i zainstalować go na wszystkich lokalnych komputerach lub urządzeniach.
– Jeśli tylko korzystasz z systemu Access Engine (ACE), musisz zlokalizować plik certyfikatu na dysku instalacyjnym i zainstalować go w ten sam sposób na wszystkich komputerach klienckich ACE.

Pobieranie certyfikatu systemu BIS z podpisem własnym z przeglądarki

1. Na mobilnym urządzeniu klienckim otwórz w przeglądarce adres URL certyfikatu. Na przykład, jeśli nazwą Twojego serwera systemu BIS jest *MYBISSERVER*", adres URL będzie wyglądał tak: *http://MYBISSERVER/MYCERT.CER*

Uwaga!

Na tym etapie nie skonfigurowano jeszcze protokołu HTTPS, więc należy pobrać certyfikat za pośrednictwem protokołu HTTP.
Jeśli strona internetowa serwera BIS jest już używana przez protokół HTTPS, nie będzie można pobrać certyfikatu. W takim przypadku należy wyczyścić historię przeglądarki i wczytać ponownie adres URL za pomocą protokołu HTTP.

2. Zapisz plik certyfikatu w lokalnej pamięci masowej na urządzeniu klienckim.

Lokalizowanie certyfikatu dla Access Engine (ACE)

Certyfikat można znaleźć w następującej lokalizacji:
<installation drive>:\MgtS\Certificates
Access Management System Internal CA.cer.

Instalowanie certyfikatów z podpisem własnym na komputerze klienckim lub na serwerze logowania systemu BIS

1. Kliknij dwukrotnie plik *.CER* certyfikatu, aby obejrzeć.
2. Na karcie **Informacje ogólne** kliknij przycisk **Zainstaluj certyfikat**
3. W ustawieniu **Lokalizacja przechowywania** zaznacz opcję **Komputer lokalny** i kliknij przycisk **Dalej**
4. Zaznacz opcję **Umieść wszystkie certyfikaty w następującym magazynie** i kliknij przycisk **Przeglądaj**
5. Zaznacz opcję **Zaufane główne urzędy certyfikacji** i kliknij przycisk **OK**
6. Kliknij przycisk**Dalej**, a następnie **Zakończ**, aby zakończyć instalowanie certyfikatu.

Instalowanie certyfikatów z podpisem własnym na klienckim urządzeniu mobilnym

1. Na swoim urządzeniu mobilnym otwórz ustawienia urządzenia i wpisz *certificate*, aby znaleźć menu instalacji certyfikatów.
2. Wybierz opcję **Zainstaluj certyfikat z pamięci masowej** (lub podobny, w zależności od używanego systemu operacyjnego).
3. Wybierz zaimportowany certyfikat i zainstaluj go. Należy pamiętać, że niektóre urządzenia będą automatycznie instalować certyfikaty po otwarciu certyfikatu.

Uwaga: certyfikaty są tworzone dla określonej nazwy hosta, więc próby zalogowania się za pomocą *https://localhost* nie powiodą się. Zawsze używaj nazwy hosta w adresie URL*https://<hostname>*

7.1.1 Zaufane ustawienia witryny

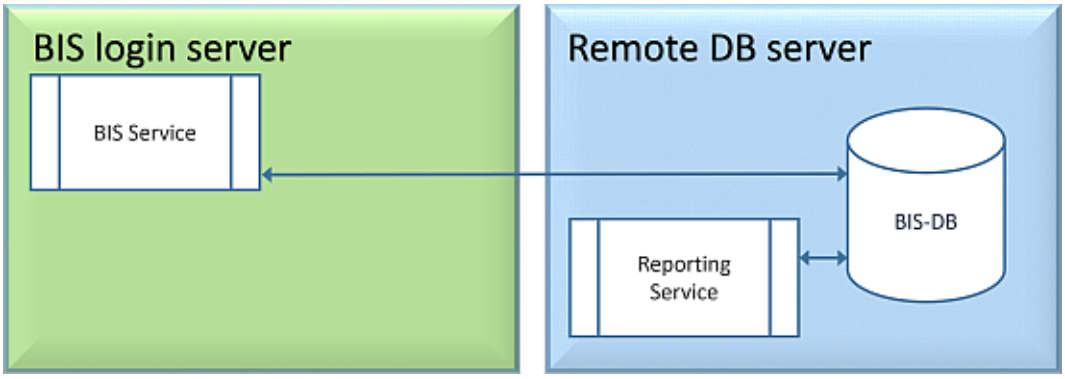
Zgodnie z opisem zawartym w instrukcji instalacji systemu BIS (rozdział **Konfigurowanie klientów systemu BIS i dodatkowych narzędzi**) najprostszym sposobem konfigurowania wymaganych zaufanych witryn w przeglądarce Internet Explorer na komputerach klienckich systemu BIS jest użycie pliku *.REG* dostarczanego przez system BIS.
HTTPS wymaga ręcznego dodania dodatkowych witryn.

