AXIS S3016 Recorder

Podręcznik użytkownika

O urządzeniu

O urządzeniu

O urządzeniu

AXIS S3016 Recorder to sieciowy rejestrator wideo ze zintegrowanym switchem PoE i dyskami twardymi klasy systemu dozoru. Ponadto posiada port USB 3.0 ułatwiający eksportowanie materiału wizyjnego. Dostępne są trzy modele rejestratora: 8 TB, 16 TB i 32 TB.

Rozpocznij

Uzyskiwanie dostępu do urządzenia

Wyszukiwanie urządzenia w sieci

Aby znaleźć urządzenia Axis w sieci i przydzielić im adresy IP w systemie Windows®, użyj narzędzia AXIS IP Utility lub AXIS Device Manager Extend. Obie aplikacje są darmowe i można je pobrać ze strony *axis.com/support*.

Więcej informacji na temat wykrywania i przydzielania adresów IP znajduje się w dokumencie *Jak przydzielić adres IP i uzyskać dostęp do urządzenia*.

Obsługiwane przeglądarki

Urządzenie obsługuje następujące przeglądarki:

	Chrome™	Firefox®	Edge™	Safari®
Windows®	zalecenie	zalecenie	✓	
macOS®	zalecenie	zalecenie	✓	✓
Linux®	zalecenie	zalecenie	✓	
Inne systemy operacyjne	✓	✓	✓	✓*

** Aby korzystać z interfejsu WWW AXIS OS w systemie iOS 15 lub iPadOS 15, przejdź do menu **Settings (Ustawienia) > Safari > Advanced (Zaawansowane) > Experimental Features (Funkcje eksperymentalne)** i wyłącz NSURLSession Websocket.*

Więcej informacji na temat zalecanych przeglądarek można znaleźć na stronie *AXIS OS Portal*.

Otwórz interfejs WWW urządzenia

1. Otwórz przeglądarkę i wpisz adres IP lub nazwę hosta urządzenia Axis.

   Jeśli nie znasz adresu IP, użyj narzędzia AXIS IP Utility lub AXIS Device Manager Extend, aby zlokalizować urządzenie w sieci.

2. Wprowadź nazwę użytkownika i hasło. Jeśli korzystasz z urządzenia po raz pierwszy, musisz utworzyć konto administratora. Patrz *Utwórz konto administratora na stronie 3*.

Opisy wszystkich elementów sterowania i opcji w interfejsie WWW urządzenia można znaleźć tutaj: *Interfejs WWW na stronie 12*.

Utwórz konto administratora

Przy pierwszym logowaniu do urządzenia należy utworzyć konto administratora.

1. Wprowadź nazwę użytkownika.
2. Wprowadź hasło. Patrz *Bezpieczne hasła na stronie 4*.
3. Wprowadź ponownie hasło.
4. Zaakceptuj umowę licencyjną.
5. Kliknij kolejno opcje **Add account (Dodaj konto)**.

Ważne

W urządzeniu nie ma konta domyślnego. Jeśli nastąpi utrata hasła do konta administratora, należy zresetować urządzenie. Patrz *Twarde resetowanie rejestratora na stronie 10*.

Bezpieczne hasła

Ważne

Urządzenia Axis wysyłają wstępnie ustawione hasło przez sieć jako zwykły tekst. Aby chronić urządzenie po pierwszym zalogowaniu, skonfiguruj bezpieczne i szyfrowane połączenie HTTPS, a następnie zmień hasło.

Hasło urządzenia stanowi podstawową ochronę danych i usług. Urządzenia Axis nie narzucają zasad haseł, ponieważ mogą być one używane w różnych typach instalacji.

Aby chronić dane, zalecamy:

- Używanie haseł o długości co najmniej ośmiu znaków, najlepiej utworzonego automatycznym generatorem haseł.
- Nieujawnianie haseł.
- Regularną zmianę haseł co najmniej raz na rok.

Sprawdzanie braku zmian w oprogramowaniu urządzenia

Aby upewnić się, że w urządzeniu zainstalowano oryginalny system AXIS OS lub aby odzyskać kontrolę nad urządzeniem w razie ataku:

1. Przywróć domyślne ustawienia fabryczne. Patrz *Twarde resetowanie rejestratora na stronie 10*.

   Po zresetowaniu opcja bezpiecznego uruchamiania gwarantuje bezpieczeństwo urządzenia.

2. Skonfiguruj i zainstaluj urządzenie.

Omówienie interfejsu WWW

Ten film przybliża najważniejsze elementy i schemat działania interfejsu WWW urządzenia.

Interfejs WWW urządzenia Axis

Rozpocznij

Uwaga

Podczas konfiguracji systemu wymagany jest dostęp do Internetu.

