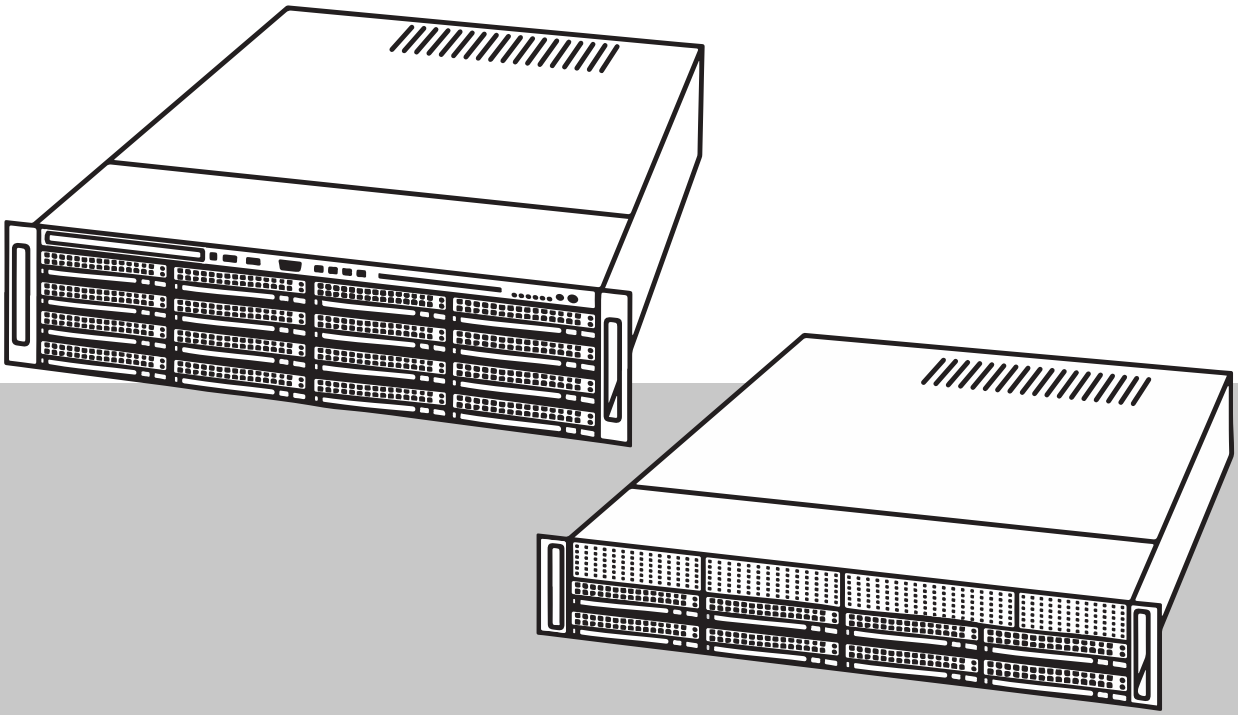
DIVAR IP all-in-one 7000 2U | DIVAR IP all-in-one 7000 3U

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



pl Instrukcja obsługi

Spis treści

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 przemyślne 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 Zalecenia dotyczące bezpieczeństwa danych

Ze względu na bezpieczeństwo danych należy przestrzegać następujących zaleceń:

- Fizyczny dostęp do systemu powinien mieć wyłącznie autoryzowany personel. Stanowczo zalecamy, aby umieścić system w obszarze o kontrolowanym dostępie, tak aby zapobiec ewentualności fizycznego ingerowania w system.
- W celu aktualizowania zabezpieczeń systemu operacyjnego można używać funkcji aktualizacji systemu Windows przez Internet lub odpowiednich miesięcznych zbiorczych poprawek instalowanych w trybie offline.
- Stanowczo zalecamy, aby dostęp do sieci lokalnej przyznawać tylko zaufanym urządzeniom. Szczegółowe informacje znajdują się w uwagach technicznych Uwierzytelnianie sieciowe 802.1X i w Przewodniku dotyczącym ochrony danych oraz urządzeń wizyjnych IP firmy Bosch. Oba dokumenty są dostępne w internetowym katalogu produktów.
- W przypadku dostępu przez sieci publiczne należy używać wyłącznie zabezpieczonych (szyfrowanych) kanałów komunikacyjnych.

1.3 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 zagrożenia 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.

