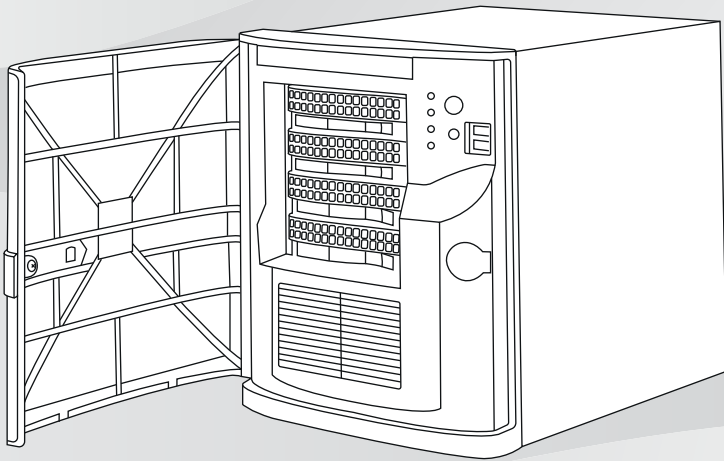




BOSCH

DIVAR IP all-in-one 5000

DIP-5240IG-00N | DIP-5244IG-4HD | DIP-5248IG-4HD |
DIP-524CIG-4HD | DIP-5240GP-00N | DIP-5244GP-4HD |
DIP-5248GP-4HD | DIP-524CGP-4HD



pl

Instrukcja instalacji

Spis treści

1	Zasady bezpieczeństwa	5
1.1	Ogólne zasady bezpieczeństwa	5
1.2	Zasady bezpieczeństwa dotyczące instalacji elektrycznych	8
1.3	Zasady bezpieczeństwa dotyczące wyładowań elektrostatycznych	9
1.4	Zasady bezpieczeństwa dotyczące eksploatacji	11
1.5	Zalecenia dotyczące bezpieczeństwa danych	11
2	Wstęp	12
2.1	Zawartość zestawu	12
2.2	Rejestracja produktu	13
3	Ogólne informacje o systemie	13
3.1	Widok urządzenia	14
3.2	Elementy na panelu sterowania	17
4	Montaż dysku twardego	19
4.1	Wymywanie kieszeni napędu z wnęki dyskowej	20
4.2	Instalowanie dysku twardego w kieszeni napędu	21
4.3	Instalowanie kieszeni napędu we wnęce dyskowej	23
5	Konfiguracja systemu	23
5.1	Ustawienia domyślne	23
5.2	Warunki wstępne	24
5.3	Tryby pracy	24
5.4	Przygotowanie dysków twardych do zapisu sygnału wizyjnego	25
5.5	Uruchamianie aplikacji	26
5.5.1	Używanie jako pełnego systemu zapisu sygnału wizyjnego i zarządzania	28
5.5.2	Używanie tylko do zapisu sygnału wizyjnego	28
5.5.3	Używanie jako rozszerzenia pamięci masowej iSCSI	28
5.6	Używanie aplikacji BVMS Config Wizard	29
5.7	Dodawanie kolejnych licencji	30
5.8	Używanie aplikacji BVMS Operator Client	31
6	Zdalne połączenie z systemem	32
6.1	Ochrona systemu przed nieautoryzowanym dostępem	33
6.2	Konfigurowanie przekierowania portów	33

6.3	Wybór odpowiedniego klienta	33
6.3.1	Połączenie zdalne za pomocą aplikacji Operator Client	34
6.3.2	Połączenie zdalne za pomocą aplikacji Video Security	34
7	Obsługa serwisowa	35
7.1	Monitorowanie systemu	35
7.2	Przywracanie ustawień fabrycznych	36
7.3	Serwisowanie i naprawa	37
8	Informacje dodatkowe	38
8.1	Dodatkowa dokumentacja i oprogramowanie	38
8.2	Usługi pomocy technicznej i Bosch Academy	38

1 Zasady bezpieczeństwa

Należy przestrzegać zasad bezpieczeństwa wyszczególnionych w tym rozdziale.

1.1 Ogólne zasady bezpieczeństwa

Zapewnienie ogólnego bezpieczeństwa wymaga przestrzegania następujących zasad:

- System powinien się znajdować w otoczeniu czystym i przestronnym.
- Górną pokrywę obudowy i inne podzespoły systemu po wymontowaniu należy umieścić z dala od jednostki lub na stole, tak aby nie można było przez przypadek na nie nadepnąć.
- W trakcie pracy przy systemie nie należy mieć na sobie luźnych elementów ubioru, takich jak krawaty czy niezapięte rękawy koszuli. Mogą się one stykać z obwodami elektrycznymi lub zostać wciągnięte w wentylator chłodzący.
- Należy zdjąć z siebie biżuterię i przedmioty metalowe, które stanowią dobre przewodniki prądu elektrycznego. Mogą one spowodować zwarcie w razie zetknięcia się z płytkami drukowanymi lub elementami przewodzącymi prąd elektryczny.

Ostrzeżenie!

Zanik zasilania sieciowego:



Napięcie jest przykładane do jednostki natychmiast po umieszczeniu wtyczki w gnieździe sieci zasilającej.

Jednakże urządzenia wyposażone w wyłącznik zasilania są gotowe do pracy dopiero po jego ustawieniu w pozycji WŁ. Po wyjęciu wtyczki kabla zasilającego z gniazda zasilanie urządzenia zanika całkowicie.

Ostrzeżenie!

Usuwanie obudowy:

Aby uniknąć porażenia prądem, obudowę musi zdejmować wykwalifikowany personel serwisowy.



Przed wymontowaniem obudowy wtyczkę kabla zasilającego należy wyjąć i nie należy jej podłączać do momentu ponownego założenia obudowy. Czynności serwisowe może wykonywać jedynie wykwalifikowany personel serwisowy. Użytkownikowi nie wolno przeprowadzać napraw samodzielnie.

Ostrzeżenie!

Kabel zasilający i zasilacz prądu zmiennego:

Instalując ten system, należy używać kabli i zasilaczy dostarczonych przez producenta lub odpowiednich do tego celu. Stosowanie niewłaściwych kabli i zasilaczy może spowodować awarię lub pożar. Przepisy dotyczące bezpieczeństwa materiałów i urządzeń elektrycznych zabraniają używania kabli z certyfikatami UL oraz CSA (zawierających skróty UL/CSA w kodzie) w połączeniu z innymi urządzeniami elektrycznymi.

