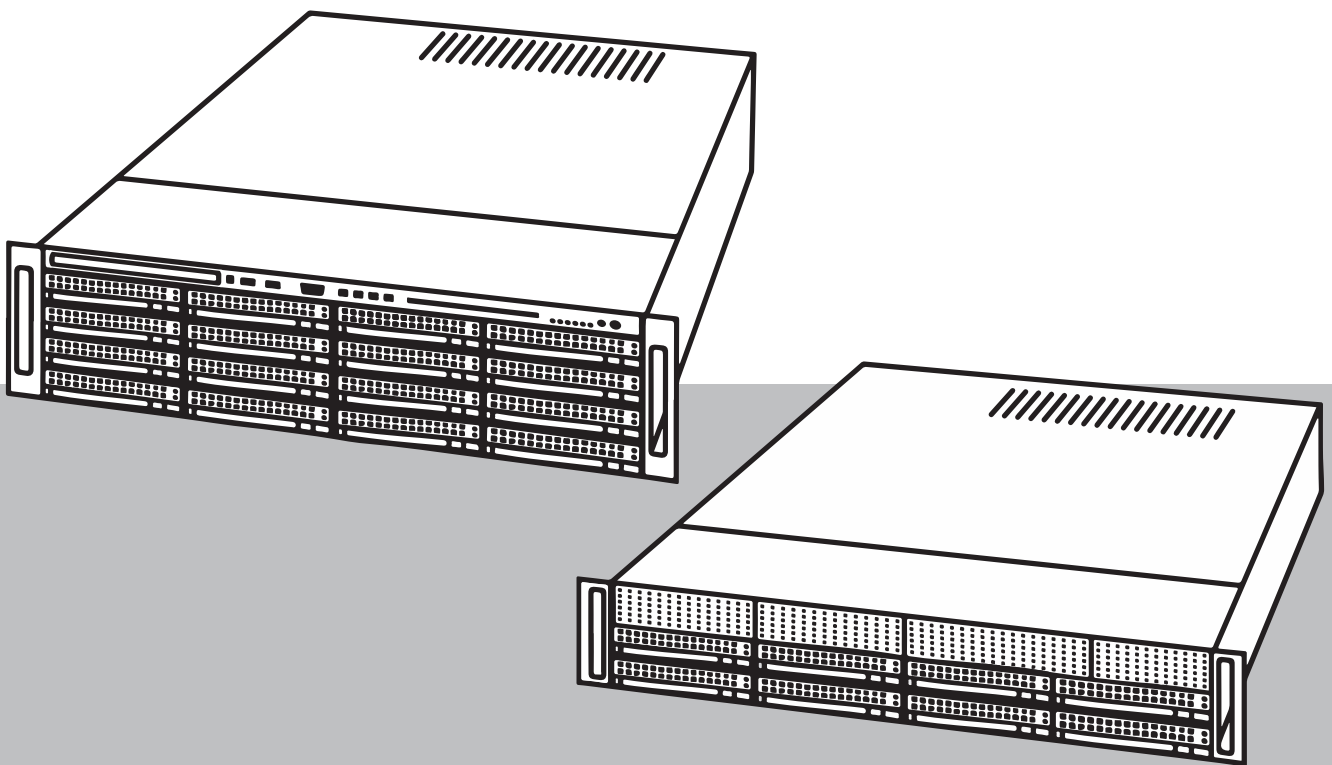


DIVAR IP all-in-one 7000 2U | DIVAR IP all-in-one 7000 3U

DIP-7380-00N | DIP-7384-8HD | DIP-7388-8HD | DIP-738C-8HD |
DIP-73G0-00N | DIP-73G8-16HD | DIP-73GC-16HD



Spis treści

1	Bezpieczeństwo	4
1.1	Zasady bezpieczeństwa dotyczące eksploatacji	4
1.2	Środki ostrożności w zakresie cyberbezpieczeństwa	4
1.3	Zalecenia dotyczące oprogramowania	5
1.3.1	Użyj najnowszego oprogramowania	5
1.3.2	Informacje o przepisach OSS	5
2	Wstęp	6
3	Ogólne informacje o systemie	7
4	Konfiguracja systemu	9
4.1	Ustawienia domyślne	9
4.2	Warunki wstępne	9
4.3	Pierwsze logowanie i wstępna konfiguracja systemu	9
5	Uaktualnianie oprogramowania	13
5.1	Zastąpienie DIVAR IP Software Center przez DIVAR IP System Manager	13
5.2	Aktualizacja oprogramowania za pomocą programu System Manager	14
5.3	Aktualizacja oprogramowania za pomocą programu Software Center	16
6	Zdalne połączenie z systemem	17
6.1	Ochrona systemu przed nieautoryzowanym dostępem	17
6.2	Konfigurowanie przekierowania portów	17
6.3	Wybór odpowiedniego klienta	17
6.3.1	Połączenie zdalne za pomocą aplikacji BVMS Operator Client.	17
6.3.2	Połączenie zdalne za pomocą aplikacji Video Security	18
6.4	Łączenie z serwerem Enterprise Management Server	18
6.5	Nawiązywanie połączenia z Remote Portal	18
6.5.1	Tworzenie konta w portalu Remote Portal	19
6.5.2	Rejestrowanie urządzeń DIVAR IP all-in-one w portalu Remote Portal	19
6.5.3	Wyrejestrowanie urządzeń DIVAR IP all-in-one z aplikacji Remote Portal	19
7	Obsługa serwisowa	21
7.1	Logowanie do konta administratora	21
7.2	Monitorowanie systemu	21
7.2.1	Monitorowanie systemu za pomocą aplikacji SuperDoctor podczas pracy z DIVAR IP Remote Portal	21
7.2.2	Monitorowanie systemu za pomocą aplikacji SuperDoctor podczas pracy z DIVAR IP Software Center	22
7.2.3	Monitorowanie systemu za pomocą interfejsu IPMI	22
7.3	Pobieranie plików rejestrów programu DIVAR IP System Manager	23
7.4	Przywracanie ustawień fabrycznych	23
8	Informacje dodatkowe	24
8.1	Dodatkowa dokumentacja i oprogramowanie	24
8.2	Usługi pomocy technicznej i Bosch Academy	24

1 Bezpieczeństwo

Należy przestrzegać zasad bezpieczeństwa wyszczególnionych w tym rozdziale.

1.1 Zasady bezpieczeństwa dotyczące eksploatacji

Urządzenie może być instalowane tylko przez wykwalifikowanych specjalistów. Urządzenie nie jest przeznaczone do użytku osobistego lub w gospodarstwach domowych. Urządzenie może być dowolnie używane w handlu i przemysłne z wyjątkiem sytuacji opisanych w sekcji Bezpieczeństwo.



Uwaga!

Produkt jest urządzeniem **klasy A**. W środowisku mieszkalnym urządzenie może powodować zakłócenia radiowe. W wypadku ich wystąpienia może być konieczne podjęcie określonych działań zapobiegawczych.



Uwaga!

Zanik sygnału wizyjnego jest nieodłącznym elementem jego cyfrowego zapisu. W związku z tym firma Bosch Security Systems nie ponosi odpowiedzialności za szkody spowodowane utratą określonych danych wizyjnych.

Aby ograniczyć do minimum ryzyko utraty danych, zaleca się stosowanie kilku nadmiarowych systemów zapisu, jak również tworzenie kopii zapasowych wszystkich danych analogowych i cyfrowych.