2 Wprowadzenie

Tryby pracy

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

– Pełny system zapisu sygnału wizyjnego i zarządzania, z wykorzystaniem podstawowych składników i usług modułów BVMS oraz VRM: ten tryb pozwala korzystać z zaawansowanych funkcji zarządzania sygnałem wizyjnym, takich jak obsługa zdarzeń i alarmów.
– System samego zapisu sygnału wizyjnego, z wykorzystaniem podstawowych składników i usług modułu VRM.
– Rozszerzenie pamięci masowej iSCSI dla systemu BVMS lub VRM, który działa na innym urządzeniu.

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).

DIVAR IP Software Center

DIVAR IP Software Center to centralny interfejs użytkownika służący do konfiguracji oprogramowania, aktualizacji oraz wyboru trybu pracy.
Po zakończeniu instalacji DIVAR IP Software Center należy wybrać żądany tryb pracy, aby skonfigurować system.
Za pomocą DIVAR IP Software Center można również aktualizować i uaktualniać 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/

3 Ogólne informacje o systemie

Systemy DIVAR IP all-in-one 7000 są obsługiwane przez system operacyjny Microsoft Windows Server IoT 2019 for Storage Standard. W systemie operacyjnym dostępny jest interfejs użytkownika służący do wstępnej konfiguracji serwera, ujednoliconego 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.

Uwaga!
Informacje przedstawione w niniejszym rozdziale dotyczą modeli urządzeń DIVAR IP all-in-one 7000, które są fabrycznie wyposażone w dyski twarde.
System operacyjny pustych urządzeń, w których zamontowano dyski twarde innych producentów, zostanie uruchomiony normalnie, ale dodane dyski twarde należy przed pierwszą konfiguracją oprogramowania skonfigurować za pomocą aplikacji **MegaRAID Storage Manager**.
Więcej informacji można znaleźć w instrukcji obsługi.

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: ustawiane przy pierwszym logowaniu.
  Wymagania dotyczące hasła:
  - Co najmniej 14 znaków.
  - Co najmniej jedna wielka litera.
  - Co najmniej jedna mała litera.
  - Co najmniej jedna cyfra.

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 Pierwsze logowanie i konfiguracja systemu

Uwaga!
Usilnie zaleca się, by nie zmieniać żadnych ustawień systemu operacyjnego. Zmiana ustawień systemu operacyjnego może spowodować nieprawidłowe działanie systemu.

Uwaga!
W celu wykonywania zadań administracyjnych należy się zalogować na koncie 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 moduł DIVAR IP all-in-one 7000 i kamery do sieci.
2. Włącz moduł.
   Wykonywane są procedury konfiguracji Microsoft Windows Server IoT 2019 for Storage Standard. Cały ten proces może potrwać kilka minut. Nie wyłączaj 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 treści dokumentów Microsoft Software License Terms i EULA.
4. Kliknij **Akceptuj**, aby zaakceptować postanowienia licencyjne, i poczekaj na ponowne uruchomienie systemu Windows. Cały ten proces może potrwać kilka minut. Nie wyłączaj 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.