**Ostrzeżenie!**

Akumulator litowy:

Niewłaściwie zamontowane akumulatory mogą spowodować eksplozję. Zużyte akumulatory należy zawsze wymieniać na akumulatory tego samego typu lub podobnego typu zalecane przez producenta.



Ze zużytymi akumulatorami należy się obchodzić ostrożnie.

Akumulatorów nie wolno w żaden sposób niszczyć.

Z uszkodzonych akumulatorów mogą wyciekać do środowiska niebezpieczne substancje.

Puste akumulatory należy usuwać zgodnie z zaleceniami producenta lub lokalnymi przepisami.

**Ostrzeżenie!**

Dotykanie materiałów lutowanych związkami z ołowiem, które znajdują się w tym produkcie, naraża użytkownika na działanie ołowiu — substancji uznanej w stanie Kalifornia za uszkadzającą płody oraz szkodliwie wpływającą na układ rozrodczy.

**Uwaga!**

Urządzenie podatne na wyładowania elektrostatyczne:

W celu uniknięcia wyładowań elektrostatycznych należy poprawnie zastosować wszystkie zabezpieczenia obwodów układów scalonych typu CMOS/MOSFET.

Na czas manipulowania płytkami drukowanymi wewnątrz urządzenia należy mieć założone na nadgarstkach opaski uziemiające i przestrzegać zasad bezpieczeństwa dotyczących wyładowań elektrostatycznych.

**Uwaga!**

Instalację powinien przeprowadzać wyłącznie wykwalifikowany personel zgodnie z obowiązującymi przepisami w sprawie urządzeń elektrycznych.

**Uwaga!**

System operacyjny zawiera najnowsze poprawki bezpieczeństwa systemu Windows, które były dostępne w momencie tworzenia obrazu oprogramowania. Zalecamy regularne instalowanie najnowszych poprawek bezpieczeństwa przy użyciu funkcji Windows Update.

**Utylizacja**

Niniejszy produkt marki Bosch został skonstruowany i wyprodukowany z najwyższej jakości materiałów i podzespołów, które mogą zostać ponownie użyte.

Ten symbol oznacza, że wyrzucanie urządzeń elektrycznych i elektronicznych wycofanych z eksploatacji wraz z odpadami pochodzącymi z gospodarstw domowych jest zabronione.

W Unii Europejskiej funkcjonują systemy selektywnej zbiórki zużytych produktów elektrycznych i elektronicznych. Urządzenia takie powinny być utylizowane w lokalnych punktach zbiórki odpadów lub w odpowiednich centrach recyklingu.

1.2 Zasady bezpieczeństwa dotyczące instalacji elektrycznych

Aby uchronić użytkowników przed obrażeniami, a system przed uszkodzeniem, należy przestrzegać podstawowych zasad bezpieczeństwa pracy przy instalacjach elektrycznych.

- Należy zapamiętać, gdzie znajdują się wyłącznik zasilania na obudowie oraz główny wyłącznik awaryjny, odłącznik lub gniazdo elektryczne w pomieszczeniu. Dzięki tym elementom w razie awarii lub wypadku związanego z instalacją elektryczną można szybko odłączyć zasilanie elektryczne od systemu.
- W pracach przy podzespołach pod wysokim napięciem musi uczestniczyć druga osoba.
- Przed przystąpieniem do instalacji lub demontażu podzespołów z komputera, w tym płytki montażowej, odłączyć przewody zasilania.
- Aby odłączyć zasilanie, należy w pierwszej kolejności wyłączyć system, a następnie odłączyć kable zasilające od wszystkich zasilaczy systemu.
- Przy pracy w pobliżu nieosłoniętych obwodów elektrycznych powinna asystować druga osoba zaznajomiona z działaniem wyłączników zasilania, która w razie konieczności będzie mogła odłączyć zasilanie.
- Wszelkie czynności na urządzeniach elektrycznych podłączonych do zasilania należy wykonywać jedną ręką. Pozwala to zapobiec zamknięciu obwodu elektrycznego i porażeniu prądem elektrycznym. Szczególną ostrożność należy zachować w przypadku używania metalowych narzędzi, które mogą łatwo uszkodzić podzespoły elektryczne lub płytki drukowane w razie zetknięcia z nimi.

- Kable zasilające muszą być wyposażone we wtyczki z uziemieniem i należy je podłączać wyłącznie do uziemionych gniazd elektrycznych. W jednostce znajduje się więcej niż jeden kabel zasilający. Przed rozpoczęciem prac serwisowych należy odłączyć oba kable zasilające, aby uniknąć porażenia prądem elektrycznym.
- Wymienne bezpieczniki przylutowane do płyty głównej: samoczynnie resetujące się bezpieczniki PTC (o dodatnim współczynniku temperaturowym) na płycie głównej mogą być wymieniane wyłącznie przez odpowiednio przeszkolonych techników serwisowych. Nowy bezpiecznik musi być taki sam, jak wymieniany, lub stanowić jego odpowiednik. Dodatkowe informacje na ten temat można uzyskać, kontaktując się z działem pomocy technicznej, który pomaga także dobrać właściwe elementy.



Przestroga!

Akumulator płyty głównej: zainstalowanie akumulatora na płycie do góry dnem, skutkujące zamianą biegunów, może doprowadzić do eksplozji. Akumulator ten należy wymieniać wyłącznie na elementy dokładnie tego samego typu lub na ich odpowiedniki polecane przez producenta (CR2032). Zużyte akumulatory należy utylizować zgodnie z zaleceniami producenta.

1.3 Zasady bezpieczeństwa dotyczące wyładowań elektrostatycznych

Wyładowanie elektrostatyczne (ESD) zachodzi między dwoma przedmiotami o różnych ładunkach elektrycznych w momencie ich zetknięcia. Wyładowanie elektrostatyczne powstaje w celu zniwelowania tej różnicy, grożąc uszkodzeniem podzespołów elektronicznych i płytek drukowanych. Aby chronić urządzenia przed ESD, zasadniczo wystarczy stosować następujące środki zaradcze, które polegają na niwelowaniu różnicy między ładunkami elektrycznymi przed, zanim przedmioty się zetkną.