1.2 Środki ostrożności w zakresie cyberbezpieczeństwa

Ze względu na cyberbezpieczeństwo należy przestrzegać następujących zasad:

- Fizyczny dostęp do systemu może mieć tylko uprawniony personel. System umieścić w obszarze z kontrolą dostępu, aby uniknąć fizycznej manipulacji.
- System operacyjny zawiera najnowsze poprawki bezpieczeństwa systemu Windows, które były dostępne w momencie tworzenia obrazu oprogramowania. Do regularnego instalowania aktualizacji zabezpieczeń systemu operacyjnego należy używać aktualizacji systemu Windows przez Internet lub — dla systemów offline — odpowiednich comiesięcznych poprawek typu roll-up.
- Nie wolno wyłączać programu Windows Defender ani zapory systemu Windows i zawsze należy je aktualizować.
- Nie wolno instalować dodatkowego oprogramowania antywirusowego.
- Nie udostępniać informacji o systemie i wrażliwych danych nieznanym osobom, o ile nie ma pewności co do uprawnień danej osoby.
- Nie wolno wysyłać wrażliwych informacji przez Internet zanim nie zostanie potwierdzone bezpieczeństwo danej strony.
- Dostęp do sieci lokalnej mogą mieć tylko zaufane urządzenia. Szczegóły opisano w poniższych dokumentach dostępnych w katalogu produktów online:
 - *Uwierzytelnianie sieciowe 802.1X*
 - *Poradnik cyberbezpieczeństwa dla produktów wideo IP firmy Bosch*
- W przypadku dostępu przez sieci publiczne należy używać tylko bezpiecznych (szyfrowanych) kanałów komunikacji.
- Konto administratora zapewnia pełne uprawnienia administracyjne i nieograniczony dostęp do systemu. Uprawnienia administratora umożliwiają użytkownikom instalowanie, aktualizowanie lub usuwanie oprogramowania oraz zmianę ustawień konfiguracyjnych. Ponadto uprawnienia administratora umożliwiają użytkownikom bezpośredni dostęp do rejestru i zmianę jego kluczy, a tym samym obejście mechanizmów centralnego

zarządzania i ustawień zabezpieczeń. Użytkownicy zalogowani na konto administratora mogą pokonywać zapory sieciowe i usuwać oprogramowanie antywirusowe, co może narazić system na infekcje wirusowe i cyberataki. Może to stanowić poważne zagrożenie dla bezpieczeństwa systemu i danych.

Aby zminimalizować zagrożenia związane z cyberbezpieczeństwem, należy przestrzegać następujących zasad:

- Konto administratora musi być chronione skomplikowanym hasłem zbudowanym zgodnie z polityką haseł.
- Tylko ograniczona liczba zaufanych użytkowników może mieć dostęp do konta administratora.
- Ze względu na wymagania operacyjne dysk systemowy nie może być szyfrowany. Bez szyfrowania dane przechowywane na tym dysku mogą być łatwo dostępne i usunięte. Aby uniknąć kradzieży lub przypadkowej utraty danych, należy upewnić się, że dostęp do systemu i konta administratora mają tylko upoważnione osoby.
- Do instalacji i aktualizacji oprogramowania, a także do odzyskiwania systemu może być konieczne użycie urządzeń USB. Dlatego nie wolno wyłączać portów USB w systemie. Podłączanie urządzeń USB do systemu stwarza jednak ryzyko infekcji złośliwym oprogramowaniem. Aby uniknąć ataków złośliwym oprogramowaniem, do systemu nie mogą zostać nigdy podłączone żadne zainfekowane urządzenia USB.

1.3 Zalecenia dotyczące oprogramowania

1.3.1 Użyj najnowszego oprogramowania

Przed pierwszym rozpoczęciem obsługi urządzenia należy upewnić się, że jest instalowana najnowsza dostępna wersja oprogramowania. Aby zapewnić spójność działania, zgodność, wydajność i bezpieczeństwo, oprogramowanie należy regularnie aktualizować przez cały okres eksploatacji urządzenia. Należy postępować zgodnie z instrukcjami podanymi w dokumentacji produktu w zakresie aktualizacji oprogramowania.

Więcej informacji można znaleźć w następujących miejscach:

- Informacje ogólne: <https://www.boschsecurity.com/xc/en/support/product-security/>
- Forum bezpieczeństwa, czyli lista rozpoznanych zagrożeń i proponowanych rozwiązań: <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>

Firma Bosch nie ponosi odpowiedzialności za szkody spowodowane korzystaniem ze starej wersji oprogramowania.

Najnowsze oprogramowanie oraz dostępne pakiety aktualizacyjne można znaleźć w materiałach do pobrania Bosch Security and Safety Systems na stronie:

<https://downloadstore.boschsecurity.com/>

1.3.2 Informacje o przepisach OSS

W produktach DIVAR IP all-in-one Bosch używa oprogramowania OSS (Open Source Software). Licencje na używane składniki oprogramowania OSS znajdują się na dysku systemowym:

```
C:\license txt\
```

Licencje składników oprogramowania OSS używane w innym oprogramowaniu zainstalowanym w systemie są przechowywane w folderze instalacyjnym odpowiedniego oprogramowania, na przykład:

```
C:\Program Files\Bosch\SysMgmService\apps\sysmgm-  
commander\[version]\License
```

lub:

```
C:\Program Files\Bosch\SysMgmService\apps\sysmgm-executor\[version]\License
```

2 Wstęp

DIVAR IP all-in-one 7000 jest przystępnym cenowo, uniwersalnym rozwiązaniem do rejestrowania, wyświetlania oraz zarządzania obrazami. Jest stosowany w sieciowych systemach dozoru wizyjnego wykorzystujących maksymalnie 256 kanały (w tym 8 kanałów licencjonowanych w pakiecie).

Rejestrator DIVAR IP all-in-one 7000 2U/3U to urządzenie o wysokości 2U/3U przystosowane do montażu w szafie typu rack, które łączy w sobie możliwości Bosch Video Management System i zaawansowane funkcje zapisu i zarządzania nagraniami, tworząc zintegrowane, ekonomiczne, wygodne w instalacji i obsłudze urządzenie do nagrywania skierowane do klientów obeznanych z technologiami IT.

DIVAR IP all-in-one 7000 wykorzystuje wbudowaną konstrukcję i podstawowe komponenty oraz opiera się na systemie operacyjnym Microsoft Windows Server IoT 2019 for Storage Standard. DIVAR IP all-in-one 7000 posiada dyski twarde SATA „klasy korporacyjnej”, wymieniane podczas pracy, zapewniające do 96/192 TB pojemności brutto.

3 Ogólne informacje o systemie

System operacyjny

W systemach operacyjnych Microsoft Windows Server IoT 2019 for Storage Standard dostępny jest interfejs użytkownika służący do wstępnej konfiguracji serwera, ujednoczonego zarządzania urządzeniami pamięci masowej, uproszczonej konfiguracji i zarządzania pamięcią masową oraz obsługi oprogramowania Microsoft iSCSI Software Target.

Interfejs ten jest specjalnie dostosowany, aby zapewniać optymalne działanie sieciowych pamięci masowych. System operacyjny Microsoft Windows Server IoT 2019 for Storage Standard oferuje znaczne ulepszenia w zakresie zarządzania urządzeniami pamięci masowej, a także integracji składników i funkcji zarządzania takimi urządzeniami.

DIVAR IP System Manager

Aplikacja DIVAR IP System Manager jest centralnym interfejsem użytkownika zapewniającym łatwą instalację, konfigurację i uaktualnienie oprogramowania.



Uwaga!

DIVAR IP Software Center w starszych wersjach oprogramowania DIVAR IP all-in-one 7000 (DIP-73xx) było stosowane jako oprogramowanie do zarządzania. Zaleca się aktualizację systemu do DIVAR IP System Manager... Aktualizacja do wersji BVMS wyższych niż 11.1.1 wymaga instalacji oprogramowania DIVAR IP System Manager 2.x.