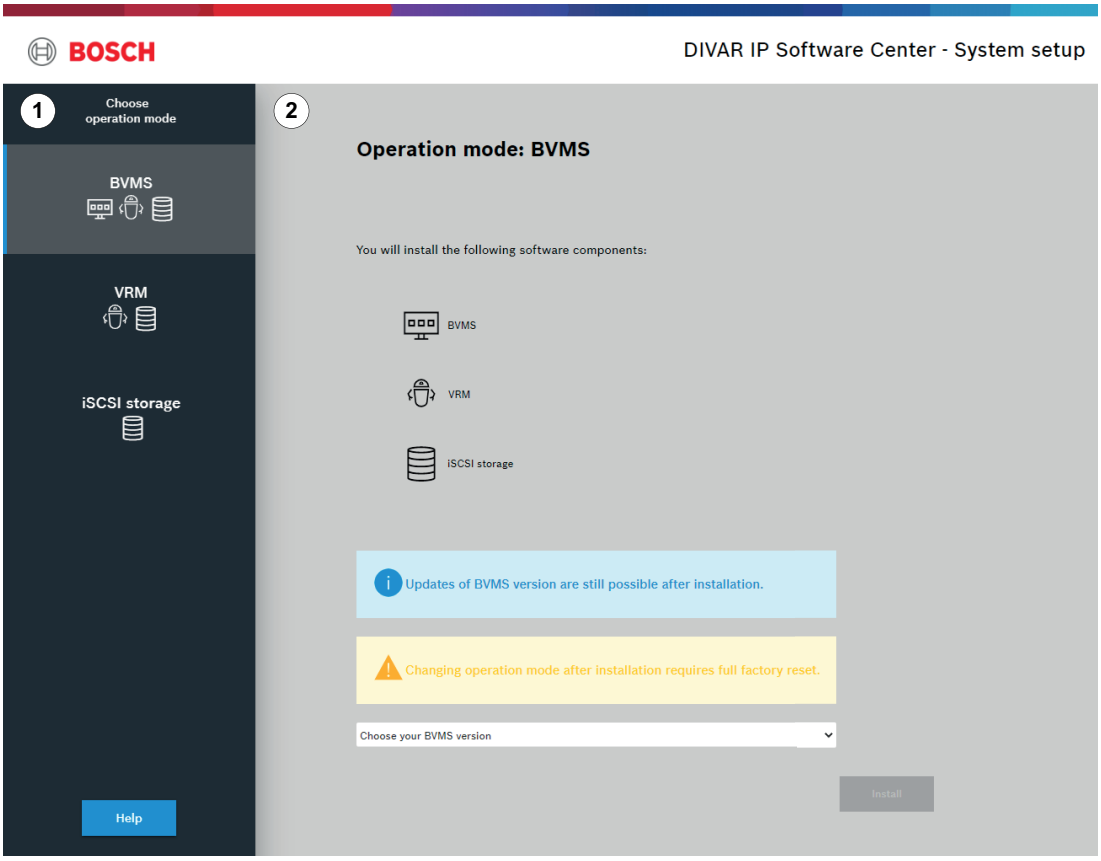
   Naciśnij ENTER**.**
   Zostanie wyświetlona strona **wyboru oprogramowania**.
6. Kliknij plik instalacji DIVAR IP Software Center.
   Rozpocznie się proces instalacji DIVAR IP Software Center. Po ukończeniu instalacji, system Windows zostanie uruchomiony ponownie i nastąpi przekierowanie na stronę logowania systemu Windows.
   Uwaga: jeśli nie masz pliku instalacyjnego DIVAR IP Software Center zapisanego na dysku lokalnym, włóż nośnik pamięci (napęd flash USB, DVD-ROM) z plikiem instalacyjnym. Nośnik jest automatycznie skanowany w poszukiwaniu pliku instalacyjnego DIVAR IP Software Center, który zostanie następnie wyświetlony na stronie **wyboru oprogramowania**.
7. Zaloguj się na konto administratora.
   Przeglądarka Microsoft Edge uruchamia się automatycznie.

8. Wprowadź nazwę użytkownika **BVRAdmin** i hasło administratora, a następnie kliknij przycisk **Zaloguj się**. Uruchomi się
DIVAR IP Software Center i ładowane są pakiety oprogramowania.
Uwaga: Jeśli odpowiednie pakiety oprogramowania żądanego trybu pracy nie są dostępne na dysku lokalnym, należy włożyć nośnik pamięci z pakietami oprogramowania, aby kontynuować konfigurację systemu.
Najnowsze oprogramowanie oraz dostępne pakiety aktualizacyjne można znaleźć w **materiałach do pobrania** Bosch Security and Safety Systems na stroni:
https://downloadstore.boschsecurity.com/

4.1 Wybór trybu pracy

W aplikacji DIVAR IP Software Center należy wybrać żądany tryb pracy, aby skonfigurować system DIVAR IP all-in-one 7000.

Uwaga!
Zmiana trybu pracy po instalacji wymaga przeprowadzenia pełnego resetu do ustawień fabrycznych.



1	Okno wyboru
2	Okno główne

Patrz
– *Tryby pracy, Strona 6*

4.1.1 Używanie jako pełnego systemu zapisu sygnału wizyjnego i zarządzania

Aby używać systemu DIVAR IP do zapisu sygnału wizyjnego i zarządzania:

1. W oknie wyboru kliknij **BVMS**.
   Składniki oprogramowania, które zostaną zainstalowane, są widoczne w oknie głównym.
2. Wybierz żądaną wersję BVMS z listy, a następnie kliknij **Install**.
   Wyświetlane jest okno dialogowe **BVMS installation** pokazujące pakiety oprogramowania, które zostaną zainstalowane.
3. Kliknij **Install**, aby kontynuować.
   Rozpocznie się instalacja pakietów oprogramowania. Cały ten proces może potrwać kilka minut. Nie wyłączaj systemu ani nie usuwaj nośnika pamięci.
   Uwaga: jeśli podczas instalacji wystąpi błąd, kliknij **Finish**. Spowoduje to ponowne uruchomienie systemu. Po ponownym uruchomieniu zaktualizuj odpowiednie pakiety oprogramowania i kontynuuj instalację.
4. Po zainstalowaniu wszystkich pakietów kliknij **Finish**.
   System zostanie uruchomiony ponownie. Po ponownym uruchomieniu systemu nastąpi przekierowanie do pulpitu nawigacyjnego BVMS.
5. Na pulpicie nawigacyjnym BVMS kliknij odpowiednią wybraną aplikację, aby skonfigurować system.