- Mat chroniących przed wyładowaniami elektrostatycznymi nie wolno używać do ochrony przed porażeniem prądem elektrycznym. Do tego celu zaleca się stosowanie mat gumowych, zaprojektowanych specjalnie jako izolatory prądu elektrycznego.
- Należy używać uziemiających opasek na nadgarstki, które zabezpieczają przed wyładowaniami elektrostatycznymi.
- Wszystkie podzespoły i płytki drukowane należy przechowywać w odpowiednich torbach antystatycznych, dopóki nie będą potrzebne.
- Przed wyjęciem podzespołu/płytki z torby antystatycznej należy dotknąć uziemionego metalowego przedmiotu.
- Należy dopilnować, aby podzespoły ani płytki drukowane nie zetknęły się z ubraniem, na którym nawet pomimo zastosowania opaski uziemiającej może pozostawać ładunek elektryczny.
- Płytkę należy przynosić, trzymając ją za krawędzie. Nie wolno dotykać podzespołów, układów scalonych, modułów pamięci ani styków zamontowanych na płytce.
- W przypadku przenoszenia układów scalonych lub modułów należy się starać nie dotykać ich zestyków.
- Na czas, kiedy nie będą używane, płytę główną i/lub urządzenia peryferyjne należy umieścić z powrotem w torbach antystatycznych.
- Aby zapewnić prawidłowe uziemienie rejestratora, należy dopilnować, by obudowa komputera doskonale przewodziła prąd elektryczny pomiędzy zasilaczem, pokrywą, elementami mocującymi i płytą główną.

1.4 Zasady bezpieczeństwa dotyczące eksploatacji



Uwaga!

Aby zapewnić prawidłowe chłodzenie, na czas pracy systemu musi być założona pokrywa obudowy.

Nieprzestrzeżenie tej zasady grozi uszkodzeniem systemu, które nie jest objęte gwarancją.



Uwaga!

Ze zużyтыми akumulatorami należy się obchodzić ostrożnie.

Akumulatorów nie wolno w żaden sposób niszczyć.

Z uszkodzonych akumulatorów mogą wyciekać do środowiska niebezpieczne substancje. Zużytych akumulatorów nie wolno wrzucać do śmieci ani wywozić na publiczne składowiska.

Zużyte akumulatory należy oddawać do wyspecjalizowanego punktu zbiórki odpadów niebezpiecznych.



Ostrzeżenie!

Podczas serwisowania i pracy przy płycie montażowej należy zachować ostrożność. Uwaga: podczas pracy systemu do płytki montażowej doprowadzone jest napięcie. Należy upewnić się, że płytki montażowej nie dotykają żadne metalowe przedmioty ani kable taśmowe.

1.5 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.

Patrz

- *Zdalne połączenie z systemem, Strona 32*

2 Wstęp

Przed rozpoczęciem instalacji należy zapoznać się z instrukcjami dotyczącymi bezpieczeństwa.

2.1 Zawartość zestawu

Należy upewnić się, że wszystkie części są dołączone i nie są uszkodzone. Jeśli opakowanie lub jakiegokolwiek części są uszkodzone, należy skontaktować się z spedytorem. W przypadku braku jakichkolwiek części należy powiadomić pracownika działu handlowego lub działu obsługi klienta firmy Bosch Security Systems.

Liczba	Komponent
1	DIVAR IP all-in-one 5000
1	Instrukcja instalacji
1	Kabel zasilający EU

Liczba	Komponent
1	Kabel zasilający US
2	Klucze

2.2 Rejestracja produktu

Zarejestruj swój produkt:

<https://www.boschsecurity.com/product-registration/>



3 Ogólne informacje o systemie

System DIVAR IP all-in-one 5000 jest uniwersalnym rozwiązaniem do zapisu, oglądania i zarządzania obrazem wideo stosowane w sieciowych systemach dozoru wizyjnego.

To inteligentne, sieciowe urządzenie z możliwością przechowywania danych, eliminujące konieczność stosowania osobnego serwera sieciowego rejestratora wizyjnego (NVR) i urządzeń do przechowywania danych. System działa w oparciu o kompleksowe rozwiązanie BVMS (BVMS) i oprogramowanie Bosch Video Recording Manager (VRM) oraz umożliwia integrację kamer innych producentów poprzez zastosowanie systemu Bosch Video Streaming Gateway (VSG).

System BVMS zarządza wszystkimi urządzeniami sieciowymi oraz danymi cyfrowych urządzeń wideo i audio, a także danymi dotyczącymi bezpieczeństwa przesyłanymi w sieci. Zapewnia bezproblemowe łączenie kamer sieciowych i nadajników oraz

umożliwia zarządzanie zdarzeniami oraz alarmami, monitorowanie stanu systemu, a także administrowanie użytkownikami i priorytetami.

System DIVAR IP all-in-one 5000 to jednostka typu „mini tower” z 4 wnękami, wyposażona w wymienne od przodu dyski twarde SATA.

Łatwo go instalować i obsługiwać. Całość oprogramowania systemowego jest fabrycznie zainstalowana. W ten sposób klient otrzymuje urządzenie gotowe do pracy bezpośrednio po wyjęciu z opakowania.

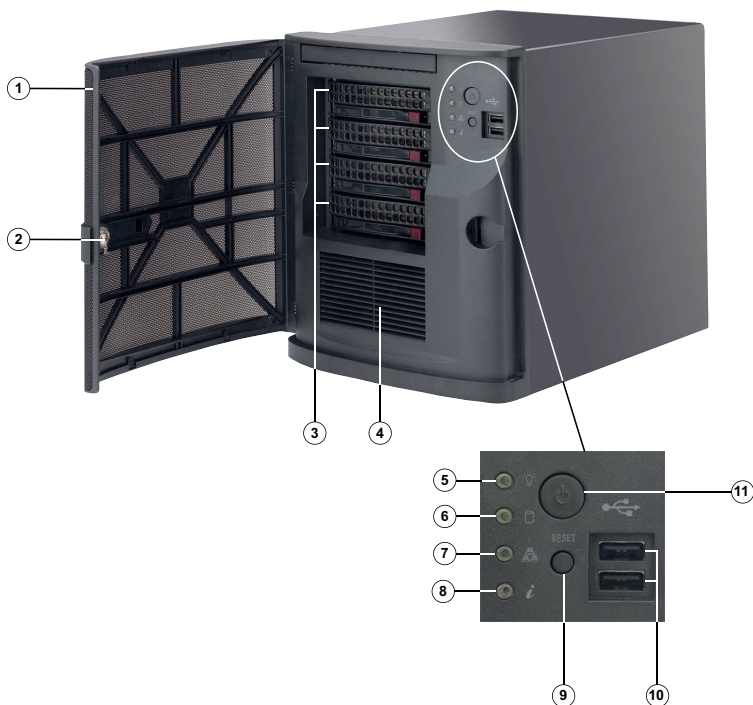
Urządzenie DIVAR IP all-in-one 5000 działa w oparciu o system operacyjny Windows Storage Server 2016.