1. Na mobilnym urządzeniu klienckim otwórz w przeglądarce adres URL certyfikatu. Na przykład, jeśli nazwą Twojego serwera systemu BIS jest *MYBISSERVER*", adres URL będzie wyglądał tak: *http://MYBISSERVER/MYCERT.CER*
2. Zapisz plik certyfikatu w lokalnej pamięci masowej na urządzeniu klienckim.
3. Na serwerze BIS otwórz ten adres URL w przeglądarce Internet Explorer: *https://localhost/ClientDeploy/tools.aspx*
4. Ze strony aspx pobierz następujący plik: *IE_InternetSettings_Zone2_TrustedSites_BIS.zip*
5. Wyodrębnij plik *.REG* z pliku *.ZIP*
6. Korzystając z kont z uprawnieniami administratora, należy uruchomić plik *.REG* na każdym z komputerów klienckich systemu BIS.
   Ustawienia aplikacji IE są tworzone globalnie za pomocą rejestru systemu Windows.

7.2 Konfigurowanie certyfikatu z podpisem własnym za pomocą usługi raportowania systemu BIS

Wstęp

Ta sekcja dotyczy tylko topologii serwerów, w której na zdalnym serwerze bazy danych działa usługa raportowania systemu BIS, a **nie** na serwerze logowania systemu BIS. We wszystkich innych topologiach usługa raportowania systemu BIS nie potrzebuje własnego certyfikatu.



Należy wykonać trzy kroki:

1. Wyeksportuj certyfikat z menedżera certyfikatów na zdalnym serwerze bazy danych

2. Skopiuj plik *.CER* do serwera logowania systemu BIS i do klientów systemu BIS
3. Zainstaluj certyfikat na serwerze logowania systemu BIS i na klientach systemu BIS

Eksportowanie certyfikatu

1. Na zdalnym serwerze bazy danych, na którym działa usługa raportowania, należy uruchomić przystawkę certyfikatów systemu Windows w *Certlm.msc* z menu Start systemu Windows
2. W programie Certlm przejdź do menu **Certyfikaty lokalnego komputera** > **Osobiste** > **Certyfikaty**
3. Kliknij prawym przyciskiem myszy certyfikat **usługi raportowania** i wybierz opcję **Wszystkie zadania** > **Eksportuj...**
4. Kliknij **Dalej** , aby kontynuować pracę z kreatorem, pobierając tylko wartości domyślne
5. Zapisz plik *.CER* (certyfikat) w wygodnej lokalizacji, z której można go łatwo skopiować na serwer logowania i do klientów systemu BIS.
6. Po zapisaniu pliku zamknij *Certlm.msc*

Kopiowanie certyfikatu

1. Skopiuj plik *.CER* wyeksportowany do serwera logowania systemu BIS i wszystkich klientów systemu BIS.
2. Aby zainstalować certyfikat na każdym z tych komputerów, należy wykonać poniższą procedurę.

Instalowanie certyfikatów z podpisem własnym na komputerze klienckim lub na serwerze logowania systemu BIS

1. Kliknij dwukrotnie plik *.CER* certyfikatu, aby obejrzeć.
2. Na karcie **Informacje ogólne** kliknij przycisk **Zainstaluj certyfikat**
3. W ustawieniu **Lokalizacja przechowywania** zaznacz opcję **Komputer lokalny** i kliknij przycisk **Dalej**
4. Zaznacz opcję **Umieść wszystkie certyfikaty w następującym magazynie** i kliknij przycisk **Przeglądaj**
5. Zaznacz opcję **Zaufane główne urzędy certyfikacji** i kliknij przycisk **OK**
6. Kliknij przycisk**Dalej**, a następnie **Zakończ**, aby zakończyć instalowanie certyfikatu.

