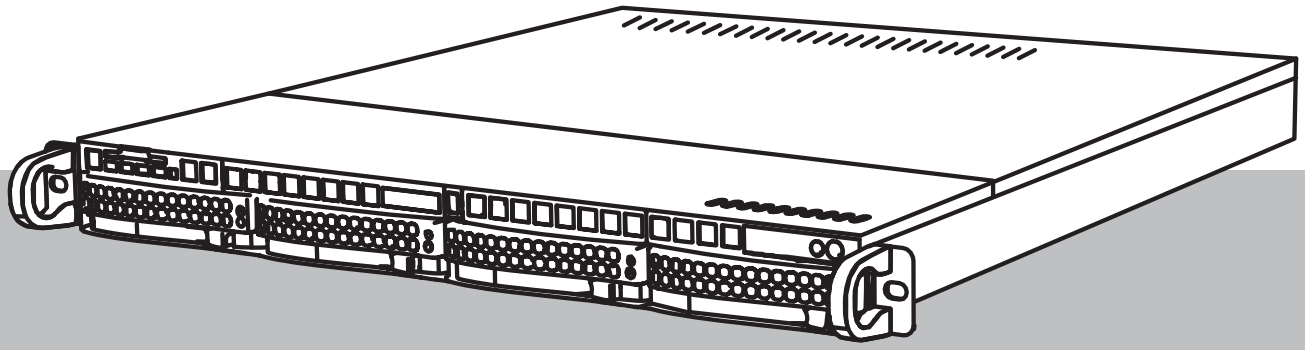
DIVAR IP all-in-one 6000

DIP-6440IG-00N | DIP-6444IG-4HD | DIP-6448IG-4HD | DIP-644IIG-4HD



pl Instrukcja obsługi

Spis treści

1 Bezpieczeństwo

Należy przestrzegać zasad bezpieczeństwa wyszczególnionych w tym rozdziale.

1.1 Zasady bezpieczeństwa dotyczące eksploatacji

Uwaga!
Użycie zgodne z przeznaczeniem
Produkt jest przeznaczony wyłącznie do użytku profesjonalnego. Produkt nie jest przeznaczony do instalacji w ogólnie dostępnych miejscach publicznych.

Uwaga!
Nie należy korzystać z produktu w miejscach, w których panuje wilgoć.

Uwaga!
Urządzenie należy zabezpieczyć przed wyładowaniami atmosferycznymi i skokami napięcia w sieci energetycznej.

Uwaga!
Urządzenie powinno znajdować się w otoczeniu czystym i przestronnym.

Uwaga!
Otwory w obudowie
Nie wolno zatykać ani zakrywać tych otworów. Wszystkie otwory w obudowie pełnią funkcję wentylacyjną. Otwory te zapobiegają przegrzaniu i zapewniają niezawodne działanie urządzenia.

Uwaga!
Nie należy otwierać ani zdejmować pokrywy urządzenia. Otwarcie lub zdjęcie pokrywy może spowodować uszkodzenie systemu i unieważnienie gwarancji.

Uwaga!
Na urządzenie nie wolno wylewać żadnych cieczy.

Ostrzeżenie!
Podczas serwisowania i pracy przy płytce 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.

Uwaga!
Przed przeniesieniem produktu odłączyć go od zasilania. Produkt należy przenosić z zachowaniem należytej ostrożności. Nadmierna siła lub wstrząs mogą spowodować uszkodzenie produktu i dysków twardych.

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!
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 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.

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 Wprowadzenie

DIVAR IP all-in-one 6000 jest przystępnym cenowo, uniwersalnym rozwiązaniem do rejestrowania, wyświetlania oraz zarządzania obrazami. Jest stosowany w sieciowych systemach dozoru wizyjnego wykorzystujących maksymalnie 64 kanały (w tym 8 kanałów licencjonowanych w pakiecie).