Uwaga!
Więcej informacji można znaleźć w dokumentacji BVMS.

4.1.2 Używanie tylko do zapisu sygnału wizyjnego

Aby używać systemu DIVAR IP tylko do zapisu sygnału wizyjnego

1. W oknie wyboru kliknij **VRM**.
   Składniki oprogramowania, które zostaną zainstalowane, są widoczne w oknie głównym.
2. Wybierz żądaną wersję VRM z listy, a następnie kliknij **Install**.
   Wyświetlane jest okno dialogowe **VRM installation** pokazujące pakiety oprogramowania, które zostaną zainstalowane.
3. Kliknij **Install**, aby kontynuować.
   Rozpocznie się instalacja pakietów oprogramowania. Cały ten proces może potrwać kilka minut. Nie wyłączaj systemu ani nie usuwaj nośnika pamięci.
   Uwaga: jeśli podczas instalacji wystąpi błąd, kliknij **Finish**. Spowoduje to ponowne uruchomienie systemu. Po ponownym uruchomieniu zaktualizuj odpowiednie pakiety oprogramowania i kontynuuj instalację.
4. Po zainstalowaniu wszystkich pakietów kliknij **Finish**.
   System zostanie uruchomiony ponownie. Po ponownym uruchomieniu zostanie wyświetlone okno logowania systemu Windows.

Uwaga!
Więcej informacji można znaleźć w dokumentacji VRM.

4.1.3 Używanie jako rozszerzenia pamięci masowej iSCSI

Aby używać systemu DIVAR IP jako rozszerzenia pamięci masowej iSCSI:

1. W oknie wyboru kliknij **iSCSI storage**.
   Składniki oprogramowania, które zostaną zainstalowane, są widoczne w oknie głównym.

2. Wybierz żądane komponenty z listy, a następnie kliknij **Install**.
   Wyświetlane jest okno dialogowe **iSCSI storage installation** pokazujące pakiety oprogramowania, które zostaną zainstalowane.
3. Kliknij **Install**, aby kontynuować.
   Rozpocznie się instalacja pakietów oprogramowania. Cały ten proces może potrwać kilka minut. Nie wyłączaj systemu ani nie usuwaj nośnika pamięci.
   Uwaga: jeśli podczas instalacji wystąpi błąd, kliknij **Finish**. Spowoduje to ponowne uruchomienie systemu. Po ponownym uruchomieniu zaktualizuj odpowiednie pakiety oprogramowania i kontynuuj instalację.
4. Po zainstalowaniu wszystkich pakietów kliknij **Finish**.
   System zostanie uruchomiony ponownie. Po ponownym uruchomieniu zostanie wyświetlone okno logowania systemu Windows.
5. Dodaj system jako rozszerzenie pamięci masowej iSCSI do zewnętrznego serwera BVMS lub VRM za pomocą aplikacji BVMS Configuration Client lub Configuration Manager.

Uwaga!
Więcej informacji można znaleźć w dokumentacji BVMS lub Configuration Manager.

5 Aktualizowanie i uaktualnianie oprogramowania

Za pomocą DIVAR IP Software Center można aktualizować i uaktualniać 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/

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.

Aktualizacja oprogramowania

Aby zaktualizować 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 **Updates** wyświetlane są dostępne aktualizacje. Kliknij **Update all**, aby zaktualizować wszystkie pakiety oprogramowania do nowej wersji.
   Wyświetlane jest okno dialogowe **Update**, pokazujące pakiety oprogramowania, które zostaną zaktualizowane.
   Uwaga: aktualizacja 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

W tej części opisano czynności niezbędne w celu uzyskania dostępu do systemu DIVAR IP z Internetu.

6.1 Ochrona systemu przed nieautoryzowanym dostępem

W celu zabezpieczenia systemu przed nieautoryzowanym dostępem zalecamy ustawienie silnych haseł, zanim system zostanie połączony 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 przez Internet za pośrednictwem routera z funkcjonalnością NAT/PAT, w systemie DIVAR IP 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.
  - Port 443 do obsługi dostępu przez protokół HTTPS do programu VRM za pomocą aplikacji Video Security Client lub Video Security App.

