

DSS4004S2 – skrócona instrukcja użytkownika

Wersja 1.0.1

Zalecenia dotyczące cyberbezpieczeństwa



Obowiązkowe działania do podjęcia celem zwiększenia cyberbezpieczeństwa

1. Zmieniaj hasła i wybieraj silne hasła:

Najczęstszym powodem zhakowania systemu jest słabe lub domyślne hasło. Zaleca się bezzwłoczną zmianę domyślnych haseł oraz wybranie silnego hasła zawsze, kiedy to tylko możliwe. Silne hasło powinno składać się z co najmniej 8 znaków i być kombinacją znaków specjalnych, cyfr oraz małych i wielkich liter.

2. Aktualizuj oprogramowanie sprzętowe

Zgodnie ze standardowymi procedurami w branży technologicznej zalecamy aktualizowanie oprogramowania sprzętowego urządzeń NVR, DVR oraz kamer IP celem zapewnienia, że system jest aktualny oraz zostały zainstalowane najnowsze łatki i poprawki.

Zalecane działania nakierowane na zwiększenie bezpieczeństwa w sieci

1) Regularnie zmieniaj hasła

Regularnie zmieniaj dane logowania do swoich urządzeń celem zapewnienia, że tylko upoważnieni użytkownicy mogą uzyskać dostęp do systemu.

2) Włącz filtr adresów IP

Włączenie filtra adresów IP uniemożliwi osobom z innymi niż wskazane adresami IP uzyskanie dostępu do systemu.

3) Ustaw przekierowanie tylko tych portów, których musisz używać

W przypadku platform za zaporą sieciową liczba mapowanych portów na zaporze musi zostać ograniczona. Zaleca się mapowanie tylko tych portów, które muszą być używane przez platformę. Mapowanie innych portów jest zabronione.

4) UPnP

- UPnP spróbuje automatycznie przekierować porty w Twoim routerze lub modemie. W normalnych okolicznościach byłoby to pożądane. Jednak jeśli Twój system automatycznie przekieruje porty, a Ty zostawisz domyślne dane logowania, może się to skończyć wizytą nieproszonych gości.
- Nawet jeśli ręcznie przekierujesz porty HTTP i TCP w swoim routerze/modemie, tę funkcję i tak należy wyłączyć. Wyłączenie UPnP zaleca się też generalnie wtedy, gdy funkcja ta nie jest wykorzystywana.

5) SNMP

Wyłącz protokół SNMP, jeśli z niego nie korzystasz. Jeśli korzystasz z protokołu SMNP, włączaj go tylko tymczasowo, wyłącznie do celów śledzenia pakietów i testowania.

6) Multicast

Funkcja Multicast służy do udostępniania strumieni wideo pomiędzy dwoma rejestratorami. Obecnie nie są znane żadne problemy dotyczące tej funkcji, ale jeśli z niej nie korzystasz, wyłączenie jej zwiększy bezpieczeństwo Twojej sieci.

7) Zabezpiecz urządzenie fizycznie

W idealnym scenariuszu chcesz zabezpieczyć swój system przed jakimkolwiek nieuprawnionym dostępem. Najlepszym sposobem, aby to osiągnąć, jest zamontowanie rejestratora w zamkniętej szafce, szafie serwerowej lub w pomieszczeniu zamkniętym na klucz.

8) Odizoluj sieć urządzenia NVR i kamer IP

Sieć, w której działają Twoje kamery IP oraz urządzenia NVR, nie powinna być publiczną siecią komputerową. Dzięki temu nieproszeni goście nie będą mogli uzyskać dostępu do tej samej sieci, której do prawidłowego funkcjonowania potrzebuje system bezpieczeństwa.

Informacje ogólne



Niniejszy dokument ma za zadanie dostarczyć użytkownikom informacji na temat listy kontrolnej, instalacji oraz konfiguracji platformy zarządzania monitoringiem wizyjnym DSS.

Modele

DSS7016D-S2, DHI-DSS7016DR-S2, DSS7016D-S2 oraz DSS7016DR-S2.