Tryby pracy

Systemy DIVAR IP all-in-one 7000 mogą pracować w trzech trybach:

- Kompletny system zarządzania telewizją dozorową i nagraniami, z wykorzystaniem podstawowych składników i usług BVMS i Video Recording Manager. Ten tryb zapewnia zaawansowane rozwiązanie w zakresie sieciowego dozoru wizyjnego, umożliwiające łatwe zarządzanie cyfrowym obrazem, dźwiękiem i danymi w dowolnej sieci IP. Zapewnia bezproblemowe łączenie kamer sieciowych i nadajników oraz umożliwia zarządzanie zdarzeniami oraz alarmami, monitorowanie stanu systemu, a także administrowanie użytkownikami i priorytetami. To najlepszy system zarządzania obrazem z systemów dozoru wizyjnego firmy Bosch, który zwiększa niepowtarzalność możliwości kamer i rozwiązań do zapisu obrazu firmy Bosch. Zawiera komponenty Video Streaming Gateway do integracji kamer innych firm.
- Zaawansowane rozwiązanie do nagrywania wideo dla systemu BVMS wykorzystujące podstawowe komponenty i usługi Video Recording Manager oraz unikalne możliwości kamer i rozwiązań zapisu firmy Bosch. Do systemu można uruchomić na urządzeniu DIVAR IP all-in-one można dodać dwa serwery Video Recording Manager.
- Rozszerzenie pamięci masowej iSCSI dla systemu BVMS lub Video Recording Manager, który działa na innym urządzeniu. Do systemu można uruchomić na urządzeniu DIVAR IP all-in-one 7000 można dodać cztery rozszerzenia pamięci masowej iSCSI.

Aby skonfigurować system, w aplikacji DIVAR IP System Manager należy wybrać żądany tryb pracy.

Za pomocą aplikacji DIVAR IP System Manager można również uaktualnić zainstalowane oprogramowanie.

Najnowsze oprogramowanie oraz dostępne pakiety aktualizacyjne można znaleźć w materiałach do pobrania Bosch Security and Safety Systems na stronie:

<https://downloadstore.boschsecurity.com/>



Uwaga!

Zapisane strumienie wizyjne muszą być skonfigurowane w taki sposób, aby nie doszło do przekroczenia maksymalnej szerokości pasma dostępnej dla systemu (podstawowego systemu BVMS/VRM plus rozszerzenia pamięci masowej iSCSI).

4 Konfiguracja systemu

4.1 Ustawienia domyślne

Wszystkie systemy DIVAR IP mają fabrycznie skonfigurowany adres IP oraz domyślne ustawienia iSCSI:

- Adres IP: automatycznie przypisywany przez usługę DHCP (adres IP przełączania awaryjnego: 192.168.0.200).
- Maska podsieci: automatycznie przypisywana przez usługę DHCP (maska podsieci przełączania awaryjnego: 255.255.255.0).

Domyślne ustawienia użytkownika dla konta administratora

- Nazwa użytkownika: **BVRAdmin**
- Hasło: należy ustawić przy pierwszym logowaniu.

Wymagania dotyczące hasła:

- Co najmniej 14 znaków.
- Co najmniej jedna wielka litera.
- Co najmniej jedna mała litera.
- Co najmniej jedna cyfra.

4.2 Warunki wstępne

Przestrzegać poniższych zaleceń:

- Podczas instalacji DIVAR IP musi korzystać z aktywnego połączenia z siecią. Należy upewnić się, że jest włączony przełącznik, do którego podłączono urządzenie.
- Domyślny adres IP nie może być zajęty przez inne urządzenie w tej sieci. Upewnij się, że domyślne adresy IP systemów DIVAR IP istniejących w sieci zostały zmienione przed dodaniem kolejnych urządzeń DIVAR IP.

4.3 Pierwsze logowanie i wstępna konfiguracja systemu



Uwaga!

Nie należy zmieniać żadnych ustawień systemu operacyjnego. Zmiana ustawień systemu operacyjnego może spowodować nieprawidłowe działanie systemu.



Uwaga!

Aby wykonywać zadania administracyjne należy zalogować się do konta administratora.



Uwaga!


W przypadku utraty hasła system należy odzyskać zgodnie z procedurą opisaną w Instrukcji instalacji. Konfigurację należy przeprowadzić od podstaw lub zaimportować.

Aby skonfigurować system:

1. Podłączyć jednostkę DIVAR IP all-in-one i kamery do sieci.
2. Włączyć jednostkę.

Wykonywane są procedury konfiguracji Microsoft Windows Server IoT 2019 for Storage Standard. Cały ten proces może potrwać kilka minut. Nie wyłączać systemu.

Po zakończeniu procesu zostanie wyświetlony ekran wyboru języka w systemie Windows.

3. Wybierz z listy swój kraj/region, żądany język systemu operacyjnego oraz układ klawiatury, a następnie kliknij przycisk **Dalej**.
Zostaną wyświetlone warunki licencji oprogramowania Microsoft.
4. Kliknij **Akceptuj**, aby zaakceptować postanowienia licencyjne, i poczekaj na ponowne uruchomienie systemu Windows. Cały ten proces może potrwać kilka minut. Nie wyłączać systemu.
Po ponownym uruchomieniu zostanie wyświetlona strona logowania systemu Windows.
5. Ustaw nowe hasło dla konta administratora **BVRAdmin** i potwierdź je.
Wymagania dotyczące hasła:
 - Co najmniej 14 znaków.
 - Co najmniej jedna wielka litera.
 - Co najmniej jedna mała litera.
 - Co najmniej jedna cyfra.Następnie nacisnąć Enter (Zatwierdź).
Zostanie wyświetlona strona **Software Selection**.
6. System automatycznie skanuje dysk lokalny i podłączone zewnętrzne nośniki pamięci w poszukiwaniu pliku instalacyjnego **BoschAppliance_Setup_DSC_[wersja oprogramowania].exe**, który znajduje się w folderze o następującej strukturze: katalog główny dysku\BoschAppliance\. Skanowanie może zająć trochę czasu. Należy poczekać na jego zakończenie.
7. Aby przygotować urządzenie do instalacji programu DIVAR IP System Manager, należy najpierw zainstalować plik **BoschAppliance_Setup_DSC_10.01.0001.exe**.
Plik instalacyjny wykryty przez system zostanie wyświetlony na stronie Software Selection (Wybór oprogramowania). Aby rozpocząć instalację i przejść do kroku 14, kliknij pasek, na którym wyświetlany jest plik instalacyjny.
Jeśli plik instalacyjny nie zostanie wykryty:
8. Przejdź na stronę <https://downloadstore.boschsecurity.com/>.
9. Pod kartą **Software** wybrać z listy **BVMS Appliances**, a następnie kliknąć **Select**.
Zostanie wyświetlona lista dostępnych pakietów oprogramowania.
10. Znajdź plik ZIP **SystemManager_[software version 2.0.0 or higher].zip** i zapisz go na nośniku pamięci, takim jak pamięć USB.
11. Rozpakuj plik na nośniku pamięci. Pamiętaj, aby folder **BoschAppliance** zapisać w katalogu głównym nośnika.
12. Podłącz nośnik pamięci do urządzenia DIVAR IP all-in-one.
System automatycznie przeskanuje nośnik pamięci w poszukiwaniu pliku instalacyjnego **BoschAppliance_Setup_DSC_10.01.0001.exe**.
Skanowanie może zająć trochę czasu. Należy poczekać na jego zakończenie.
13. Po wykryciu przez system pliku instalacyjnego, jest on wyświetlany na stronie **Software Selection**. Kliknij pasek wyświetlający plik instalacyjny, aby rozpocząć instalację.
Uwaga: aby plik instalacyjny został automatycznie wykryty, musi znajdować się w folderze o następującej strukturze: Drive root\BoschAppliance\ (na przykład F:\BoschAppliance\).
Jeśli plik instalacyjny jest w innej lokalizacji, która nie pasuje do uprzednio zdefiniowanej struktury folderów, kliknij , aby przejść do odpowiedniej lokalizacji. Następnie należy kliknąć plik instalacyjny, aby rozpocząć instalację.
14. Rozpocznie się instalacja. Proces instalacji może zająć kilka minut. W trakcie instalacji nie wyłączaj systemu i nie wyjmuj nośnika pamięci. Po pomyślnym zakończeniu instalacji system uruchomi się ponownie i przejdzie do strony logowania Windows.