Rejestrator DIVAR IP all-in-one 6000 to urządzenie o wysokości 1U 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 6000 wykorzystuje wbudowaną konstrukcję i podstawowe komponenty oraz opiera się na systemie operacyjnym Microsoft Windows Server IoT 2022 for Storage Workgroup. DIVAR IP all-in-one 6000 posiada dyski twarde SATA „klasy korporacyjnej”, wymieniane podczas pracy, zapewniające do 72 TB pojemności brutto.

3 Ogólne informacje o systemie

System operacyjny

W systemach operacyjnych Microsoft Windows Server IoT 2022 for Storage Workgroup 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 2022 for Storage Workgroup 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.

Tryby pracy

Systemy DIVAR IP all-in-one 6000 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 urządzeń dozoru wizyjnego firmy Bosch, który zwiększa niepowtarzalne możliwości kamer i rozwiązań do zapisu obrazu firmy Bosch. Zawiera komponenty Video Streaming Gateway do integracji kamer innych firm.
– System czystego zapisu wideo oparty na podstawowych elementach i usługach Video Recording Manager, wykorzystujący wyjątkowe możliwości kamer i systemów zapisu firmy Bosch.
– Rozszerzenie pamięci masowej iSCSI dla systemu BVMS lub Video Recording Manager, który działa na innym urządzeniu. Maksymalnie cztery rozszerzenia pamięci masowej iSCSI można dodać do systemu BVMS lub Video Recording Manager działającego na urządzeniu DIVAR IP all-in-one 6000.

Aby skonfigurować system, w aplikacji DIVAR IP System Manager należy wybrać żądany tryb pracy.
Za pomocą aplikacji DIVAR IP System Manager można również 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/

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 2022 for Storage Workgroup. 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 dyski lokalne i podłączone zewnętrzne nośniki pamięci w poszukiwaniu pliku instalacyjnego DIVAR IP System Manager **SystemManager_x64_[software version].exe**, który znajduje się w folderze o następującej strukturze: *Drive root\BoschAppliance*.
   Skanowanie może chwilę potrwać. Należy poczekać na jego zakończenie.
7. Po wykryciu przez system pliku instalacyjnego, jest on wyświetlany na stronie **Software Selection**. Aby rozpocząć instalację, należy kliknąć pasek, na którym widoczny jest plik instalacyjny.
8. Jeśli podczas skanowania plik instalacyjny nie zostanie odnaleziony, 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 plik ZIP **SystemManager_[software version].zip** i zapisać go na nośniku pamięci, takim jak pamięć USB.
   - Rozpakować plik na nośniku pamięci, upewniając się, że folder **BoschAppliance** został umieszczony w głównym folderze nośnika pamięci.
   - Podłączyć nośnik pamięci do systemu DIVAR IP all-in-one.
     System automatycznie przeskanuje nośnik pamięci w poszukiwaniu pliku instalacyjnego.
     Skanowanie może chwilę potrwać. Należy poczekać na jego zakończenie.
   - Po wykryciu pliku instalacyjnego zostanie on wyświetlony na stronie **Software Selection**. Aby rozpocząć instalację, należy kliknąć pasek, na którym widoczny jest plik instalacyjny.
     Uwaga: Aby plik instalacyjny został wykryty automatycznie, musi znajdować się w folderze o następującej strukturze: *Drive root\BoschAppliance* (na przykład *F:\BoschAppliance*).
     Jeśli plik instalacyjny znajduje się w innej lokalizacji, która nie odpowiada wstępnie zdefiniowanej strukturze folderu, kliknąć  , aby przejść do odpowiedniej lokalizacji. Następnie należy kliknąć plik instalacyjny, aby rozpocząć instalację.
9. Przed rozpoczęciem instalacji zostanie wyświetlone okno dialogowe **End User License Agreement (EULA)**. Należy przeczytać warunki umowy licencyjnej, a następnie kliknąć przycisk **Accept**, aby kontynuować. Rozpocznie się instalacja.