Informacje dotyczące bezpieczeństwa

W instrukcji mogą pojawiać się symbole o określonych znaczeniach przedstawione w poniższej tabeli.

Symbol	Znaczenie
 CAUTION	Oznacza potencjalne zagrożenie, które może doprowadzić do uszkodzenia mienia, utraty danych, obniżenia wydajności pracy, lub mieć inne, nieprzewidziane skutki.
 NOTE	Oznacza dodatkowe informacje, które stanowią uzupełnienie głównej treści dokumentu.

Historia zmian

Nr	Wersja	Historia zmian	Data publikacji
1	Wersja 1.0.0	Wydanie pierwsze.	1 sierpnia 2018 r.
2	Wersja 1.0.1	Dodana aplikacja lokalna i usunięta konfiguracja inicjalizacji.	25 PAŹDZIERNIKA 2018 r.

Informacja o ochronie prywatności

Właściciel urządzenia lub administrator danych może zbierać dane osobowe, takie jak zdjęcia twarzy, odciski palców, numery rejestracyjne samochodów, adresy e-mail, numery telefonów, współrzędne GPS itp. Właściciel urządzenia lub administrator danych musi przestrzegać lokalnych przepisów i regulacji dotyczących ochrony prywatności, aby chronić uzasadnione prawa i interesy innych osób, wdrażając odpowiednie środki, w tym m.in. zapewniając osobom, których dane dotyczą, wyraźne i widoczne oznakowanie strefy monitorowanej oraz podając dane odpowiednich osób do kontaktu w sprawie ochrony danych osobowych.

Informacje o instrukcji

- Niniejsza instrukcja ma charakter wyłącznie referencyjny. W razie rozbieżności między treścią instrukcji a faktycznym wyglądem lub działaniem produktu należy kierować się stanem faktycznym.
- Firma nie ponosi żadnej odpowiedzialności za szkody powstałe wskutek użytkowania urządzenia niezgodnie z instrukcją.

- Podręcznik będzie aktualizowany wraz ze zmianami przepisów i regulacji obowiązujących w poszczególnych krajach. Szczegółowe informacje dostępne są w papierowej instrukcji użytkownika, na płycie CD-ROM, po zeskanowaniu kodu QR oraz na oficjalnej stronie internetowej firmy. W razie rozbieżności między treścią wersji papierowej i elektronicznej instrukcji obowiązuje wersja elektroniczna.
- Wszystkie projekty oraz oprogramowanie mogą ulec zmianie bez wcześniejszego zawiadomienia na piśmie. Aktualizacje produktu mogą skutkować pewnymi różnicami między dokumentacją produktu a niniejszą instrukcją. W celu uzyskania najnowszego opisu oprogramowania i dokumentacji uzupełniającej prosimy o kontakt z działem obsługi klienta.
- Możliwe są pewne rozbieżności w zakresie danych technicznych, opisów funkcji i obsługi urządzenia, a także błędy w druku. W przypadku wątpliwości lub niejasności należy zwrócić się do nas z prośbą o wyjaśnienia.
- Jeśli nie można otworzyć instrukcji w formacie PDF, należy zaktualizować program do otwierania takich plików lub skorzystać z innego oprogramowania.
- Wszelkie znaki towarowe, zastrzeżone znaki towarowe oraz nazwy firm wymienione w niniejszej instrukcji należą do ich prawowitych właścicieli.
- Jeśli podczas korzystania z urządzenia wystąpiły jakiegokolwiek problemy, należy poszukać pomocy na naszej stronie internetowej, skontaktować się z dostawcą lub działem obsługi klienta.
- W przypadku wątpliwości lub niejasności należy zwrócić się do nas z prośbą o wyjaśnienia.