7.3 Konfigurowanie przeglądarek internetowych na potrzeby klientów

Klienta systemu BIS uruchamia się z poziomu przeglądarki internetowej MS Internet Explorer. Wykorzystuje się w tym celu adres URL serwera systemu BIS lub adres *https://<Name_of_BIS_Server>*, jeśli klient ma działać na samym serwerze systemu BIS.
Aby zapewnić bezproblemową komunikację między różnymi składnikami systemu BIS, należy zmodyfikować ustawienia zabezpieczeń przeglądarki, rezygnując z ustawień domyślnych. Zmiany te należy wprowadzić we wszystkich przeglądarkach, na których uruchamia się klienta systemu BIS, niezależnie od użytkowników i systemu operacyjnego.

7.3.1 Ustawienia dla przeglądarki Internet Explorer (IE)

Tworzenie ustawień przeglądarki za pomocą pliku .REG

Najprostszą metodą zmiany ustawień przeglądarki jest wykorzystanie pliku poleceń rejestru. Po zainstalowaniu oprogramowania serwera BIS wykonaj następujące czynności.

1. Na serwerze BIS otwórz ten adres URL w przeglądarce Internet Explorer: *https://<Name of BIS server>/ClientDeploy/tools.aspx*
2. Ze strony aspx pobierz następujący plik: *IE_InternetSettings_Zone2_TrustedSites_BIS.zip*
3. Wyodrębnij plik *.REG* z pliku *.ZIP*
4. Za pomocą konta z uprawnieniami administratora uruchom plik *.REG* na każdym komputerze klienta BIS.
   - **Skutek:** ustawienia przeglądarki IE zostały utworzone globalnie za pomocą rejestru systemu Windows.

Importowanie certyfikatów dla usług

W przypadku komunikacji HTTPS między klientem a składnikami systemu BIS należy zainstalować odpowiednie certyfikaty na każdym kliencie:

- Usługa systemu BIS (w każdym przypadku)
- Usługa raportowania (w przypadkach, gdy usługi raportowania działają na zdalnym serwerze bazy danych)
- Usługa ACE (w przypadkach, w których zainstalowano Access Engine).

Szczegółowe informacje na ten temat można znaleźć w głównym podręczniku instalacji systemu BIS.

Ręczne tworzenie ustawień przeglądarki

Możliwe jest ręczne tworzenie lub korygowanie ustawień przeglądarki, choć jest to rozwiązanie bardziej narażone na błędy i z tego względu niezalecane. Wykonaj następujące czynności:

1. Otwórz przeglądarkę Internet Explorer i przejdź do strony **Opcje internetowe** w tej wersji przeglądarki, tzn. kliknij opcję **Narzędzia** (lub ikonę koła zębatego) > **Opcje internetowe**.
2. Jeśli chcesz, aby ekran logowania operatora systemu BIS ładował się automatycznie, gdy operator uruchomi przeglądarkę Internet Explorer, na karcie Informacje ogólne ustaw adres strony domowej na *https://<Name_of_Bis_Server>* (tzn. na adres URL swojego serwera systemu BIS).
3. Kliknij kartę:**Zabezpieczenia** > ikona:**Zaufane witryny** przycisk:**Witryny**
4. Wprowadź adres *https://<Name_of_Bis_Server>* (zamieniając *<Name_of_Bis_Server>* na nazwę własnego serwera systemu BIS) i kliknij przycisk **Dodaj**, aby dodać ten adres do listy zaufanych witryn.
   Jeśli konfigurujesz tego klienta na serwerze BIS, dodaj również adres *https://localhost*.
5. Kliknij przycisk: **Zamknij**
6. Pozostając na karcie:**Zabezpieczenia** > ikona:**Zaufane witryny**, kliknij przycisk:**Poziom niestandardowy...**.
7. Na nośniku instalacyjnym systemu BIS zlokalizuj i otwórz plik *<language folder>\Documents\BIS platform\IE-Settings.xls*.
8. W pliku **IE-Settings.xls** otwórz kartę odnoszącą się do Twojej wersji przeglądarki.
9. W zależności od swojego domyślnego poziomu zabezpieczeń (**Średni**, **Wysoki** lub **Niestandardowy**) włącz lub wyłącz elementy sterujące wyświetlone w odpowiedniej kolumnie pliku **IE-Settings.xls**, następnie kliknij przycisk **OK**.
   UWAGA: Jeśli masz inny poziom zabezpieczeń, zalecamy rozpoczęcie od domyślnego poziomu **Średni**.