10. Po zakończeniu instalacji system zostanie ponownie uruchomiony i wyświetlona zostanie strona logowania systemu Windows. Należy zalogować się do konta administratora.
11. W przeglądarce Microsoft Edge zostanie wyświetlona strona systemu **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 żądaną wersję oprogramowania, aby skonfigurować system DIVAR IP all-in-one.
    Uwaga: 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.
    – Następnie podłączyć nośnik pamięci do systemu DIVAR IP all-in-one.

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

4.3.1 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 żądaną 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/

4.3.2 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 żądaną do zainstalowania wersję 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.

4.3.3 Wybór trybu pracy pamięci masowej 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 żądaną do zainstalowania wersję 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 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.
4. 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 Uaktualnianie oprogramowania

Za pomocą aplikacji DIVAR IP System Manager można uaktualnić zainstalowane oprogramowanie w systemie.
Najnowsze oprogramowanie oraz dostępne pakiety aktualizacyjne można znaleźć w materiałach do pobrania Bosch Security and Safety Systems na stronie:
https://downloadstore.boschsecurity.com/

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. Uruchamianie aplikacji 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.
     Aplikacja DIVAR IP System Manager zostanie uruchomiona.
   - Jeśli system pracuje w trybie pracy BVMS, kliknij ikonę DIVAR IP System Manager na pulpicie BVMS i zaloguj się do konta administratora BVRAdmin. Aplikacja DIVAR IP System Manager otworzy się w oknie dialogowym w trybie pełnoekranowym (okno można zamknąć, naciskając klawisz 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 żądaną 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 wyłączać systemu ani nie usuwać 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 naciśnij 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.

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 15*.
2. *Konfigurowanie przekierowania portów, Strona 15*.
3. *Wybór odpowiedniego klienta, Strona 15*.

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 15*.
- – *Połączenie zdalne za pomocą aplikacji Video Security, Strona 16*.

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 skrótu  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_rozwiązania_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.

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

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 17*).
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 17*).
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 interfejsu IPMI

Urządzenie DIVAR IP all-in-one 6000 ma dedykowany port IPMI na tylnej ściance.
Interfejs IPMI umożliwia dostęp, monitorowanie, diagnozowanie i zarządzanie systemem DIVAR IP all-in-one 6000 jako serwerem zdalnym.
W każdym urządzeniu DIVAR IP all-in-one 6000 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 6000 uruchomi się ponownie.

7.3 Wymiana uszkodzonego dysku twardego i konfiguracja nowego dysku twardego

Jeśli dysk twardy zainstalowany w systemie DIVAR IP all-in-one 6000 jest uszkodzony, dioda LED odpowiedniego dysku twardego świeci na czerwono. W takiej sytuacji należy wykonać następujące czynności:

1. *Wymiana uszkodzonego dysku twardego, Strona 19*.
2. *Rekonstrukcja macierzy RAID5 za pomocą nowego dysku twardego, Strona 19*.

Uwaga!
Ta procedura dotyczy tylko domyślnej konfiguracji RAID5 i tylko przypadku, gdy jeden dysk twardy w konfiguracji RAID5 jest uszkodzony. Tylko w takim przypadku można zapewnić, że żadne dane nie zostaną utracone.

Uwaga!
Bosch nie ponosi odpowiedzialności za utratę danych, uszkodzenia ani systemowe awarie jednostek wyposażonych w dyski twarde niedostarczane przez firmę Bosch. Bosch nie może zapewnić wsparcia technicznego, jeśli przyczyną problemu są dyski twarde niedostarczane przez firmę Bosch. Aby rozwiązać potencjalne problemy sprzętowe, firma Bosch będzie wymagała zainstalowania dostarczonych przez nią dysków twardych.

7.3.1 Wymiana uszkodzonego dysku twardego

Aby wymienić uszkodzony dysk twardy:

- Wyjmij uszkodzony dysk twardy z jednostki i zainstaluj nowy dysk twardy.
  Zob. *Instalacja dysku twardego SATA* w Instrukcji instalacji.