15. Zaloguj się na konto administratora BVRAdmin.
Pojawi się strona **Software Selection** pokazująca plik instalacyjny DIVAR IP System Manager 2.x **SystemManager_x64_[wersja oprogramowania].exe**.
16. Aby rozpocząć instalację, należy kliknąć pasek, na którym widoczny jest plik instalacyjny.
17. Przed rozpoczęciem instalacji zostanie wyświetlone okno dialogowe **End User License Agreement (EULA)**. Przeczytaj warunki licencji, a następnie kliknij **Accept**, aby kontynuować.
Rozpocznie się instalacja.
Po pomyślnym zakończeniu instalacji system uruchomi się ponownie i przejdzie do strony logowania Windows.
18. Zaloguj się na konto administratora BVRAdmin.
Otworzy się przeglądarka Microsoft Edge ze stroną **DIVAR IP - Konfiguracja systemu**. Na stronie znajduje się typ urządzenia i numer seryjny urządzenia, a także trzy tryby pracy i dostępne dla nich wersje oprogramowania.
Użytkownik musi wybrać żądany tryb pracy oraz żadaną wersję oprogramowania, aby skonfigurować system DIVAR IP all-in-one.
19. Jeśli żądana wersja oprogramowania dla danego trybu pracy nie jest dostępna na dysku lokalnym, należy postępować w następujący sposób:
 - Przejdź na stronę <https://downloadstore.boschsecurity.com/>.
 - Pod kartą **Software** wybrać z listy **BVMS Appliances**, a następnie kliknąć **Select**. Zostanie wyświetlona lista dostępnych pakietów oprogramowania.
 - Odszukać pliki ZIP żądanych pakietów oprogramowania, na przykład **BVMS_[BVMS version]_SystemManager_package_[package version].zip**, i zapisać je na nośniku pamięci, takim jak pamięć USB.
 - Rozpakować pliki na nośniku pamięci. Nie należy zmieniać struktury rozpakowanych plików.
 - Podłączyć nośnik pamięci do urządzenia DIVAR IP all-in-one.



Uwaga!

Przed pierwszym rozpoczęciem obsługi urządzenia należy upewnić się, że jest instalowana najnowsza dostępna wersja oprogramowania. Najnowsze wersje oprogramowania sprzętowego i naszych pakietów uaktualnień można znaleźć w sklepie z plikami do pobrania Bosch Security and Safety Systems pod adresem: <https://downloadstore.boschsecurity.com/>.

Wybór trybu pracy BVMS

Aby używać systemu DIVAR IP all-in-one do pełnego zapisu sygnału wizyjnego i zarządzania:

1. Na stronie **DIVAR IP - Konfiguracja systemu**, wybrać tryb pracy **BVMS** i żadaną do zainstalowania wersję BVMS, następnie kliknąć **Dalej**.
Zostanie BVMS wyświetlona treść umowy licencyjnej.
2. Przeczytać i zaakceptować warunki umowy licencyjnej, a następnie kliknąć przycisk **Instaluj**, aby kontynuować.
Rozpocznie się instalacja, a w oknie dialogowym będzie pokazywany jej postęp. W trakcie instalacji nie wyłączać systemu ani nie usuwać nośnika.
3. Po pomyślnym zainstalowaniu wszystkich pakietów oprogramowania system zostanie uruchomiony ponownie. Po ponownym uruchomieniu systemu nastąpi przekierowanie do pulpitu nawigacyjnego BVMS.
4. Na pulpicie nawigacyjnym BVMS kliknij odpowiednią wybraną aplikację, aby skonfigurować system.

**Uwaga!**

Aby uzyskać więcej informacji, należy zapoznać się z odpowiednim szkoleniem internetowym dotyczącym systemu DIVAR IP all-in-one oraz dokumentacją oprogramowania BVMS. Szkolenie można znaleźć na stronie: www.boschsecurity.com/xc/en/support/training/

Wybór trybu pracy VRM

Aby używać systemu DIVAR IP all-in-one tylko do zapisu sygnału wizyjnego:

1. Na stronie **DIVAR IP - Konfiguracja systemu**, wybrać tryb pracy **VRM** i żądać do zainstalowania wersji VRM, następnie kliknąć **Dalej**.
Zostanie VRM wyświetlona treść umowy licencyjnej.
2. Przeczytać i zaakceptować warunki umowy licencyjnej, a następnie kliknąć przycisk **Instaluj**, aby kontynuować.
Rozpocznie się instalacja, a w oknie dialogowym będzie pokazywany jej postęp. W trakcie instalacji nie wyłączać systemu ani nie usuwać nośnika.
3. Po pomyślnym zainstalowaniu wszystkich pakietów oprogramowania system zostanie uruchomiony ponownie. Po ponownym uruchomieniu zostanie wyświetlone okno logowania systemu Windows.

**Uwaga!**

Więcej informacji można znaleźć w dokumentacji VRM.

Wybór trybu pracy pamięci iSCSI

Aby używać systemu DIVAR IP all-in-one jako rozszerzenia pamięci masowej iSCSI:

1. Na stronie **DIVAR IP - Konfiguracja systemu** wybrać tryb pracy **pamięci masowej iSCSI** i żądać do zainstalowania wersji iSCSI, następnie kliknąć **Dalej**.
Zostanie wyświetlone okno dialogowe instalacji.
2. W oknie dialogowym instalacji kliknąć przycisk **Instaluj**, aby kontynuować.
Rozpocznie się instalacja, a w oknie dialogowym instalacji pokazywany będzie jej postęp. W trakcie instalacji nie wyłączaj systemu i nie wyjmuj nośnika pamięci.
3. Po pomyślnym zainstalowaniu wszystkich pakietów oprogramowania system zostanie uruchomiony ponownie. Po ponownym uruchomieniu zostanie wyświetlone okno logowania systemu Windows.
4. Dodaj system jako rozszerzenie pamięci masowej iSCSI do zewnętrznego serwera BVMS lub VRM za pomocą aplikacji BVMS Configuration Client lub Configuration Manager.

**Uwaga!**

Aby znaleźć więcej szczegółów, przejdź do dokumentacji systemu BVMS lub aplikacji Configuration Manager.

5 Uaktualnianie oprogramowania



Uwaga!

DIVAR IP Software Center w starszych wersjach oprogramowania DIVAR IP all-in-one 7000 (DIP-73xx) było stosowane jako oprogramowanie do zarządzania. Zaleca się aktualizację systemu do DIVAR IP System Manager... Aktualizacja do wersji BVMS wyższych niż 11.1.1 wymaga instalacji oprogramowania DIVAR IP System Manager 2.x.