Ważne instrukcje dotyczące bezpieczeństwa oraz ostrzeżenia



Wymogi dotyczące środowiska roboczego

- Nie umieszczaj ani nie montuj urządzenia w miejscu, na które bezpośrednio padają promienie słoneczne, ani w pobliżu źródeł ciepła.
- Chroń urządzenie przed wilgocią, kurzem oraz sadzą.
- Zamontuj urządzenie w pozycji poziomej na stabilnym podłożu, aby zapobiegać jego upadkowi.
- Nie wolno dopuścić do kapania ani pryskania cieczy na urządzenie. Upewnij się, że na urządzeniu nie stoją żadne naczynia z cieczą. Ma to na celu ochronę przed dostaniem się cieczy do urządzenia.
- Zamontuj urządzenie w dobrze wentylowanym miejscu i nie przesłaniaj jego otworów wentylacyjnych.
- Urządzenia należy używać zgodnie z oznaczeniami dotyczącymi znamionowego napięcia wyjściowego i wejściowego.
- Nie należy demontować urządzenia.
- Urządzenie należy transportować, użytkować oraz przechowywać w dozwolonym przedziale wilgotności i temperatur.

Bezpieczeństwo elektryczne

- Niewłaściwe korzystanie z akumulatora może skutkować pożarem, wybuchem lub zapłonem.
- Podczas wymiany akumulatora należy się upewnić, że stosowany jest ten sam model.
- Należy używać kabli zasilających zalecanych dla danego regionu oraz przestrzegać wartości znamionowych zasilania.
- Należy używać zasilacza dołączonego do urządzenia. W przeciwnym razie może to doprowadzić do urazów u osób bądź uszkodzenia urządzenia.
- Należy korzystać ze źródła zasilania zgodnego z wymogami dla instalacji niskonapięciowych (SELV) oraz ze standardem LPS (Limited Power Source) IEC60950-1. Wymagania dotyczące zasilania przedstawiono na etykiecie urządzenia.
- Produkty z wtyczką typu I należy podłączać do gniazdek z uziemieniem.
- Przewód zasilający daje się odłączyć od urządzenia. Należy prowadzić go tak, aby nie utrudniał obsługi urządzenia.

Zalecenia dotyczące cyberbezpieczeństwa	II
Wstęp	III
Ważne instrukcje dotyczące bezpieczeństwa oraz ostrzeżenia	V
1 Lista kontrolna	1
1.1 Opakowanie	1
1.2 Porty	1
1.2.1 Panel przedni	2
1.2.2 Panel tylny	2
1.3 Instalacja urządzenia	3
Aplikacja lokalna	4
2.1 Funkcjonalność	4
2.2 Konfiguracja	5
2.2.1 Ustawienia podstawowe	5
2.2.2 Konfiguracja sieci	5
2.3 Analiza działania	8
2.3.1 Analiza działania	8
2.3.2 Zarządzanie systemem	9
Konfiguracja systemu	17

1.1 Opakowanie

Otwórz opakowanie celem sprawdzenia zawartości. Zwróć uwagę na stan opakowania, urządzenia i akcesoriów. Sprawdź, czy produkt nie jest uszkodzony oraz czy nie brakuje jakichś części.

- **Opakowanie:** Urządzenie nie powinno być uszkodzone. Po otwarciu opakowania sprawdź, czy zawiera ono kompletny zestaw akcesoriów oraz dysk twardy.
- **Urządzenie:** Urządzenie nie powinno mieć rys ani uszkodzeń, a opakowanie ochronne nie powinno być w widoczny sposób uszkodzone.
- **Akcesoria:** typ i liczba podana na liście kontrolnej powinny być zgodne ze stanem faktycznym. Akcesoria nie powinny być uszkodzone.



Po sprawdzeniu, czy w zestawie znajdują się wszystkie materiały i akcesoria, należy umieścić je w bezpiecznym miejscu.

Tabela 1-1

Nr	Lista kontrolna	Liczba	Opis
1	Serwer	1	-
2	Śruby antywibracyjne do dysku twardego	12	-
3	Podkładki antywibracyjne	12	-
4	Kabel zasilający	1	1,5 m
5	Skrócona instrukcja użytkownika	1	-

1.2 Porty

Przedni panel urządzenia zawiera przycisk zasilania, porty USB oraz diody stanu (dysku systemowego, alarmu i sieci). Panel tylny urządzenia zawiera gniazdo zasilania, porty sieci Ethernet, port szeregowy oraz inne porty, a dodatkowo zarezerwowane złącze alarmowe, złącze HDMI i inne porty rozszerzeń.