10. Uruchom ponownie przeglądarkę Internet Explorer, aby uwzględnić nowe ustawienia.

Uwaga!
Ustawienie systemu Windows **Zaktualizuj certyfikaty główne** sprawia, że system operacyjny weryfikuje każdy z certyfikatów za pomocą serwera Microsoft Windows Update Server, generując wpis w dzienniku zdarzeń. Aby temu zapobiec, wyczyść pole wyboru **Zaktualizuj certyfikaty główne** w następującym oknie dialogowym:
Start > **Panel sterowania** > **Dodaj lub usuń programy** > **Dodaj/Usuń składniki systemu Windows**.

7.4 Używanie silnych haseł

W celu podniesienia poziomu bezpieczeństwa system zmusza wszystkich użytkowników do ustawienia silnego hasła podczas logowania się do klienta systemu Windows z użyciem domyślnego hasła, które jest takie samo jak nazwa użytkownika.
Postępuj zgodnie z instrukcjami wyświetlanymi w oknie dialogowym **Zmiana hasła**, aby zresetować hasło zgodnie z zasadami haseł.

Uwaga!
System odrzuca wszystkie logowania na urządzeniach przenośnych sieci Web, dopóki nie zostanie ustawione silne hasło w kliencie systemu Windows.

7.5 Konfigurowanie zapory

Aby skonfigurować zaporę na urządzeniach klienckich, postępuj tak jak opisano dla serwera systemu BIS pod adresem *Konfigurowanie zapory, Strona 33*.

7.6 Instalowanie dodatkowych narzędzi systemu BIS

System BIS udostępnia dodatkowe narzędzia do realizacji następujących zadań:
- Ograniczanie przepustowości pasma sieciowego wykorzystywanego przez system BIS.
- Sprawdzanie szczegółowych informacji na temat komputera klienckiego systemu BIS.
- Tworzenie i modyfikowanie raportów systemu SQL Server dla dziennika zdarzeń systemu BIS.
- Wykonywanie aplikacji zaprojektowanych na platformy .NET Framework 2.0, 3.5, 4.0 i 4.8.

Zasady korzystania z tych narzędzi są opisane w pomocy ekranowej konfiguracji systemu BIS. Może je zainstalować na serwerze systemu BIS i/lub na klientach systemu BIS z aktywnej strony serwera BIS. Procedura instalacji wygląda następująco:
1. Uruchom aplikację Internet Explorer.
2. Wprowadź następujący adres URL: *https://<Name_of_Bis_Server>/ClientDeploy/Tools.aspx* (podstaw nazwę własnego serwera systemu BIS). **Uwaga**: Jeśli przeglądarka Internet Explorer nie wyświetla już pola adresu, ten sam efekt można osiągnąć klikając przyciski **Start** > **Uruchom** i wprowadzając **iexplore** *https://<Name_of_Bis_Server>/ClientDeploy/Tools.aspx*
3. Spowoduje to wyświetlenie strony pobierania. Kliknij przycisk **Pobierz** dla żądanego narzędzia.
4. Spowoduje to wyświetlenie okna dialogowego z potwierdzeniem — kliknij wtedy przycisk **Uruchom**.
5. Efekt zależy od wybranego narzędzia:
   - Program NetLimiter zainstaluje się i zażąda ponownego uruchomienia komputera.
   - Narzędzie Client Information zostanie natychmiast uruchomione.

- Program Report Builder można zainstalować bezpośrednio po naciśnięciu przycisku **Pobierz...**.
- Środowisko uruchomieniowe platformy .NET Framework (2.0, 3.5 lub 4.0) można zainstalować bezpośrednio po naciśnięciu przycisku **Pobierz....** Należy pamiętać , że w przypadku systemów Windows 8.1 i Windows Server 2012 konieczne będą nośniki instalacyjne firmy Microsoft.

Narzędzie zmiany hasła

W wersji BIS 4.6 dodaliśmy nowe narzędzie do obsługi haseł użytkowników systemu BIS, to znaczy zarówno użytkowników systemu operacyjnego Windows, jak i SQL.
Szczegółowe informacje na ten temat można znaleźć w pomocy do konfiguracji systemu BIS.

7.7 Instalowanie wraz z systemem BIS oprogramowania innych producentów

Informacje wstępne

Jako system bezpieczeństwa o znaczeniu krytycznym dla firmy, system BIS powinien zawsze funkcjonować na komputerach dedykowanych. Dodanie do takiej instalacji oprogramowania innych producentów, o ile nie da się tego uniknąć, wymaga starannego rozważenia i zaplanowania.