Uwaga!

Przed pierwszym rozpoczęciem obsługi urządzenia należy upewnić się, że jest instalowana najnowsza dostępna wersja oprogramowania. Najnowsze wersje oprogramowania sprzętowego i naszych pakietów uaktualnień można znaleźć w sklepie z plikami do pobrania Bosch Security and Safety Systems pod adresem: <https://downloadstore.boschsecurity.com/>.

5.1 Zastąpienie DIVAR IP Software Center przez DIVAR IP System Manager

Aby zastąpić DIVAR IP Software Center aplikacją DIVAR IP System Manager w wersji 2.0 (lub wyższej):

1. Uruchom program DIVAR IP Software Center.
2. Oprogramowanie dla trybów pracy można zaktualizować w następujący sposób:
 - Jeśli system pracuje w trybie pracy BVMS, uaktualnij wersję do BVMS **BVMS 11.1.1**.
 - Jeśli system pracuje w trybie pracy VRM, uaktualnij wersję do VRM **VRM 4.03.0025**.
 - Więcej informacji o uaktualnianiu oprogramowania za pomocą DIVAR IP Software Center zawiera *Aktualizacja oprogramowania za pomocą programu Software Center*, Strona 16.
3. Przejdź na stronę <https://downloadstore.boschsecurity.com/>.
4. Pod kartą **Software** wybrać z listy **BVMS Appliances**, a następnie kliknąć **Select**. Zostanie wyświetlona lista dostępnych pakietów oprogramowania.
5. Znajdź plik ZIP **SystemManager_[software version 2.0.0 or higher].zip** i zapisz go na nośniku pamięci, takim jak pamięć USB.
6. Rozpakuj plik na nośniku pamięci.
7. Podłącz nośnik pamięci do urządzenia DIVAR IP all-in-one.
8. Na nośniku pamięci masowej odszukaj plik instalacyjny **SystemManager_x64_software version].exe** i kliknij go dwukrotnie, aby rozpocząć instalację.
9. Przed rozpoczęciem instalacji zostanie wyświetlone okno dialogowe z umową licencyjną. Przeczytaj umowę licencyjną, zaznacz pole wyboru, aby ją zaakceptować, a następnie kliknij **Instaluj**, aby kontynuować.
Zostanie wyświetlone okno dialogowe **DIVAR IP System Manager setup** z żądaniem aktualizacji SuperDoctor.

Uwaga!

Zaktualizuj usługę SuperDoctor

Oprogramowanie DIVAR IP System Manager w wersji 2.0 (lub wyższej) wymaga aktualizacji usługi SuperDoctor. Aktualizacja zastąpi istniejące ustawienia aplikacji SuperDoctor. Po aktualizacji należy ponownie zastosować określone ustawienia. Przed rozpoczęciem aktualizacji należy wykonać kopię konfiguracji.

Po aktualizacji usługi SuperDoctor zostanie ona dezaktywowana, a hasło aplikacji SuperDoctor zostanie zresetowane do hasła domyślnego **DivaripSD5**. Bosch zaleca zmianę hasła domyślnego natychmiast po pierwszym zalogowaniu się do aplikacji SuperDoctor,



10. Kliknij **Install**, aby kontynuować.
Rozpocznie się aktualizacja DIVAR IP System Manager.
Proces instalacji może zająć kilka minut. Nie należy wyłączać systemu i nie usuwać nośnika podczas instalacji.
Uwaga: podczas instalacji systemu DIVAR IP System Manager w wersji 2.0 (lub wyższej) DIVAR IP Software Center zostanie automatycznie odinstalowany.
Podczas instalacji systemu DIVAR IP System Manager w wersji 2.0 (lub wyższej) usługa monitorowania SuperDoctor zostanie wyłączona. Należy uaktywnić ją po instalacji.

Uaktywnienie usługi SuperDoctor

Aby uaktywnić usługę SuperDoctor:

1. Na komputerze w folderze **Tools** kliknij prawym przyciskiem myszy skrypt **startSD5Service**, a następnie kliknij polecenie **Run with PowerShell**.
2. Kliknij dwukrotnie ikonę **SuperDoctor 5 Web** na pulpicie
3. Zaloguj się do interfejsu sieciowego przy użyciu następujących domyślnych danych uwierzytelniających:
 - Nazwa użytkownika: **admin**
 - Hasło: **DivaripSD5**
4. Kliknij kartę **Configuration**, a następnie kliknij **Account Setting** i zmień hasło domyślne.
Uwaga: firma Bosch stanowczo zaleca zmianę hasła domyślnego natychmiast po pierwszym zalogowaniu się do aplikacji **SuperDoctor**.
5. Należy ponownie zastosować ustawienia SuperDoctor, które zostały zastosowane przed zastąpieniem DIVAR IP Software Center.

5.2

Aktualizacja oprogramowania za pomocą programu System Manager

Za pomocą aplikacji DIVAR IP System Manager można uaktualnić zainstalowane oprogramowanie w systemie.






Uwaga!

Zmiana zainstalowanego oprogramowania na wcześniejszą wersję nie jest obsługiwana.

Aby uaktualnić zainstalowane oprogramowanie:

1. Przejdź na stronę <https://downloadstore.boschsecurity.com/>.
2. Pod kartą **Software** wybrać z listy **BVMS Appliances**, a następnie kliknąć **Select**.
Zostanie wyświetlona lista dostępnych pakietów oprogramowania.
3. Odszukać pliki ZIP żądanych pakietów oprogramowania, na przykład **BVMS_[BVMS version]_SystemManager_package_[package version].zip**, i zapisać je na nośniku pamięci, takim jak pamięć USB.
4. Rozpakować pliki na nośniku pamięci. Nie należy zmieniać struktury rozpakowanych plików.
5. Uruchom program DIVAR IP System Manager:
 - Jeśli użytkownik jest zalogowany do systemu Windows za pomocą konta administratora **BVRAdmin**, należy dwukrotnie kliknąć ikonę DIVAR IP System Manager na pulpicie systemu Windows.
Uruchomi się DIVAR IP System Manager.