3.1 Widok urządzenia

System DIVAR IP all-in-one 5000 jest zabudowany w kompaktowej obudowie typu mini tower. Ma uchylaną pokrywę przednią, za którą znajdują się dyski twarde i panel sterowania. Panel sterowania z przodu zawiera przyciski zasilania i diody LED monitorowania stanu.

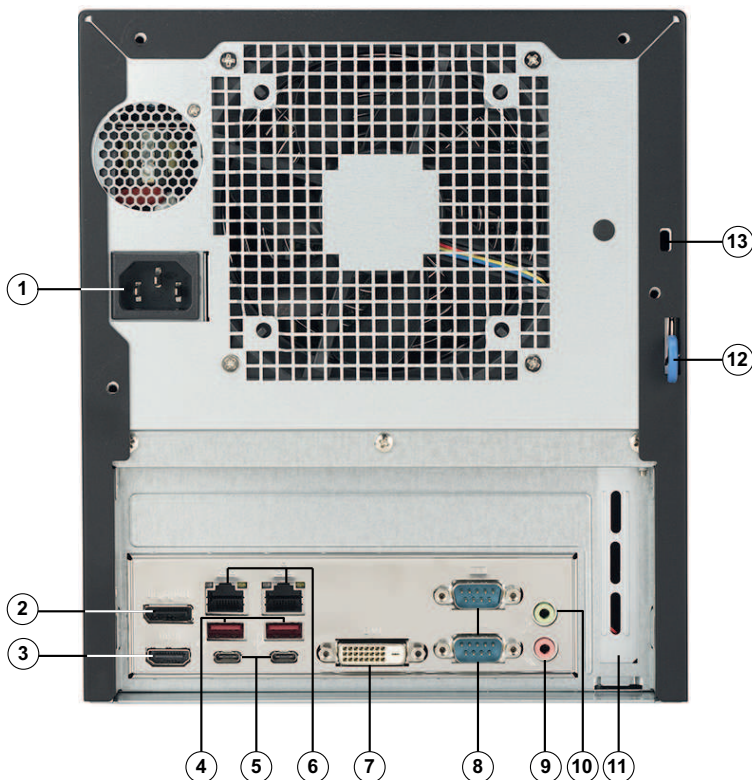
Z tyłu umieszczono różne porty we/wy.

Widok z przodu



1	Pokrywa przednia	2	Blokada pokrywy przedniej
3	4 gniazda na dyski twarde (3,5 cala)	4	Filtr wlotowy powietrza
5	Dioda LED zasilania	6	Dioda LED dysku twardego (nieużywana)
7	Dioda LED sieci	8	Dioda LED informacji
9	Przycisk Reset	10	2 porty USB 2.0
11	Włącznik/wyłącznik zasilania		

Widok z tyłu




1	Gniazdo sieci elektrycznej	2	Port DisplayPort
3	Port HDMI 2.0	4	2 porty USB 3.1 (typ A)
5	2 porty USB 3.1 (typ C)	6	2 porty LAN (RJ45), zgrupowane Uwaga: Nie zmieniaj ustawienia trybu grupowego!
7	Port DVI-D	8	2 porty COM
9	Wejście foniczne mikrofonu	10	Wyjście liniowe audio


11	<p>Dodatkowa karta GPU z 4 portami Mini DisplayPort (w tym przypadku do portu Mini DisplayPort należy podłączyć monitor).</p> <p>Uwaga: Dostępne tylko w modelach DIP-5240GP-00N, DIP-5244GP-4HD, DIP-5248GP-4HD i DIP-524CGP-4HD.</p>	12	<p>Skobel z tyłu obudowy (pasują do niego różne popularne kłódki).</p> <p>Uwaga: Kłódki nie wchodzi w skład zestawu.</p>
13	<p>Otwór zabezpieczenia Kensington (na standardową blokadę Kensington).</p> <p>Uwaga: Blokada Kensington nie wchodzi w skład zestawu.</p>		

3.2 Elementy na panelu sterowania





Panel sterowania z przodu obudowy zawiera przyciski zasilania i diody LED monitorowania stanu.

Przyciski panelu sterowania

Przycisk	Opis
 <p>Zasilanie e</p>	<p>Przycisk zasilania umożliwia doprowadzenie i odcięcie zasilania elektrycznego od systemu.</p> <p>Uwaga: Wyłączenie systemu za pomocą tego przycisku odcina główne zasilanie, ale utrzymuje zasilanie trybu gotowości systemu.</p>

Przycisk	Opis
	Aby odciąć całe zasilanie, na przykład w celu wykonania prac konserwacyjnych, przed ich rozpoczęciem należy odłączyć system od sieci elektrycznej.
 Reset	Przycisk resetowania umożliwia ponowne uruchomienie systemu.

Diody LED panelu sterowania

LED	Opis	
 Zasilanie	Ta dioda LED sygnalizuje, że zasilanie elektryczne jest doprowadzane do zasilacza systemu. Ta dioda LED normalnie powinna świecić podczas pracy systemu.	
 Dysk twardy	Ta dioda LED nie jest używana.	
 Sieć	Miganie tej diody LED sygnalizuje aktywność sieci.	
 Informacje	Ta dioda LED informuje o stanie systemu.	
	Stan systemu Świeci jednostajnie na czerwono	Opis Nastąpiło przegrzanie (może to być spowodowane zbyt gęstym upakowaniem kabli).