1.2.1 Panel przedni

Rysunek 1-1



Tabela 1-2

Nr	Złącze lub oznaczenie	Definicja
1	Wskaźnik połączenia z siecią	Dioda mruga na niebiesko, gdy urządzenie jest połączone z siecią.
2	Wskaźnik alarmowy	Dioda mruga na niebiesko, gdy urządzenie uruchomiło alarm.
3	HDD1	Wskaźnik dysku systemowego, który mruga podczas odczytywania danych z dysku.
4	HDD2	
5	HDD3	
6	HDD4	
7	Złącze USB 2.0	2 złącza (białe)
8	Przycisk zasilania	Naciśnij ten przycisk, aby włączyć urządzenie. Urządzenie ma wskaźnik stanu zasilania (niebieskie światło oznacza normalną pracę urządzenia). Naciśnij i przytrzymaj ten przycisk, aby wyłączyć urządzenie.

1.2.2 Panel tylny

Rysunek 1-2

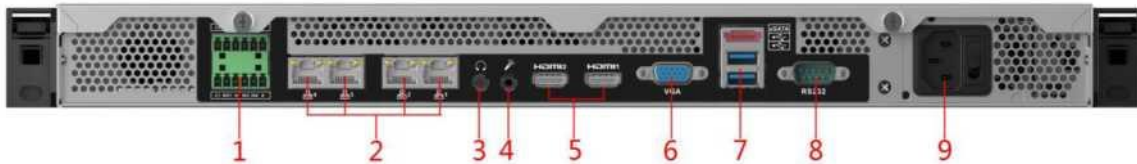


Tabela 1-3

Nr	Złącze lub oznaczenie	Definicja
1	Wejście i wyjście alarmowe	Zarezerwowane. Umożliwia dostęp za pomocą protokołu RS485.
2	Port Ethernet	Obsługa pełnego duplexu na obu portach z automatycznym doбором prędkości 10 Mb/s, 100 Mb/s lub 1 Gb/s. Domyślnie platforma używa portu Ethernet 1.
3	Wyjście audio	Wyjście audio 3,5 mm.
4	Wejście interkomu audio	Wejście audio 3,5 mm.
5	Złącze HDMI	2 kanały (zarezerwowane).
6	Złącze VGA	DB 15 pinów. Umożliwia podłączenie urządzenia ze złączem VGA.
7	Port eSATA	Umożliwia podłączenie urządzenia ze złączem eSATA.
8	RS232	Port szeregowy do debugowania.
9	Port zasilania	100–240 V AC / 47–63 Hz. Możliwa podmiana w trakcie pracy.

1.3 Instalacja urządzenia

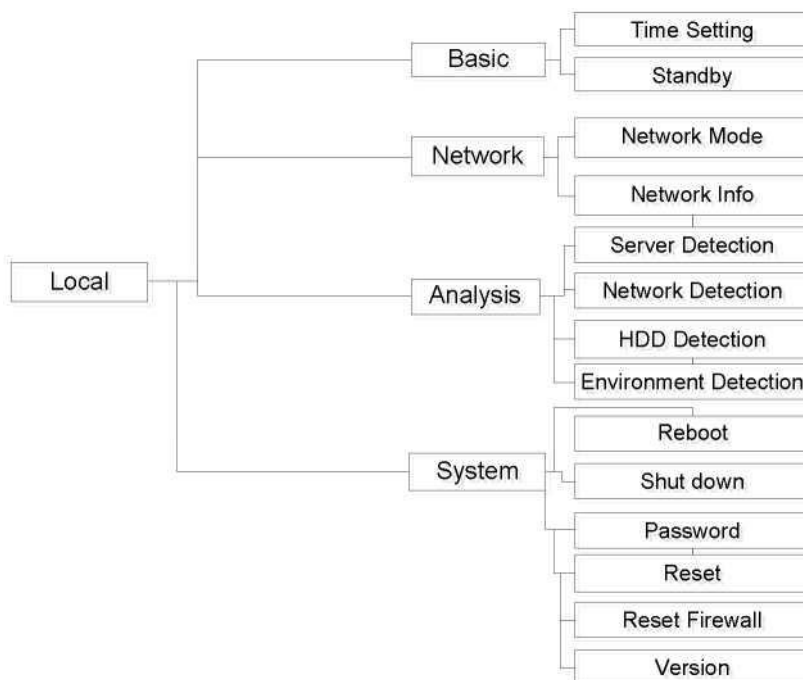
Podłącz wszystkie kable do odpowiednich złączy, a następnie podłącz urządzenie do źródła zasilania.