Uwaga!
Firma Bosch zdecydowanie zaleca, aby przed zainstalowaniem oprogramowania innych producentów w rzeczywistym systemie produkcyjnym, najpierw zainstalować je w systemie testowym funkcjonującym offline.

Procedura

Wykonaj zawsze następujące kroki i starannie je udokumentuj, na wypadek gdyby później była potrzebna pomoc techniczna.

1. Przed zainstalowaniem w rzeczywistym systemie oprogramowania innych producentów:
   - Upewnij się, że ograniczenia i wymagania oprogramowania innych producentów nie kolidują z ograniczeniami i wymaganiami systemu BIS.
   - Utwórz punkt przywracania.
   - Utwórz kopię zapasową systemu BIS.
2. Po zainstalowaniu w rzeczywistym systemie oprogramowania innych producentów:
   - Upewnij się, że system BIS osiągnął pełną zdolność operacyjną.

8 Licencjonowanie instalacji systemu BIS

Licencje dla systemów BIS 4.0 i nowszych są zamawiane online i dostarczane drogą elektroniczną. Wykonaj następujące czynności:

1. Zamów potrzebne licencje w lokalnym punkcie składania zamówień firmy Bosch lub w dziale sprzedaży. Otrzymasz od pracowników wiadomość e-mail z numerem autoryzacyjnym.

Uwaga!
Licencjonowanie w sytuacji awaryjnej
Licencje są ściśle powiązane ze sprzętem. Jeśli z uwagi na pewną sytuację awaryjną musisz zmienić sprzęt serwerowy, zadzwoń do lokalnego partnera firmy Bosch lub jej przedstawiciela ds. obsługi klienta. Firma może wtedy przenieść Twoje licencje na identyfikatory nowego sprzętu lub udostępnić na ograniczony czas licencje awaryjne.

2. Uruchom menedżera systemu BIS
3. W zakładce **Licencja** kliknij przycisk **Uruchom menedżera licencji**.
   – **Skutek:** Zostaje wyświetlone okno dialogowe menedżera licencji.
4. Zaznacz opcje dotyczące pakietu oprogramowania, funkcji oraz rozszerzeń, które zostały przez Ciebie zamówione. W przypadku rozszerzeń wprowadź liczbę wymaganych jednostek.
5. Kliknij przycisk **Aktywuj...**.
   – **Skutek:** wyświetla się okno dialogowe **aktywacji licencji** z sygnaturą Twojego komputera.
6. Spisz sygnaturę komputera lub skopiuj ją i wklej do pliku tekstowego.
7. Na komputerze z dostępem do Internetu wprowadź następujący adres URL do paska adresu przeglądarki:
   https://activation.boschsecurity.com
   Jeżeli nie masz konta umożliwiającego dostęp do Centrum aktywacji licencji firmy Bosch, utwórz nowe i zaloguj się (zalecane) lub kliknij łącze w celu aktywowania nowej licencji bez konieczności logowania. Zauważ, że w przypadku licencji SMA (umowa o wsparcie techniczne oprogramowania) posiadanie konta zawsze jest wymagane. Dodatkową zaletą konta jest możliwość śledzenia wszystkich przeprowadzonych przez Ciebie aktywacji, co może być przydatne w przyszłości.

   Postępuj zgodnie z instrukcjami zawartymi na stronie internetowej, aby uzyskać klucz aktywacji licencji.

8. Wróć do oprogramowania. W oknie dialogowym **aktywacji licencji** wpisz lub wklej klucz aktywacji licencji uzyskany z Centrum aktywacji licencji firmy Bosch i kliknij przycisk **Aktywuj**.
   – **Skutek:** pakiety oprogramowania są aktywowane na danym komputerze.
9. Kliknij przycisk **Odśwież** w celu wyświetlenia zmodyfikowanego zestawu aktywowanych licencji

Uwaga!
Skutki zmian dotyczących sprzętu i oprogramowania
Zmiany sprzętowe serwera mogą unieważnić Twoją licencję i spowodować, że oprogramowanie przestanie działać. Zanim wprowadzisz zmiany ma serwerze, skontaktuj się z pomocą techniczną.

9 Konserwacja i deinstalacja

W rozdziale tym opisano główne zadania, które musisz wykonać, aby instalacja systemu BIS działała poprawnie lub aby odinstalować to oprogramowanie bez pozostawiania śladów.