LED	Opis	
	Miga na czerwono (z częstotliwością 1 kHz)	Awaria wentylatora: sprawdź, czy wentylator działa.
	Miga na czerwono (z częstotliwością 0,25 kHz)	Awaria zasilania: sprawdź, czy zasilacz działa.
	Świeci jednostajnie na niebiesko	Uaktywniono identyfikator UID lokalnego urządzenia. Ta funkcja służy do odnajdowania urządzenia w szafie typu rack.
	Miga na niebiesko (300 ms)	Uaktywniono identyfikator UID zdalnego urządzenia. Ta funkcja służy do odnajdowania urządzenia ze zdalnej lokalizacji.

4 Montaż dysku twardego

System DIVAR IP all-in-one 5000 jest wyposażony w wymienne od przodu cztery dyski twarde. Dyski montuje się w komorze napędów wyposażonej w kieszenie, aby uprościć dodawanie i usuwanie dysków twardych z obudowy. Kieszenie te wspomagają również prawidłowy przepływ powietrza przez wnęki dyskowe.

Procedura

W celu zainstalowania dysku twardego należy wykonać następujące czynności:

1. *Wymywanie kieszeni napędu z wnęki dyskowej, Strona 20*
2. *Instalowanie dysku twardego w kieszeni napędu, Strona 21*
3. *Instalowanie kieszeni napędu we wnęce dyskowej, Strona 23*

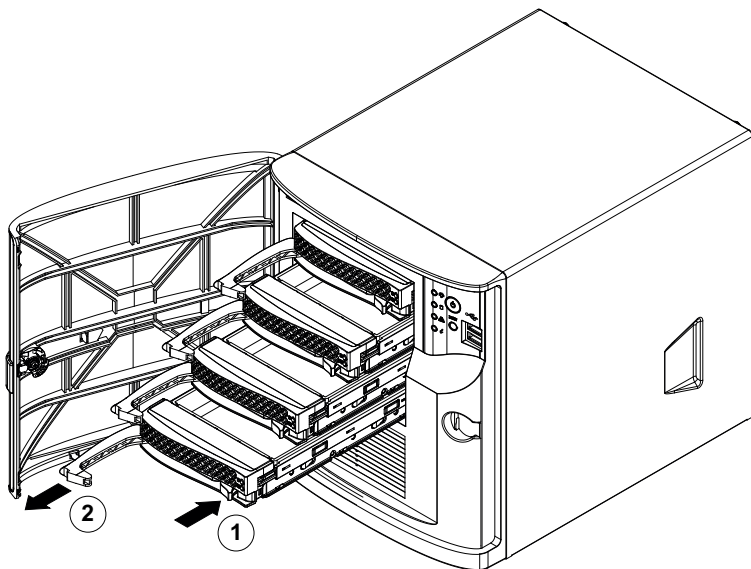
**Uwaga!**

Przed rozpoczęciem wykonywania czynności na elementach obudowy należy się zapoznać z ostrzeżeniami i zasadami bezpieczeństwa podanymi w niniejszej instrukcji.

4.1 Wyjmowanie kieszeni napędu z wnęki dyskowej

Aby wyjąć kieszeń napędu z wnęki dyskowej:

1. Odblokuj pokrywę przednią i obróć ją do pozycji otwarcia.
2. Naciśnij przycisk zwalniający na prawo od kieszeni napędu. Dzięki temu wysunie się uchwyt kieszeni napędu.
3. Za pomocą uchwytu wyciągnij kieszeń napędu z obudowy.



1 Przycisk zwalniający

2 Uchwyt kieszeni napędu

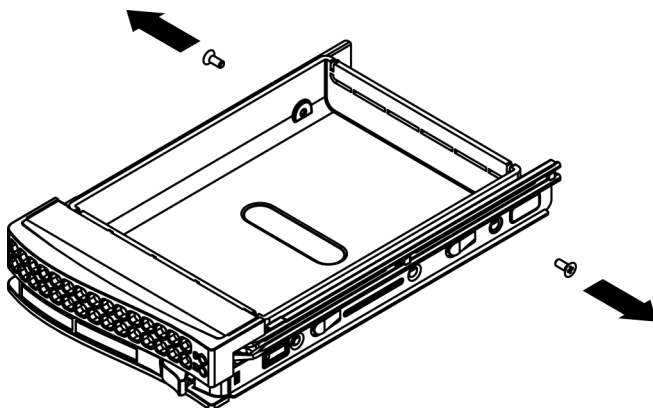
**Uwaga!**

Nie uruchamiaj urządzenia, gdy z wnęki dyskowych wyjęto kieszenie napędów.

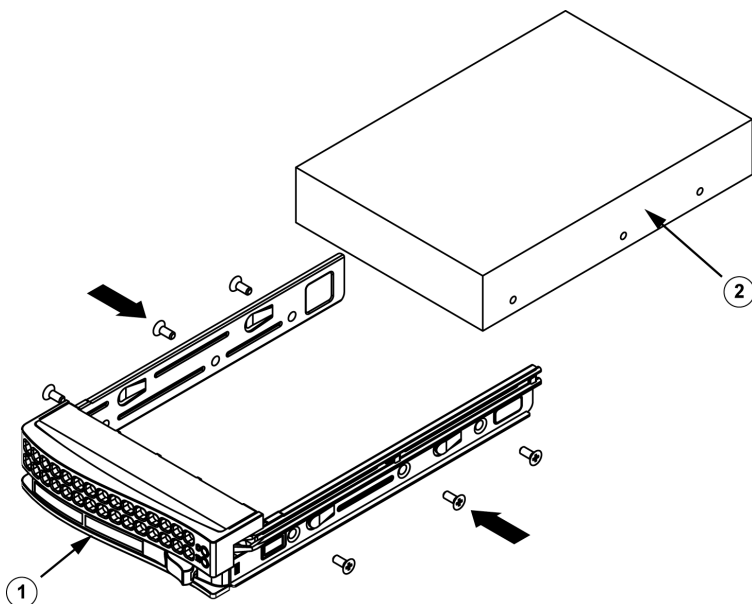
4.2 Instalowanie dysku twardego w kieszeni napędu

Aby zainstalować dysk twardy w kieszeni napędu:

1. Wykręć wkręty mocujące atrapę dysku do kieszeni napędu.



2. Wyjmij atrapę dysku z kieszeni napędu, a następnie połóż kieszeń napędu na płaskiej powierzchni.
3. Wsuń nowy dysk twardy do kieszeni napędu, płytka drukowaną do dołu.
4. Wyrównaj otwory montażowe dysku twardego z otworami kieszeni napędu.
5. Za pomocą sześciu wkrętów przymocuj dysk twardy do kieszeni napędu.