2 Aplikacja lokalna

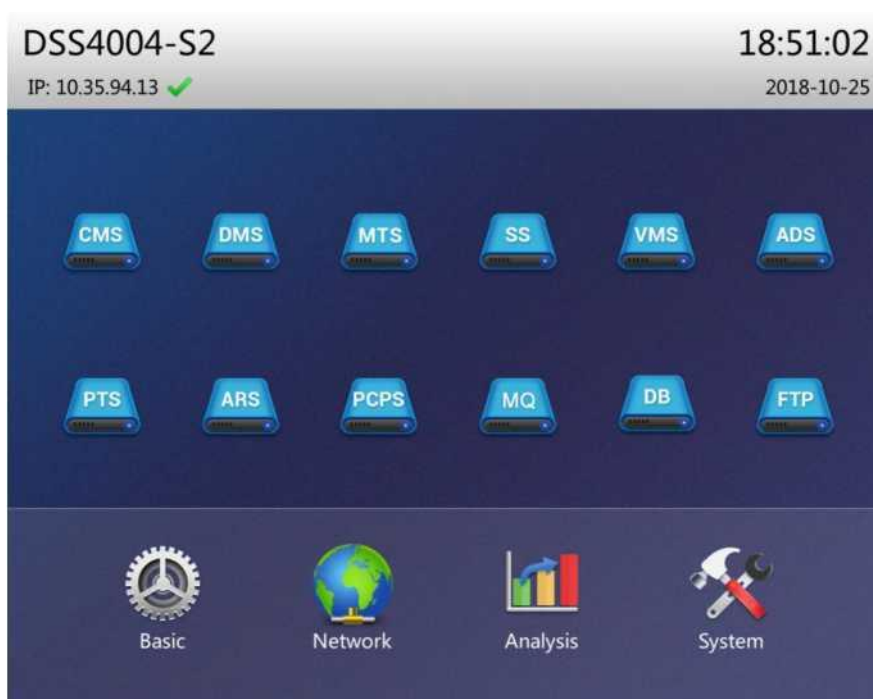
2.1 Funkcjonalność

W tej części przedstawiono funkcje aplikacji lokalnej. Patrz Rysunek 2-1. Po uruchomieniu urządzenia wyświetlany jest interfejs lokalny. Patrz Rysunek 2-2.

Rysunek 2-1



Rysunek 2-2



2.2 Konfiguracja

2.2.1 Ustawienia podstawowe

Kliknij pozycję **Basic Setting** (Ustawienia podstawowe) w interfejsie lokalnym i skonfiguruj datę, godzinę oraz inne ustawienia.

Rysunek 2-3 Ustawienia podstawowe

The screenshot shows the 'Basic Setting' window. It contains the following fields and options:

- Time Setting:**
 - System Time: 2018-10-25 18:45:05 (with a 'Save' button)
 - Date Format: YMD (dropdown)
 - Date Separator: - (dropdown)
 - Time Format: 24-hour (dropdown)
- Other Setting:**
 - Device Name: DSS4004-S2
 - Standby Time: 5 (with a note: '(Standby time must be 5-15 min)')

Buttons: 'OK' and 'Cancel' are located at the bottom right.