- Jeśli system BVMS działa w trybie pracy, kliknij ikonę DIVAR IP System Manager na pulpicie BVMS i zaloguj się do konta administratora BVRAdmin. DIVAR IP System Manager otworzy się w trybie pełnoekranowym (okno dialogowe można zamknąć, naciskając Alt+ F4).
6. Wyświetli się strona **Pakiety oprogramowania**, w górnej części strony wyświetlany jest typ i numer seryjny urządzenia.
- W kolumnie **Nazwa** widoczne są wszystkie aplikacje systemu DIVAR IP System Manager zainstalowane w systemie, a także wszystkie pozostałe aplikacje systemu DIVAR IP System Manager, które zostały wykryte przez system na dysku **Images** lub nośniku pamięci masowej.
 - W kolumnie **Zainstalowana wersja** widoczna jest wersja aplikacji systemu, która jest aktualnie zainstalowana w systemie.
 - W kolumnie **Stan** jest widoczny stan odpowiedniej aplikacji systemu:
 - Ikona  wskazuje, że system nie wykrył żadnych nowszych wersji zainstalowanego oprogramowania na dysku **Images** lub nośniku pamięci masowej. **Uwaga:** aby korzystać z najnowszej wersji oprogramowania, należy sprawdzić dostępne wersje oprogramowania dostępne w sklepie Bosch Security and Safety Systems na stronie <https://downloadstore.boschsecurity.com/>
 - Ikona  wskazuje, że system wykrył nowsze wersje zainstalowanego oprogramowania na dysku **Images** lub nośniku pamięci masowej. Ta ikona wyświetla się również wtedy, gdy system wykrył w systemie aplikację, która nie została jeszcze zainstalowana.
 - W kolumnie **Dostępna wersja** są dostępne nowsze wersje zainstalowanych aplikacji. Te wersje zostały wykryte przez system na dysku **Images** lub nośniku pamięci masowej. W tej kolumnie wyświetlają się również dostępne wersje wykrytych aplikacji oprogramowania, które nie zostały jeszcze zainstalowane w systemie. **Uwaga:** wyświetlają się tylko nowsze wersje zainstalowanych aplikacji. Zmiana aplikacji oprogramowania na wcześniejszą wersję nie jest obsługiwana.
7. W kolumnie **Nazwa** kliknij odpowiedni przycisk opcji, aby wybrać aplikację, która ma być uaktualniona lub zainstalowana.
8. W kolumnie **Dostępna wersja** wybierz żadaną wersję, do której ma zostać uaktualniona aplikacja programowa lub która ma być instalowana, a następnie kliknij przycisk **Dalej**. W razie potrzeby wyświetli się okno dialogowe umowy licencyjnej.
9. Przeczytaj i zaakceptuj warunki umowy licencyjnej, a następnie kliknij **Instaluj**, aby kontynuować.
- Instalacja rozpocznie się, a na stronie dialogowej wyświetlane są informacje o postępie instalacji. W trakcie instalacji nie wyłączaj systemu ani nie usuwaj nośnika.
10. Po pomyślnym zainstalowaniu wszystkich pakietów oprogramowania otrzymasz komunikat **Instalacja zakończyła się pomyślnie**. w górnej części strony.
11. Jeśli instalacja nie powiedzie się, zostanie wyświetlony komunikat **Instalacja nie powiodła się**. i pojawi się ikona . W takim przypadku należy nacisnąć przycisk F5, aby wrócić na stronę **Pakiety oprogramowania**. Pobierz po raz kolejny odpowiednie pakiety oprogramowania i spróbuj ponownie.
- Jeśli problem występuje nadal, skontaktuj się z pomocą techniczną.

5.3 Aktualizacja oprogramowania za pomocą programu Software Center

Uaktualnianie oprogramowania

Aby uaktualnić zainstalowane oprogramowanie:

1. Pobierz żądane pakiety oprogramowania ze strony z **materiałami do obrania** i zapisz je na dysku lokalnym lub nośniku pamięci. Następnie podłącz nośnik pamięci do systemu.
2. Uruchom program DIVAR IP Software Center.
Zostanie wyświetlona strona **Installed software**.
3. W sekcji **Upgrades** wyświetlane są dostępne uaktualnienia. Kliknij **Upgrade**, aby uaktualnić żądane oprogramowanie.
Zostanie wyświetlone okno dialogowe **Upgrade** z pakietami oprogramowania wchodzącymi w skład uaktualnienia.
Uwaga: uaktualnienie spowoduje zapisanie wszystkich ustawień, zaktualizowanie oprogramowania oraz ponowne uruchomienie systemu.
4. Kliknij przycisk **Install**, aby kontynuować.
Rozpocznie się instalacja pakietów oprogramowania. Cały ten proces może potrwać kilka minut. Nie wyłączaj systemu ani nie usuwaj nośnika pamięci.
Po zakończeniu instalacji system uruchamia się ponownie.

6 Zdalne połączenie z systemem

Użytkownik może nawiązać zdalne połączenie z systemem DIVAR IP all-in-one i uzyskać do niego dostęp przez Internet.

Aby utworzyć połączenie zdalne, należy wykonać następujące czynności:

1. *Ochrona systemu przed nieautoryzowanym dostępem, Strona 17.*
2. *Konfigurowanie przekierowania portów, Strona 17.*
3. *Wybór odpowiedniego klienta, Strona 17.*

Możesz także połączyć się z urządzeniem DIVAR IP all-in-one za pośrednictwem Bosch Remote Portal i wykorzystać aktualne i przyszłe funkcje dostępne dzięki Remote Portal. Więcej informacji znajduje się w *Nawiązywanie połączenia z Remote Portal, Strona 18.*

6.1 Ochrona systemu przed nieautoryzowanym dostępem

W celu zabezpieczenia systemu przed nieautoryzowanym dostępem należy ustawić silne hasła przed połączeniem systemu z Internetem. Im silniejsze hasło, tym lepiej system będzie chroniony przed dostępem nieuprawnionych osób i atakami złośliwego oprogramowania.

6.2 Konfigurowanie przekierowania portów

Aby mieć dostęp do systemu DIVAR IP all-in-one przez Internet za pośrednictwem routera z funkcjonalnością NAT/PAT, w systemie DIVAR IP all-in-one i routerze należy skonfigurować ustawienia przekierowywania przez porty.

Aby skonfigurować przekierowanie portów:

- ▶ Na routerze internetowym wprowadź następujące reguły w ustawieniach funkcji przekierowywania przez porty:
 - port 5322 do obsługi dostępu przez tunel SSH przy użyciu aplikacji BVMS Operator Client.
Uwaga: to połączenie ma zastosowanie tylko w trybie pracy BVMS.
 - Port 443 do obsługi dostępu przez protokół HTTPS do programu VRM za pomocą aplikacji Video Security Client lub Video Security App.
Uwaga: to połączenie ma zastosowanie tylko w trybie pracy BVMS lub VRM.

Dostęp do urządzenia DIVAR IP all-in-one jest teraz możliwy za pośrednictwem Internetu.

6.3 Wybór odpowiedniego klienta

Dostępne są dwie opcje zdalnego połączenia z systemem DIVAR IP all-in-one:

- *Połączenie zdalne za pomocą aplikacji BVMS Operator Client., Strona 17.*
- *Połączenie zdalne za pomocą aplikacji Video Security, Strona 18.*



Uwaga!

Zgodność wersji BVMS Operator Client lub Video Security App zależy od wersji oprogramowania BVMS lub VRM zainstalowanego w DIVAR IP.

Szczegółowe informacje można znaleźć w odpowiedniej dokumentacji oprogramowania i materiałach szkoleniowych.

6.3.1 Połączenie zdalne za pomocą aplikacji BVMS Operator Client.



Uwaga!

To połączenie ma zastosowanie tylko w trybie pracy BVMS.

Aby nawiązać zdalne połączenie przy użyciu aplikacji BVMS Operator Client:

1. Zainstaluj program BVMS Operator Client na stacji roboczej klienta.
2. Po pomyślnym zakończeniu instalacji uruchom aplikację Operator Client za pomocą

skrót  na pulpicie.

3. Wprowadź następujące informacje, a następnie kliknij przycisk **OK**.

Nazwa użytkownika: admin (lub inny skonfigurowany użytkownik)

Hasło: hasło użytkownika

Połączenie: ssh://[publiczny_adres_IP_rozwiazania_DIVAR-IP_all-in-one]:5322

6.3.2

Połączenie zdalne za pomocą aplikacji Video Security



Uwaga!

To połączenie ma zastosowanie tylko w trybie pracy BVMS lub VRM.

Aby nawiązać zdalne połączenie przy użyciu aplikacji Video Security App:

1. W sklepie App Store firmy Apple wyszukaj aplikację Bosch Video Security.
2. Zainstaluj aplikację Video Security na swoim urządzeniu z systemem iOS.
3. Uruchom aplikację Video Security.
4. Dotknij pola **Dodaj**.
5. Wprowadź publiczny adres IP lub nazwę DynDNS.
6. Upewnij się, że jest włączona funkcja bezpiecznych połączeń (SSL).
7. Dotknij pola **Dodaj**.
8. Wprowadź następujące informacje:

Nazwa użytkownika: admin (lub inny skonfigurowany użytkownik)

Hasło: hasło użytkownika

6.4

Łączenie z serwerem Enterprise Management Server

Do centralnego zarządzania wieloma systemami DIVAR IP all-in-one w trybie pracy BVMS można użyć programu BVMS Enterprise Management Server zainstalowanego na osobnym serwerze.