1	Kieszeń napędu	2	Dysk twardy SATA
---	----------------	---	------------------

Uwaga!

Zalecamy stosowanie odpowiednich dysków twardego od firmy Bosch. Dyski twarde należą do najistotniejszych składników sprzętowych i dlatego firma Bosch dobiera je starannie na podstawie dostępnych wskaźników awaryjności. Dyski twarde od dostawców innych niż Bosch nie są obsługiwane.

Więcej informacji o obsługiwanych dyskach twardego zamieszczono w arkuszu danych w internetowym katalogu produktów firmy Bosch:

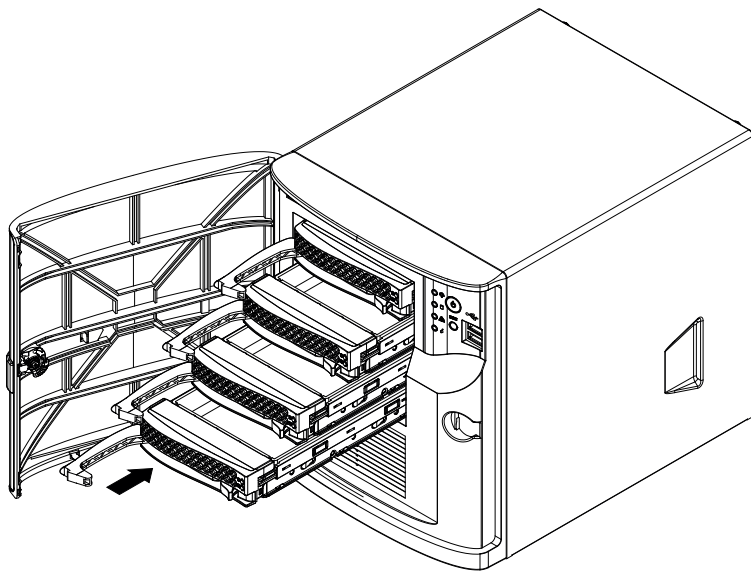
www.boschsecurity.com



4.3 Instalowanie kieszeni napędu we wnęce dyskowej

Aby zainstalować kieszeń napędu we wnęce dyskowej:

1. Włóż kieszeń napędu poziomo do wnęki dyskowej, ustawiając ją w taki sposób, aby przycisk zwalniający znalazł się po prawej stronie.
2. Wsuwaj kieszeń napędu do wnęki do chwili, aż uchwyt się cofnie, a kieszeń z wyraźnym kliknięciem zatrzaśnie się w docelowym położeniu.
3. Zamknij i zablokuj pokrywę przednią.



5 Konfiguracja systemu

5.1 Ustawienia domyślne

Systemy DIVAR IP są dostarczane z fabrycznie zainstalowanym kreatorem konfiguracji.

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

- Użytkownik: BVRAdmin
- Hasło: WSS4Bosch

5.2 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.
- Określić, czy pierwsza instalacja przebiega w sieci DHCP. Jeśli tak nie jest, należy przypisać prawidłowe adresy IP do urządzeń wideo. Aby uzyskać poprawny zakres adresów IP, które mogą być używane z DIVAR IP i przypisanymi urządzeniami, skontaktuj się z administratorem.
- Domyślne ustawienia iSCSI są zoptymalizowane pod kątem używania z oprogramowaniem VRM.

5.3 Tryby pracy

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).

5.4 Przygotowanie dysków twardych do zapisu sygnału wizyjnego

Systemy fabrycznie wyposażone w dyski twarde są od razu przygotowane do operacji zapisu.

Natomiast dyski twarde dodane do pustego systemu należy odpowiednio przygotować (sformatować), zanim będzie można na nich zapisywać sygnał wizyjny.

Dostępne są następujące opcje formatowania dysków twardych:

- Przeprowadzanie początkowej konfiguracji fabrycznej: patrz *Przywracanie ustawień fabrycznych, Strona 36*.
- Wykonanie skryptu formatowania.

Wykonywanie skryptu formatowania

Aby wykonać skrypt formatowania, trzeba się zalogować na koncie administratora (BVRAdmin).

1. Uruchom system.
2. Gdy pojawi się domyślny ekran systemu BVMS, naciśnij kombinację klawiszy CTRL+ALT+DELETE.
3. Wciśnij klawisz SHIFT, kliknij przycisk **Przełącz użytkownika** i trzymaj wciśnięty klawisz SHIFT jeszcze przez około pięć sekund.
4. Wprowadź nazwę użytkownika i hasło administratora.

5. Na komputerze w folderze **Narzędzia** kliknij prawym przyciskiem myszy skrypt **Format_data_hard_drives**, a następnie kliknij polecenie **Uruchom jako administrator**.
6. Postępuj zgodnie z instrukcjami.
7. Po sformatowaniu dysku możesz go dodać do konfiguracji zarządzania sygnałem wizyjnym.

**Uwaga!**

Sformatowanie dysku twardego powoduje usunięcie z niego wszystkich istniejących danych.

5.5 Uruchamianie aplikacji

Aplikacja jest intuicyjna, prosta w instalacji i pozwala łatwo zarządzać sieciowym systemem dozorowym.

Aby uruchomić aplikację:

1. Podłączyć jednostkę i kamery do sieci.
2. Włączyć jednostkę.
Zostanie uruchomiony proces konfiguracji Windows Storage Server 2016.
3. Wybrać odpowiedni język instalacji i kliknąć przycisk **Dalej**.
4. Wybrać odpowiednie pozycje z list **Kraj lub region**, **Godzina i waluta** oraz **Układ klawiatury**, kliknąć wybrany element, a następnie kliknąć przycisk **Dalej**.
Zostaną wyświetlone dokumenty Microsoft Software License Terms i EULA (Umowa licencyjna dla użytkownika końcowego).
5. Zaakceptować warunki umowy licencyjnej, a następnie kliknąć przycisk **Uruchom**. System Windows zostanie uruchomiony ponownie.
6. Po ponownym uruchomieniu systemu nacisnąć kombinację klawiszy CTR+ALT+DELETE. Zostanie wyświetlone okno logowania systemu Windows.
7. Wprowadzić domyślne hasło **WSS4Bosch**.