Tabela 2-1 Opis ustawień podstawowych

Parametr	Opis
System Time (Czas systemowy)	Ustaw czas lokalny.
Date Format (Format daty)	Te ustawienia dotyczą przede wszystkim formatu wyświetlania daty i godziny na stronie głównej aplikacji lokalnej. Można je dopasować stosownie do potrzeb użytkownika.
Date Separator (Separator daty)	
Time Format (Format godziny)	
Device Name (Nazwa urządzenia)	Domyślna nazwa to model urządzenia. W nazwie można użyć znaków alfabetu łacińskiego.
Standby Time (Czas czuwania)	To ustawienie określa, po jakim czasie nieużywania interfejs lokalny przełącza się w tryb czuwania. Ustawienie domyślne to 5 minut, a maksymalne to 15 minut.

2.2.2 Konfiguracja sieci

Kliknij pozycję **Network Setting** (Konfiguracja sieci) w interfejsie lokalnym, aby skonfigurować informacje o sieci.

Rysunek 2-4 Konfiguracja sieci

Network Setting

Network Mode: Multi-address

Select Port: Port 1 Default Port: Port 1

IP Address: 10 . 35 . 95 . 30

Subnet Mask: 255 . 255 . 252 . 0 Preferred DNS: 8 . 8 . 8 . 8

Default Gateway 10 . 35 . 95 . 254 Alternate DNS: 8 . 8 . 4 . 4

OK Cancel

Tabela 2-2 Opis ustawień podstawowych

Parametr	Uwaga
----------	-------

Parametr	Opis
Network Mode (Tryb sieci)	<p>Dostępne są 4 tryby.</p> <ul style="list-style-type: none"> • Multi-address (Wiele adresów) Chodzi tu o tryb multiadresacji kart sieciowych. Każda karta może być skonfigurowana do obsługi różnych segmentów sieci i być odpowiedzialna za dostęp do wielu segmentów. Rozwiązanie to sprawdza się w sytuacji, gdy ważna jest duża niezawodność sieci. Można na przykład skonfigurować podwójny zapas typu hot standby, wykorzystując kartę sieciową nr 2 do skonfigurowania adresu IP sygnału heartbeat. Można też wykorzystać tę możliwość przy rozszerzaniu pamięci masowej z wykorzystaniem protokołu iSCSI. Porty sieciowe są wykorzystywane w następujący sposób: port sieciowy 1 służy do komunikacji z usługą, port 2 jest zarezerwowany, porty 3 i 4 są używane do przechowywania danych z wykorzystaniem protokołu iSCSI. • Fault tolerance (Tolerancja usterek) Wiele kart Ethernet korzystających z jednego adresu IP. Zwykle działa tylko jedna karta sieciowa. W przypadku jej awarii urządzenie automatycznie włączy kolejną standardową kartę sieciową, aby zapewnić nieprzerwane połączenie z siecią. • Load balancing (Równoważenie obciążenia) Wiele kart Ethernet korzystających z jednego adresu IP. Te karty sieciowe działają razem, dzieląc między sobą obciążenie sieci i zapewniając lepszą przepustowość niż pojedyncza karta sieciowa. Gdy jedna z kart zacznie działać nieprawidłowo, przekaże ona swoje obciążenie pozostałym dostępnym kartom, zapewniając niezawodność sieci. • Link Aggregation (Agregacja łączy) Poprzez powiązanie kart sieciowych można sprawić, że dodatkowa karta sieciowa uczestniczy w procesie przesyłu danych i bierze na siebie część obciążenia. Chcąc przesyłać strumień większy niż 1K, można na przykład powiązać ze sobą 2 adresy IP, a trzeci zostawić niepowiązany. Wówczas przez połączenie z powiązanymi 2 adresami można przesyłać strumień 2K, a przez trzecią kartę sieciową 1K. Rozwiązanie to sprawdza się przy przekazywaniu strumieni, natomiast nie jest zalecane, gdy występuje potrzeba ich rejestrowania. Agregacja łączy jest dostępna tylko, jeśli obsługuje ją bezpośrednio podłączony switch.
Select Port (Wybierz port)	Ta opcja umożliwi skonfigurowanie domyślnego portu sieciowego. Platforma domyślnie używa portu sieciowego 1 (jeśli użytkownik wybierze gigabitowy port optyczny, dostępna jest wyłącznie opcja wielu adresów). Port można zmienić na inny stosownie do potrzeb.
Default Port (Port domyślny)	Po wybraniu domyślnego portu sieciowego karta sieciowa będzie przekierowywać pakiety danych z niesąsiadujących ze sobą segmentów (np. sieci WAN) przez port domyślny.
IP Address (Adres IP)	Po wybraniu karty sieciowej użytkownik może skonfigurować jej adres IP, maskę podsieci, bramę domyślną, adres preferowanego serwera DNS i adres zapasowego serwera DNS.
Subnet Mask (Maska podsieci)	
Preferred DNS (Preferowany DNS)	
Default Gateway (Brama domyślna)	
Alternate DNS (Zapasowy DNS)	