Szczegółowe informacje na temat konfiguracji i obsługi BVMS Enterprise System można znaleźć w dokumentacji i materiałach szkoleniowych dotyczących BVMS.

6.5

Nawiązywanie połączenia z Remote Portal

Warunki wstępne

Połączenie Remote Portal

Aby podłączyć urządzenia DIVAR IP all-in-one z portalem Remote Portal, należy upewnić się, że występują następujące warunki wstępne:

- W urządzeniu musi być zainstalowane oprogramowanie DIVAR IP System Manager w wersji 2.0 (lub wyższej).
- Aby zainstalować oprogramowanie DIVAR IP System Manager w wersji 2.0 (lub wyższej), urządzenie DIVAR IP musi obsługiwać oprogramowanie BVMS w wersji 11.1.1 lub wyższej.
- Należy utworzyć konto w portalu Remote Portal.

Komunikacja z Remote Portal

Wymagania w zakresie łączności dotyczące komunikacji z Remote Portal.

Uwaga: wszystkie połączenia są połączeniami wychodzącymi.

HTTPS (port 443)

- <https://api.remote.boschsecurity.com/rest/iot/devices>
- <https://sw-repo-remote.s3.eu-central-1.amazonaws.com>

MQTTS (port 8883)

- <mqtt://mqtt.bosch-iot-hub.com:8883>

6.5.1**Tworzenie konta w portalu Remote Portal**

Aby utworzyć konto w portalu Remote Portal:

1. Przejdź na stronę <https://remote.boschsecurity.com/login>.
2. Kliknij **Sign up**.
3. Wprowadź nazwę firmy i adres e-mail.
4. Wybierz region firmy.
5. Przeczytaj warunki oraz uwagi dotyczące ochrony danych, a następnie zaznaczyc pola wyboru, aby je zaakceptować.
6. Kliknij Wybierz **Sign up**, aby utworzyć konto.

6.5.2**Rejestrowanie urządzeń DIVAR IP all-in-one w portalu Remote Portal**

Aby zarejestrować urządzenie DIVAR IP all-in-one w portalu Remote Portal:

1. Uruchom program DIVAR IP System Manager.
2. Kliknij kartę **Remote Portal connection**.
3. Jeśli masz już konto w portalu Remote Portal, wprowadź adres e-mail i hasło, a następnie kliknij opcję , aby zarejestrować urządzenie DIVAR IP all-in-one w portalu Remote Portal.

**Uwaga!**

SingleKey ID

Firma Bosch wprowadziła SingleKey ID jako dostawcę identyfikacji (IdP), aby umożliwić scentralizowane logowanie do wszystkich aplikacji, usług i platform Bosch.

Aby połączyć urządzenie z portalem Remote Portal za pomocą SingleKey ID, należy postępować zgodnie z instrukcjami wyświetlanymi na ekranie.

**Uwaga!**

Ustawienie **Default commissioning company**

Jeśli adres e-mail jest przypisany do wielu kont firmowych, upewnij się, że urządzenie DIVAR IP all-in-one zostało zarejestrowane na odpowiednim koncie firmy.

- Zaloguj się na swoje konto Remote Portal.

- Idź do **User settings > My companies**, wybierz żądane konto, a następnie wybierz opcję **Default commissioning company**.

Uwaga: ustawienie **Default commissioning company** automatycznie wygasa po upływie 12 godzin.

4. Jeśli jeszcze nie masz konta Remote Portal, kliknij , aby najpierw utworzyć konto Remote Portal. Patrz .

6.5.3**Wyrejestrowanie urządzeń DIVAR IP all-in-one z aplikacji Remote Portal**

Aby wyrejestrować urządzenie DIVAR IP all-in-one z Remote Portal:

1. Uruchom DIVAR IP System Manager.
2. Kliknij Karta **Remote Portal connection**.

3. Kliknij przycisk **Wyrejestruj**, aby wyrejestrować urządzenie DIVAR IP all-in-one z aplikacji Remote Portal.

Uwaga: wyrejestrowanie urządzenia z Remote Portal nie powoduje usunięcia konfiguracji urządzenia w portalu Remote Portal. Aby usunąć konfigurację urządzenia, należy zalogować się do odpowiedniego konta portalu Remote Portal.

7 Obsługa serwisowa

7.1 Logowanie do konta administratora

Logowanie do konta administratora w trybie pracy BVMS

Aby zalogować się do konta administratora w trybie pracy BVMS:

1. Nacisnąć Ctrl+Alt+Del na pulpicie BVMS.
2. Nacisnąć i przytrzymać lewy klawisz Shift bezpośrednio po kliknięciu **Przełącz użytkownika**.
3. Ponownie nacisnąć Ctrl+Alt+Del.
4. Wybierz użytkownika **BVRAdmin** i wprowadź hasło ustawione podczas konfiguracji systemu. Następnie nacisnąć przycisk Enter (Zatwierdź).

Uwaga: Aby wrócić do pulpitu BVMS, należy nacisnąć Ctrl+Alt+Del i kliknąć **Przełącz użytkownika** lub **Wyloguj**. System automatycznie powróci do pulpitu BVMS bez ponownego uruchomienia systemu.

Logowanie do konta administratora w trybie pracy VRM lub iSCSI

Aby zalogować się do konta administratora w trybie pracy VRM lub iSCSI:

- ▶ Na ekranie logowania systemu Windows nacisnąć Ctrl+Alt+Del i wprowadzić hasło **BVRAdmin**.

7.2 Monitorowanie systemu

7.2.1 Monitorowanie systemu za pomocą aplikacji SuperDoctor podczas pracy z DIVAR IP Remote Portal

Systemy DIVAR IP all-in-one są wyposażone w fabrycznie zainstalowaną aplikację **SuperDoctor**, która umożliwia monitorowanie systemu.

Włączanie funkcji monitorowania

Aby włączyć funkcję monitorowania:

1. Zaloguj się do konta administratora (patrz *Logowanie do konta administratora, Strona 21*).
2. Na komputerze w folderze **Tools** kliknij prawym przyciskiem myszy skrypt **startSD5Service**, a następnie kliknij polecenie **Run with PowerShell**.
3. Kliknij dwukrotnie ikonę **SuperDoctor 5 Web** na pulpicie
4. Zaloguj się do interfejsu sieciowego przy użyciu następujących domyślnych danych uwierzytelniających:
 - Nazwa użytkownika: **admin**
 - Hasło: **DivaripSD5**
5. Kliknij kartę **Configuration**, a następnie kliknij **Account Setting** i zmień hasło domyślne.
Uwaga: firma Bosch stanowczo zaleca zmianę hasła domyślnego natychmiast po pierwszym zalogowaniu się do aplikacji **SuperDoctor**.
6. Na karcie **Configuration** kliknij **Alert Configuration**.
7. Włącz funkcję **SNMP Trap** i wprowadź adres IP odbiornika komunikatów Trap protokołu SNMP.

Wyłączanie funkcji monitorowania

Aby wyłączyć funkcję monitorowania:

1. Zaloguj się do konta administratora (patrz *Logowanie do konta administratora, Strona 21*).
2. Na komputerze w folderze **Tools** kliknij prawym przyciskiem myszy skrypt **stopSD5Service**, a następnie kliknij polecenie **Run with PowerShell**.