7.3.2 Rekonstrukcja macierzy RAID5 za pomocą nowego dysku twardego

Automatyczna rekonstrukcja macierzy RAID5

1. Na pulpicie DIVAR IP all-in-one kliknij dwukrotnie skrót **Launch LSA**.
   Aplikacja **LSI Storage Authority** uruchomi się i wyświetli się strona **Remote Server Discovery**.
2. Zaloguj się przy użyciu poświadczeń konta administratora **BVRAdmin**.
   Wyświetli się okno dialogowe z komunikatem, że istnieje sterownik, który stanowi krytyczny problem.
3. Kliknij pasek **Controller ID:**, aby otworzyć ustawienia sterownika.
   - Jeśli uszkodzony dysk twardy nie został jeszcze wyjęty, wyświetli się w **Drives** > **Foreign Drives** > **Unconfigured Drives.**
   - Po usunięciu uszkodzonego i zainstalowaniu nowego dysku twardego system automatycznie uruchamia rekonstrukcję macierzy RAID5 z nowym dyskiem twardym, a pasek postępu pokazuje postęp rekonstrukcji.
4. Po udanym zakończeniu rekonstrukcji wyświetli się ikona  .

Ręczna rekonstrukcja macierzy RAID5

Jeżeli rekonstrukcja macierzy RAID5 nowego dysku twardego nie rozpocznie się automatycznie, należy:

1. W oknie dialogowym ustawień sterownika w **Drives** > **Foreign Drives** > **Unconfigured Drives** wybierz dysk twardy o statusie **Unconfigured Bad**, a następnie w okienku po prawej stronie wybierz **Make Unconfigured Good**.
   Wyświetli się okno dialogowe.
2. Zaznacz pole wyboru **Confirm**, a następnie kliknij **Yes, Make Unconfigured Good**, aby kontynuować.
   Zostanie uruchomiona rekonstrukcja macierzy RAID5 wraz z nowym dyskiem twardym.
3. Po udanym zakończeniu rekonstrukcji wyświetli się ikona  .

7.4 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 17*).
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.

7.5 Przywracanie ustawień fabrycznych

Aby przywrócić jednostkę:

1. Włącz urządzenie i naciśnij podczas testu systemu BIOS klawisz F7, aby wejść do systemu Windows PE.
   Pojawi się okno dialogowe **System Management Utility**.
2. Należy wybrać jedną z poniższych opcji:
   - **System factory default**: ten wybór spowoduje sformatowanie partycji danych z filmami wideo i przywrócenie na partycji systemu operacyjnego fabrycznego obrazu domyślnego.
     Proces ten może zająć do 5 minut.
   - **Full data overwrite and system factory default**: ten wybór spowoduje sformatowanie partycji danych z filmami wideo z całkowitym nadpisaniem istniejących danych oraz przywrócenie na partycji systemu operacyjnego fabrycznego obrazu domyślnego.
     Uwaga: proces ten może zająć do 110 godzin.
   - **OS system recovery only**: ten wybór spowoduje przywrócenie na partycji systemu operacyjnego fabrycznego obrazu domyślnego oraz zaimportowanie istniejących wirtualnych dysków twardych z istniejących partycji danych wideo.
     Proces ten może zająć do 5 minut.

   Uwaga:
   OS system recovery only 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. Potwierdź wybraną opcję.
   System rozpocznie proces formatowania dysków i przywracania obrazu.
4. Po zakończeniu procesu przywracania należy potwierdzić ponowne uruchomienie systemu.
   System uruchomi się ponownie i wykonane zostaną procedury konfiguracyjne.
5. Po zakończeniu procesu zostanie wyświetlony ekran wyboru języka systemu Windows.
6. Kontynuuj wstępną konfigurację systemu.

Patrz

- *Pierwsze logowanie i wstępna konfiguracja systemu, Strona 9*

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/.

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.

202211241306