9.1 Konserwacja

Systemy BIS mają często znaczenie krytyczne dla firmy, zarówno z uwagi na zawarte w nich dane, jak i z uwagi na pełnione przez nie funkcje. Z tego względu firma Bosch zdecydowanie zaleca używanie macierzy RAID lub sieci SAN (Storage Area Network) oraz ich prawidłową konserwację. Musisz zadbać o regularne sprawdzanie dysków systemu pod kątem błędów odczytu/zapisu, braku miejsca i fragmentacji.
Dziennik błędów systemu BIS (**BIS Manager (Menedżer systemu BIS)** > karta:**Error log (Dziennik błędów)**) dostarcza cennych informacji na temat problemów napotkanych w systemie.
Firma Bosch zapewnia pomoc techniczną za pośrednictwem typowych kanałów udostępnionych Ci przez lokalnego sprzedawcę firmy Bosch. Jeśli musisz przekazać szczegółowe informacje na temat swojej konfiguracji, w oknie **BIS Manager (Menedżer systemu BIS)** kliknij kartę: **Error log (Dziennik błędów)** > przycisk:**Start Configuration Collector (Uruchom program Configuration Collector)**. Narzędzie Configuration Collector stanowi element każdej instalacji systemu BIS i ma własną pomoc ekranową.

9.2 Tworzenie kopii zapasowych i przywracanie konfiguracji

Musisz regularnie tworzyć kopie zapasowe operacyjnych konfiguracji swojego systemu BIS. Trzeba je również tworzyć po każdym wprowadzeniu poważnych zmian. Można to zrobić w dwojaki sposób:

- ręcznie w menedżerze systemu BIS (BIS Manager): upewnij się, że system **działa**, następnie kliknij kartę: **Backup /Restore configuration (Utwórz/przywróć kopię zapasową konfiguracji)** > przycisk: **Backup (Kopia zapasowa)**;
- automatycznie, jako zadanie zaplanowane w samym systemie BIS. Instrukcje na ten temat można znaleźć w pomocy ekranowej konfiguracji systemu BIS.

Domyślny katalog na kopie zapasowe konfiguracji to **<naped_instalacyjny>:\Backup**.

Aby przywrócić kopię zapasową konfiguracji, najpierw upewnij się, że aplikacja BIS została **zamknięta**, następnie skorzystaj z tej samej karty **Backup /Restore configuration (Utwórz/przywróć kopię zapasową konfiguracji)** > przycisk: **Restore (Przywróć)** w menedżerze systemu BIS (BIS Manager). Jeśli przywrócisz konfigurację ze starszej wersji systemu BIS, niezbędne konwersje zostaną wykonane automatycznie, gdy nowa wersja systemu BIS załaduje starą konfigurację.

9.3 Deinstalacja

Deinstalacja może się okazać konieczna na przykład w trakcie uaktualniania z jednej wersji systemu BIS do innej, gdy ścieżka uaktualniania nie jest obsługiwana — patrz *Wymagania wstępne, Strona 35*.

Uwaga!
Kreator instalacji systemu BIS nie usuwa produktów innych producentów, takich jak Microsoft SQL Server, gdyż mogą być one wykorzystywane przez inne aplikacje zainstalowane na Twoim komputerze. Jeśli następnie ponownie zainstalujesz system BIS bez ręcznego odinstalowywania systemu Microsoft SQL Server, kreator zainstaluje system BIS w oparciu o istniejące bazy danych.

1. Najpierw zamknij serwer systemu BIS na karcie menedżera systemu BIS (BIS Manager):**System start/stop (Uruchamianie/zatrzymywanie systemu)** > przycisk:**Stop Server component (Zamknij składnik serwera)**.
2. Odinstaluj oprogramowanie BIS za pomocą standardowego oprogramowania administracyjnego systemu Microsoft Windows, np. pod kontrolą systemu Windows 7 kliknij przycisk **Start** > **Panel sterowania** > **Programy i funkcje**. Komputer wyświetli wtedy listę wszystkich zainstalowanych pakietów oprogramowania. Na tej liście zaznacz pozycję **BIS — Building Integration System**, kliknij przycisk **Usuń** i postępuj zgodnie z zaleceniami programu konfiguracyjnego.
3. W ten sam sposób usuń wszystkie pakiety, których nazwa zaczyna się od „BIS”.
4. Po zakończeniu deinstalacji uruchom ponownie komputer.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com

202011261147