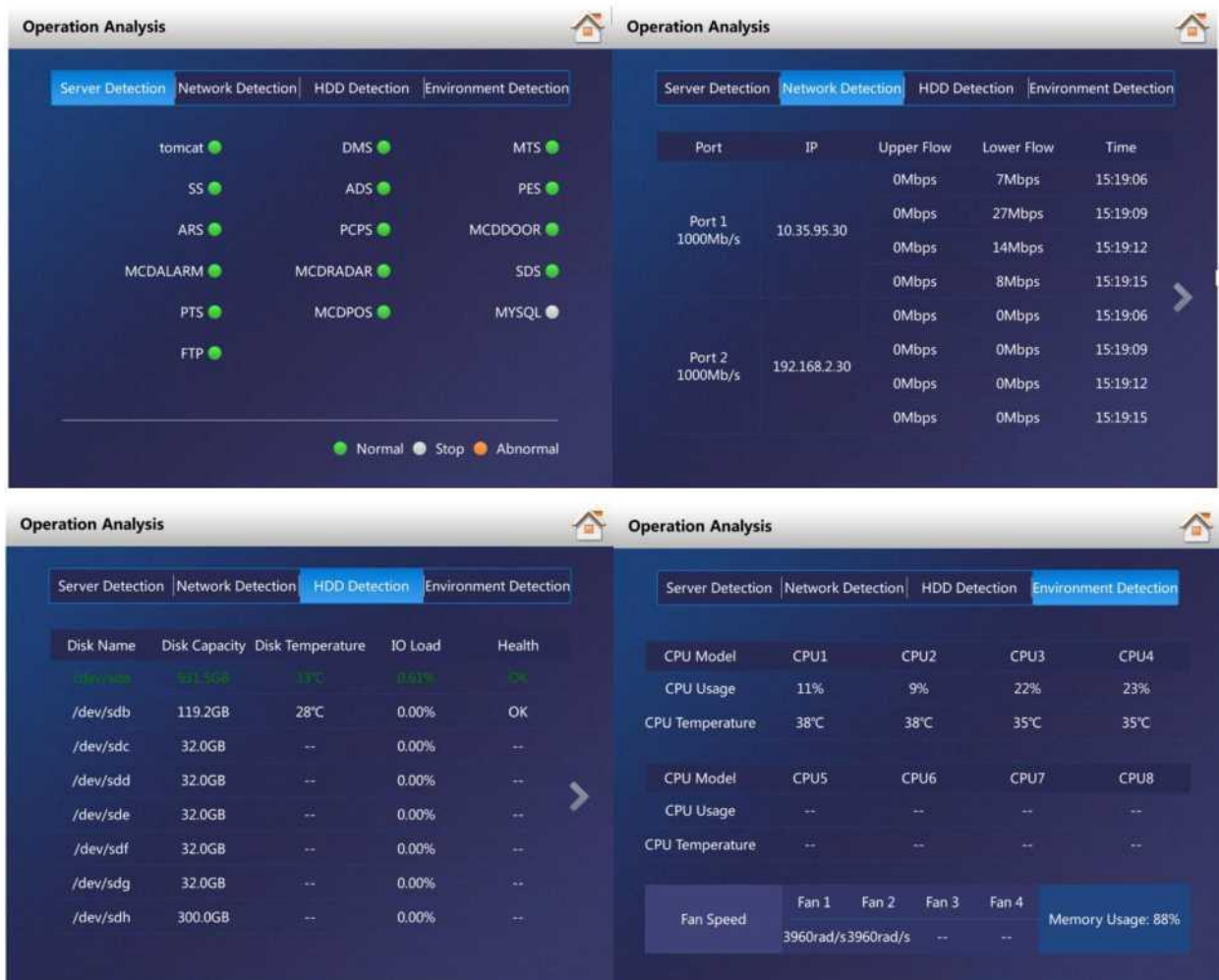
2.3 Analiza działania

2.3.1 Analiza działania

Kliknij pozycję **Operation Analysis (Analiza działania)** w interfejsie lokalnym, aby sprawdzić stan serwera platformy, sieci, dysku twardego i środowiska.

- **Server Detection (Stan serwera):** wykrywanie w czasie rzeczywistym stanu serwera platformy. Możliwe stany serwera to: Normal (Normalny), Stop (Zatrzymany), Abnormal (Nieprawidłowy) itp.
- **Network Detection (Stan sieci):** wykrywanie w czasie rzeczywistym przepływu danych przez port sieciowy w obu kierunkach.
- **HDD Detection (Stan dysku twardego):** wykrywanie w czasie rzeczywistym dostępnej przestrzeni dyskowej, temperatury, obciążenia we/wy oraz ogólnej kondycji dysku. W wierszu oznaczonym kolorem zielonym domyślnie wyświetlane są powyższe informacje o dysku twardym.
- **Environment Detection (Wykrywanie warunków środowiskowych):** wykrywanie w czasie rzeczywistym temperatury i stopnia wykorzystania procesora, szybkości pracy wentylatora oraz użycia pamięci dla bieżącej platformy.

Rysunek 2-5 Analiza działania



2.3.2 Zarządzanie systemem

W interfejsie lokalnym kliknij pozycję System Management (Zarządzanie systemem). Obsługiwane są następujące operacje:

- Reboot (Ponowne uruchomienie): przed ponownym uruchomieniem zapisz dane systemowe.