8. Po wprowadzeniu hasła zostanie wyświetlony komunikat o konieczności zmiany hasła przed pierwszym logowaniem. Aby zatwierdzić, kliknąć przycisk **OK**.
9. Zmienić hasło.
Zestaw skryptów zacznie wykonywać ważne zadania konfiguracyjne. Cały ten proces może potrwać kilka minut. Nie wyłączaj komputera.
Zostanie wyświetlony domyślny ekran oprogramowania BVMS.
Teraz możesz zdecydować, w jakim trybie chcesz używać systemu:
 - *Używanie jako pełnego systemu zapisu sygnału wizyjnego i zarządzania, Strona 28*
 - *Używanie tylko do zapisu sygnału wizyjnego, Strona 28*
 - *Używanie jako rozszerzenia pamięci masowej iSCSI, Strona 28*

**Uwaga!**

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

**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.

5.5.1 Używanie jako pełnego systemu zapisu sygnału wizyjnego i zarządzania

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

1. Na domyślnym ekranie systemu BVMS kliknij dwukrotnie aplikacji BVMS Config Wizard , a aplikacja zostanie uruchomiona. Pojawi się strona **Welcome**.
2. Skonfiguruj system za pomocą aplikacji Config Wizard.

Patrz

– *Używanie aplikacji BVMS Config Wizard, Strona 29*

5.5.2 Używanie tylko do zapisu sygnału wizyjnego

Aby używać systemu DIVAR IP tylko do zapisu sygnału wizyjnego, należy się zalogować na koncie administratora (BVRAdmin) w celu wykonania niezbędnych czynności konfiguracyjnych.

1. Gdy pojawi się domyślny ekran systemu BVMS, naciśnij kombinację klawiszy CTRL+ALT+DELETE.
2. Wciśnij klawisz SHIFT, kliknij przycisk **Przełącz użytkownika** i trzymaj wciśnięty klawisz SHIFT jeszcze przez około pięć sekund.
3. Wprowadź nazwę użytkownika i hasło administratora.
4. Na komputerze w folderze **Narzędzia** kliknij prawym przyciskiem myszy skrypt **Disable_BVMS**, a następnie kliknij polecenie **Uruchom jako administrator**.
5. Skonfiguruj oprogramowanie Video Recording Manager (VRM) z zewnętrznego urządzenia za pomocą aplikacji BVMS Configuration Client lub Configuration Manager.

5.5.3 Używanie jako rozszerzenia pamięci masowej iSCSI

Aby używać systemu DIVAR IP jako rozszerzenia pamięci masowej iSCSI, należy się zalogować na koncie administratora (BVRAdmin) w celu wykonania niezbędnych czynności konfiguracyjnych.

1. Gdy pojawi się domyślny ekran systemu BVMS, naciśnij kombinację klawiszy CTRL+ALT+DELETE.
2. Wciśnij klawisz SHIFT, kliknij przycisk **Przełącz użytkownika** i trzymaj wciśnięty klawisz SHIFT jeszcze przez około pięć sekund.
3. Wprowadź nazwę użytkownika i hasło administratora.
4. Na komputerze w folderze **Narzędzia** kliknij prawym przyciskiem myszy skrypt **Disable_BVMS_and_VRM**, a następnie kliknij polecenie **Uruchom jako administrator**.
5. Dodaj system jako rozszerzenie pamięci masowej iSCSI do zewnętrznego serwera BVMS lub VRM za pomocą aplikacji BVMS Configuration Client lub Configuration Manager.

5.6 Używanie aplikacji BVMS Config Wizard

Program Config Wizard pozwala szybko i łatwo skonfigurować mniejszy system. Pomaga uzyskać skonfigurowany system, w tym system VRM, iSCSI, kamery, profile zapisu i grupy użytkowników.

Konfiguracja grup użytkowników i ich uprawnień przebiega automatycznie. Można dodawać i usuwać użytkowników oraz ustawiać hasła.

Config Wizard ma dostęp do serwera Management Server tylko na komputerze lokalnym.

Uaktywnioną konfigurację można zapisać jako kopię zapasową i zaimportować ją w późniejszym czasie. Po zaimportowaniu konfiguracja może zostać zmodyfikowana.

Config Wizard automatycznie dodaje lokalny system VRM.

Ograniczenia:

W aplikacji Config Wizard nie są obsługiwane zadania wymienione poniżej. Do ich wykonania należy użyć aplikacji BVMS Configuration Client.

- dostosowywanie harmonogramów
- konfigurowanie systemów bez aplikacji Video Recording Manager lub z jej wieloma wystąpieniami
- konfigurowanie zewnętrznych urządzeń pamięci masowej

- dodawanie aplikacji Video Streaming Gateway
- konfigurowanie ustawień zaawansowanych (np. map i alarmów)

Aby szybko skonfigurować system za pomocą aplikacji Config Wizard:

1. Na ekranie domyślnym programu BVMS kliknij dwukrotnie ikonę aplikacji Config Wizard. Zostanie wyświetlona strona **Welcome**.
2. Wykonaj kolejne kroki w kreatorze i przestrzegaj instrukcji wyświetlanych na ekranie.

Uwaga!



W kwestii zadań, których nie można wykonać za pomocą aplikacji Config Wizard, oraz aby uzyskać szczegółowe informacje o samej aplikacji Config Wizard, patrz instrukcja oprogramowania BVMS dostępna w internetowym katalogu produktów.

Patrz

- *Dodatkowa dokumentacja i oprogramowanie, Strona 38*

5.7 Dodawanie kolejnych licencji

Za pomocą aplikacji Configuration Client można dodać więcej licencji.

Aby uaktywnić oprogramowanie:


1. Uruchom program Configuration Client.
2. W menu **Narzędzia** kliknąć **Manager licencji**. Zostanie wyświetlone okno dialogowe **Manager licencji**.
3. Zaznacz pola wyboru odpowiadające pakietowi oprogramowania, modułom i rozszerzeniom, które mają zostać aktywowane. W przypadku rozszerzeń wymagane jest określenie liczby licencji.
Jeśli dostępny jest plik z informacjami o pakiecie oprogramowania, należy go zaimportować, klikając opcję **Importuj informacje o pakiecie**.