System DIVAR IP jest teraz dostępny z Internetu.

6.3 Wybór odpowiedniego klienta

W tym rozdziale opisano metody zdalnego łączenia się z systemem DIVAR IP za pośrednictwem Internetu.

Istnieją 2 sposoby nawiązywania zdalnego połączenia:

- *Połączenie zdalne za pomocą aplikacji Operator Client, Strona 13*.
- *Połączenie zdalne za pomocą aplikacji Video Security, Strona 14*.

Uwaga!
Należy używać wyłącznie aplikacji BVMS Operator Client lub Video Security App w wersji pasującej do systemu DIVAR IP. Inne aplikacje klienckie i programy mogą działać, ale nie są oficjalnie obsługiwane.

6.3.1 Połączenie zdalne za pomocą aplikacji Operator Client

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 skrótu  na pulpicie.
3. Wprowadź następujące informacje, a następnie kliknij przycisk **OK**.
   Nazwa użytkownika: admin (lub inny skonfigurowany użytkownik)
   Hasło: wprowadź hasło użytkownika
   Połączenie: ssh://[publiczny_adres_IP_rozwiązania_DIVAR-IP_all-in-one]:5322

6.3.2 Połączenie zdalne za pomocą aplikacji Video Security

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: wprowadź hasło użytkownika

6.4 Instalowanie serwera Enterprise Management Server

Aby zapewnić centralne zarządzanie wieloma systemami, można zainstalować na osobnym serwerze oprogramowanie BVMS Enterprise Management Server.

Aby zainstalować na osobnym serwerze oprogramowanie BVMS Enterprise Management Server, należy:

1. Pobrać instalator systemu BVMS ze strony produktu.
2. Skopiować instalator systemu BVMS na serwer, który będzie pełnić funkcję serwera Enterprise Management Server.
3. Kliknij dwukrotnie program instalacyjny, a następnie zaakceptować komunikat o zabezpieczeniach.
4. W oknie dialogowym **Welcome (Powitanie)** wyczyścić wszystkie pola wyboru z wyjątkiem pól **Enterprise Management Server** i **Configuration Client**.
5. Postępować zgodnie z instrukcjami instalacji.
6. Po pomyślnym zakończeniu instalacji uruchomić aplikację Configuration Client za pomocą skrótu na pulpicie.

Uwaga!
Informacje na temat konfiguracji serwera Enterprise Management Server można znaleźć w dokumentacji systemu BVMS.

7 Obsługa serwisowa

7.1 Monitorowanie systemu

System zawiera narzędzia do monitorowania stanu.
Aby uaktywnić funkcję monitorowania, trzeba się zalogować na koncie administratora (**BVRAdmin**).

1. Na ekranie systemu (w zależności od wybranego trybu pracy będzie to pulpit nawigacyjny BVMS lub ekran logowania systemu Windows) naciśnij klawisze Ctrl+Alt+Del.
2. Naciśnij i przytrzymaj lewy klawisz SHIFT bezpośrednio po kliknięciu przycisku **Przełącz użytkownika**.
3. Wybierz użytkownika **BVRAdmin**i zaloguj się, używając hasła wybranego podczas konfiguracji systemu.
4. Na komputerze w folderze **Tools** kliknij prawym przyciskiem myszy skrypt **Enable_SuperDoctor_5_Service**, a następnie kliknij polecenie **Uruchom jako administrator**.
5. W tym samym folderze kliknij dwukrotnie ikonę narzędzia **SuperDoctor 5 Web**.
6. Zaloguj się w internetowym interfejsie przy użyciu następujących domyślnych poświadczeń
   : Nazwa użytkownika: **admin**
   Hasło: **DivaripSD5**
7. Kliknij kartę **Configuration**, następnie kliknij **Password Settings** i zmień domyślne hasło.
8. Kliknij kartę **Configuration**, a następnie kliknij **Alert Configuration**.
9. Włącz funkcję **SNMP Trap** i wprowadź adres IP odbiornika komunikatów Trap protokołu SNMP.

7.2 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 nagranego 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 http://www.boschsecurity.com albo na stronie danego produktu w katalogu produktu. 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/. Bosch Security and Safety Systems oferuje pomoc techniczną w następujących obszarach:

- Aplikacje i narzędzia
- Modelowanie statystyk budynku
- Gwarancja
- Rozwiązywanie problemów
- Naprawy i wymiana
- Bezpieczeństwo produktów

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
Netherlands
www.boschsecurity.com

Building solutions for a better life.

202111292000