- Shut down (Wyłączenie): przed wyłączeniem zapisz dane systemowe. Bezpośrednie odłączenie źródła zasilania jest zabronione.
- Password (Hasło): przywraca obecne hasło do pierwszego hasła używanego przy inicjalizacji konta administratora, systemu, serwera FTP, bazy danych i konfiguracji urządzenia.
- Reset Firewall (Resetowanie zapory sieciowej): ponowne włączenie portu SSH (22) pozwala uniknąć błędów konfiguracji białej listy w systemie, który może powodować awarię platformy.
- Version (Wersja): wyświetla model produktu, numer seryjny, identyfikator oraz wersję systemu.

Rysunek 2-6



3 Konfiguracja systemu

Lokalna aplikacja serwera umożliwia wykonywanie podstawowych czynności konfiguracyjnych, takich jak ustawienie godziny, języka, wybór sieci czy zarządzanie. Aplikacja umożliwia analizowanie i zmienianie podstawowych ustawień w samodzielnym środowisku. W celu przeprowadzenia dokładniejszej konfiguracji usług, klastra, pamięci masowej, powiązań, mapowań, bazy danych i zabezpieczeń, należy zalogować się do menu konfiguracji systemu. Szczegółowe informacje zawiera instrukcja użytkownika.

Adres dostępowy do konfiguracji systemu to <http://IP/config>.



- Domyślny adres IP serwera to 192.168.1.108, domyślna nazwa użytkownika to admin, a domyślne hasło to 123456.
- Przy pierwszym logowaniu prosimy o przeprowadzenie inicjalizacji zgodnie z komunikatami systemowymi.

Rysunek 3-1