7.2.2

Monitorowanie systemu za pomocą aplikacji SuperDoctor podczas pracy z DIVAR IP Software Center

System zawiera narzędzia do monitorowania stanu.

Aby uaktywnić funkcję monitorowania, trzeba się zalogować na koncie administratora (**BVRAdmin**).

1. Należy zalogować się do konta administratora **BVRAdmin**. Więcej informacji znajduje się w *Logowanie do konta administratora, Strona 21*.
2. Na komputerze w folderze **Tools** kliknij prawym przyciskiem myszy skrypt **Enable_SuperDoctor_5_Service**, a następnie kliknij polecenie **Uruchom jako administrator**.
3. W tym samym folderze kliknij dwukrotnie ikonę narzędzia **SuperDoctor 5 Web**.
4. Zaloguj się w internetowym interfejsie przy użyciu następujących domyślnych poświadczeń
: Nazwa użytkownika: **admin**
Hasło: **DivaripSD5**
5. Kliknij kartę **Configuration**, następnie kliknij **Password Settings** i zmień domyślne hasło.
6. Kliknij kartę **Configuration**, a następnie kliknij **Alert Configuration**.
7. Włącz funkcję **SNMP Trap** i wprowadź adres IP odbiornika komunikatów Trap protokołu SNMP.

7.2.3

Monitorowanie systemu za pomocą interfejsu IPMI

Urządzenie DIVAR IP all-in-one 7000 ma dedykowany port IPMI na tylnej ścianie.

Interfejs IPMI umożliwia dostęp, monitorowanie, diagnozowanie i zarządzanie systemem DIVAR IP all-in-one 7000 jako serwerem zdalnym.

W każdym urządzeniu DIVAR IP all-in-one 7000 jest fabrycznie skonfigurowany użytkownik ADMIN z hasłem początkowym. Hasło początkowe jest unikalne dla każdej jednostki. Podano je na etykiecie z tyłu urządzenia, pod portem IPMI.

Bosch zdecydowanie zaleca zmianę hasła początkowego podczas konfiguracji IPMI oraz zapisanie nowego hasła w bezpiecznym miejscu.



Uwaga!

Ze względów bezpieczeństwa nie można na stałe podłączać urządzenia do sieci publicznej przez port IPMI.

Aby skonfigurować ustawienia IPMI:

1. Włącz urządzenie i naciśnij podczas rozruchu klawisz Del, aby wejść do konfiguracji systemu BIOS.
2. W konfiguracji systemu BIOS przejdź do karty **IPMI**.
3. Wybierz opcję **BMC Network Configuration**, a następnie naciśnij klawisz Enter (Zatwierdź).
4. W następnym oknie dialogowym wybierz opcję **Update IPMI LAN Configuration**, a następnie naciśnij klawisz Enter (Zatwierdź).
Pojawi się okno dialogowe **Update IPMI LAN Configuration**.
5. W oknie dialogowym **Update IPMI LAN Configuration** wybierz opcję **Yes**, a następnie naciśnij klawisz Enter (Zatwierdź).
6. Ustaw żądane parametry konfiguracji sieci.
7. Naciśnij klawisze F4 i Enter (Zatwierdź) aby zapisać zmiany i wyjść z systemu BIOS. Urządzenie DIVAR IP all-in-one 7000 uruchomi się ponownie.

7.3 Pobieranie plików rejestrów programu DIVAR IP System Manager

Aplikacja DIVAR IP System Manager zawiera dedykowany skrypt, który upraszcza gromadzenie plików rejestrów.

Aby zgromadzić pliki rejestru DIVAR IP System Manager:

1. Zaloguj się do konta administratora (patrz *Logowanie do konta administratora, Strona 21*).
2. W menu **Start** systemu Windows kliknij **Export System Manager Logs**. Skrypt wyeksportuje pliki rejestru do folderu `Documents\Bosch` i tworzy plik ZIP o następującej strukturze nazwy `SysMgrLogs-[date]_[time]`.
. Pliku zip można użyć do dołączenia do szczegółowego opisu błędu.

7.4 Przywracanie ustawień fabrycznych

Poniżej opisano procedurę przywracania fabrycznych ustawień obrazu.

Aby przywrócić fabryczne ustawienia obrazu w jednostce:

1. W trakcie testu POST systemu BIOS uruchom jednostkę i naciśnij klawisz **F7**, aby otworzyć środowisko Windows PE.
Zostanie wyświetlone menu Przywracanie ustawień.
2. Należy wybrać jedną z poniższych opcji:
 - **Początkowa konfiguracja fabryczna (wszystkie dane w systemie zostaną utracone):** ta opcja powoduje usunięcie danych ze wszystkich partycji dysku twardego i nadpisanie partycji systemu operacyjnego domyślnym obrazem.
 - **Początkowa konfiguracja fabryczna (nadpisywanie istniejących danych):** ta opcja służy do usuwania i zastępowania danych ze wszystkich partycji HDD. Ponadto nadpisuje partycję systemu operacyjnego za pomocą domyślnego obrazu.
Uwaga: ta procedura może trwać bardzo długo.
 - **Odzyskiwanie systemu (powrót do ustawień fabrycznych):** ta opcja powoduje zastąpienie partycji systemu operacyjnego domyślnym obrazem i importuje istniejące wirtualne dyski twarde z dysków twardych podczas odzyskiwania.

Uwaga:

Opcja **Odzyskiwania systemu** nie usuwa materiału wideo zapisanego na dyskach twardych z danymi. Zastępuje jednak kompletną partycję systemu operacyjnego (w tym ustawienia systemu zarządzania obrazem) konfiguracją domyślną. Aby po odzyskiwaniu systemu można było przejść do istniejącego nagranych materiału wideo, należy przed odzyskiwaniem wyeksportować konfigurację systemu zarządzania sygnałem wizyjnym a po odzyskiwaniu ją zaimportować.



Uwaga!

W trakcie tej konfiguracji nie wolno wyłączać jednostki. Mogłoby to spowodować uszkodzenie nośnika przywracania danych.

3. Jednostka zostanie uruchomiona z poziomu nośnika przywracania danych. Jeśli konfiguracja przebiegnie pomyślnie, kliknij przycisk **Tak**, aby uruchomić system ponownie.
4. System Windows przeprowadzi wstępną konfigurację systemu operacyjnego.
Po zakończeniu procesu konfiguracji przez system Windows jednostka zostanie uruchomiona ponownie.
5. Po ponownym uruchomieniu jednostki zostaną zainstalowane ustawienia fabryczne.

8 Informacje dodatkowe

8.1 Dodatkowa dokumentacja i oprogramowanie

Więcej informacji, dokumentację i oprogramowanie do pobrania można znaleźć na stronie danego produktu w katalogu produktów:

<http://www.boschsecurity.com>

Najnowsze oprogramowanie oraz dostępne pakiety aktualizacyjne można znaleźć w materiałach do pobrania Bosch Security and Safety Systems na stronie:

<https://downloadstore.boschsecurity.com/>

8.2 Usługi pomocy technicznej i Bosch Academy



Pomoc techniczna

Nasza **pomoc techniczna** jest dostępna na stronie www.boschsecurity.com/xc/en/support/.



Akademia Bosch Building Technologies

Odwiedź witrynę Akademii Bosch Building Technologies, aby uzyskać dostęp do **kursów szkoleniowych, samouczków wideo i dokumentów**: www.boschsecurity.com/xc/en/support/training/

Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Holandia

www.boschsecurity.com

© Bosch Security Systems B.V., 2023

Building solutions for a better life.

202309021111