4. Kliknąć **Uaktywnij**.
Zostanie wyświetlone okno dialogowe **Licencja Uaktywnienie**.
5. Wpisz sygnaturę komputera lub skopiuj ją i wklej do pliku tekstowego.
6. W przypadku komputera z dostępem do Internetu wpisać do przeglądarki następujący adres:
`https://activation.boschsecurity.com`
W przypadku braku konta umożliwiającego dostęp do centrum licencji Bosch License Activation Center, należy utworzyć takie konto (zalecane) lub kliknąć łącznie umożliwiające uaktywnienie licencji bez konieczności logowania. Jeśli utworzysz konto i zalogujesz się przed uaktywnieniem, program License Manager będzie rejestrować wykonywane przez Ciebie czynności. Ich przegląd jest możliwy w dowolnej chwili.
Należy postępować dalej zgodnie z instrukcjami w celu otrzymania klucza uaktywnienia licencji.
7. Powróć do oprogramowania BVMS. W oknie dialogowym **Licencja Uaktywnienie** wpisać Klucz uaktywnienia licencji uzyskany z Managera licencji i kliknąć **Uaktywnij**.
Pakiet oprogramowania zostanie aktywowany.

5.8 Używanie aplikacji BVMS Operator Client

Korzystając z aplikacji BVMS Operator Client, można sprawdzać działanie funkcji podglądu na żywo, zapisu i odtwarzania w systemie DIVAR IP.

Aby za pomocą aplikacji Operator Client sprawdzić działanie funkcji obrazu na żywo

1. Na ekranie domyślnym programu BVMS kliknij dwukrotnie ikonę aplikacji Operator Client . Aplikacja zostanie uruchomiona.

2. Wprowadź podane informacje i kliknij przycisk **OK**.
Nazwa użytkownika: admin
Hasło: nie jest wymagane (chyba że je ustawiono w kreatorze)
Połączenie: 127.0.0.1
3. Kliknij ikonę obrazu na żywo. Zostanie wyświetlone drzewo logiczne z kamerami.
4. Zaznacz kamerę i przeciągnij ją do okna obrazu. Jeżeli kamera jest prawidłowo przypisana, zostanie wyświetlona jej ilustracja.
Uwaga:
Czerwona kropka na ikonie kamery w oknie obrazu oznacza, że z tej kamery jest pokazywany obraz na żywo.

Aby za pomocą aplikacji Operator Client sprawdzić działanie funkcji zapisu

- ▶ Kamery w drzewie logicznym, na których ikonie znajduje się czerwona kropka, nagrywają sygnał wizyjny.

Aby za pomocą aplikacji Operator Client sprawdzić działanie funkcji odtwarzania

- ▶ Podczas wyświetlania obrazu z kamery w trybie odtwarzania przesuwają się oś czasu.

W celu sprawdzenia innych funkcji skorzystaj z instrukcji oprogramowania BVMS dostępnej w internetowym katalogu produktów.

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 34.*
- *Połączenie zdalne za pomocą aplikacji Video Security, Strona 34.*

**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

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. Gdy pojawi się domyślny ekran systemu BVMS, naciśnij kombinację klawiszy CTRL+ALT+DELETE.
2. Wciśnij klawisz SHIFT, kliknij przycisk **Przełącz użytkownika** i trzymaj wciśnięty klawisz SHIFT jeszcze przez około pięć sekund.
3. Wprowadź nazwę użytkownika i hasło.
4. Na komputerze w folderze **Narzędzia** 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: ADMIN
7. Kliknij kartę **Konfiguracja**, a następnie kliknij opcję **Ustawienia hasła** i zmień domyślne hasło.
8. Kliknij kartę **Konfiguracja**, a następnie kliknij opcję **Konfiguracja alertu**.
9. Włącz funkcję **Komunikaty Trap SNMP** 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**.
Zostanie wyświetlone menu Przywracanie ustawień.
2. Wybierz jedną z następujących opcji:
 - **Początkowa konfiguracja fabryczna:** przywraca fabryczne domyślne ustawienia sygnału wizyjnego i usuwa wszystkie dane z dysków twardejch.
Lub
 - **Odzyskiwanie systemu (powrót do domyślnych ustawień fabrycznych):** przywraca fabryczne domyślne ustawienia sygnału wizyjnego, ale dane pozostają na dysku twardym.

Uwaga:

Mimo iż opcja **Odzyskiwanie systemu** nie usuwa materiału wizyjnego zapisanego na dyskach twardejch przechowujących dane, to w miejsce partycji systemu operacyjnego (wraz z ustawieniami oprogramowania VMS) instaluje konfigurację domyślną. Aby po odzyskiwaniu systemu można było przejść do istniejącego nagranych materiału wideo, należy przed odzyskiwaniem wyeksportować konfigurację systemu VMS, 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.

7.3 Serwisowanie i naprawa

System dyskowy jest objęty 3-letnią gwarancją. Wszelkie problemy są rozwiązywane zgodnie z zasadami obsługi klienta i serwisu Bosch.

Urządzenie pamięci masowej jest wysyłane razem z umową na serwisowanie i naprawę zawieraną z producentem.

Dział pomocy technicznej firmy Bosch jest wyłącznym punktem kontaktowym w razie awarii, natomiast zobowiązania w zakresie serwisowania i naprawy są realizowane przez producenta lub partnera.

Aby umożliwić działowi serwisu i naprawy u producenta wypełnianie zobowiązań w zakresie poziomu obsługi wynikających z umowy, system należy ponownie zarejestrować. W przeciwnym razie producent będzie mógł stosować jedynie ogólnikową zasadę najlepszych starań.

Opis niezbędnych informacji oraz spis ich adresatów są dołączone do każdej przesyłki w formie papierowej dokumentacji. Opis jest również dostępny w postaci elektronicznej w internetowym katalogu produktów Bosch.

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.

8.2 Usługi pomocy technicznej i Bosch Academy



Pomoc techniczna

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

Bosch Security and Safety Systems oferuje pomoc techniczną w następujących obszarach:

- [Aplikacje i narzędzia](#)
- [Modelowanie statystyk budynku](#)
- [Odbiór techniczny](#)
- [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**: <https://www.boschsecurity.com/xc/en/support/training/>



Bosch Security Systems B.V.

Torenallee 49
5617 BA Eindhoven
Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2020