1. *Rejestrowanie konta My Axis na stronie 5*
2. *Instalacja sprzętu na stronie 5*
3. *Instalacja aplikacji na komputer na stronie 5*
4. *Utwórz lokalizację na stronie 6*
5. *Instalacja aplikacji mobilnej na stronie 6*

Rozpocznij

Po zakończeniu instalacji:

- wszystkie urządzenia Axis w systemie będą miały najnowsze oprogramowanie sprzętowe.
- Wszystkie urządzenia będą chronione hasłami.
- Będzie aktywna funkcja nagrywania z ustawieniami domyślnymi.
- Będzie możliwe korzystanie z dostępu zdalnego.

Rejestrowanie konta My Axis

Zarejestruj konto **MyAxis** na stronie *axis.com/my-axis/login*.

Aby zwiększyć bezpieczeństwo konta My Axis, włącz uwierzytelnianie wieloskładnikowe (MFA). MFA to system bezpieczeństwa, który wnosi kolejną warstwę weryfikacji w celu zapewnienia tożsamości użytkownika.

Aby włączyć uwierzytelnianie MFA:

1. Przejdź do strony *axis.com/my-axis/login*.
2. Zaloguj się, używając poświadczeń konta **My Axis**.
3. Przejdź do strony  i kliknij opcję **Account settings (Ustawienia konta)**.
4. Kliknij opcję **Security settings (Ustawienia zabezpieczeń)**
5. Kliknij opcję **Handle your 2-factor authentication (Obsługuj uwierzytelnianie dwuskładnikowe)**.
6. Wprowadź poświadczenia dostępu do konta w serwisie **My Axis**.
7. Wybierz metodę uwierzytelniania **Authenticator App (TOTP) (Aplikacja uwierzytelniająca (TOTP))** lub **Email (E-mail)** i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Instalacja sprzętu

1. Zainstaluj kamery.
2. Połącz rejestrator z siecią za pośrednictwem portu LAN.
3. Połącz kamery z wbudowanym przełącznikiem PoE rejestratora lub zewnętrznym przełącznikiem PoE.
4. Połącz komputer z tą samą siecią, z którą jest połączony rejestrator.
5. Podłącz zasilacz do rejestratora.

Ważne

Najpierw należy podłączyć przewód zasilający do rejestratora, a następnie podłączyć przewód zasilający do gniazdka.

6. Zanim kontynuujesz, poczekaj kilka minut, aż rejestrator i kamery zostaną uruchomione.

⚠UWAGA

Rejestrator powinien znajdować się w miejscu dobrze wentylowanym, w którym jest odpowiednio dużo wolnej przestrzeni wokół niego, aby zapobiec jego przegrzaniu.

Instalacja aplikacji na komputer

1. Przejdź na stronę *axis.com/products/axis-camera-station-edge* i kliknij pozycję **Download (Pobierz)** w celu pobrania aplikacji dla systemu Windows.
2. Otwórz plik instalacyjny i postępuj zgodnie z instrukcjami asystenta konfiguracji.

3. Zaloguj się przy użyciu *konta My Axis*.

Utwórz lokalizację

Lokalizacja to jeden punkt wejścia do systemu dozoru, na przykład dla wszystkich kamer w sklepie. Można śledzić kilka lokalizacji za pośrednictwem jednego konta My Axis.

1. Włącz aplikację komputerową .
2. Zaloguj się przy użyciu *konta My Axis*.
3. Kliknij **Create new site (Utwórz nową lokalizację)** i nadaj nazwę lokalizacji.
4. Kliknij przycisk **Dalej**.
5. Wybierz urządzenia, które chcesz dodać do lokalizacji.
6. Kliknij przycisk **Dalej**.
7. Wybierz zasób.
8. Kliknij przycisk **Dalej**.
9. Na stronie **Ready to install (Gotowe do instalacji)** opcje **Offline mode (Tryb offline)** i **Upgrade firmware (Aktualizuj oprogramowanie sprzętowe)** są domyślnie wyłączone. Można je wyłączyć, jeśli nie chcesz używać trybu offline ani aktualizować urządzeń o najnowsze wersje oprogramowania sprzętowego.
10. Kliknij przycisk **Install (Instaluj)** i poczekaj, aż skonfiguruje urządzenia.

    Konfiguracja może potrwać kilka minut.

Instalacja aplikacji mobilnej

Aplikacja mobilna pozwala na dostęp do urządzeń i nagrań z dowolnego miejsca. Możesz również otrzymywać powiadomienia o wystąpieniu zdarzeń albo gdy ktoś dzwoni przez interkom.

System Android

Kliknij przycisk *Download (Pobierz)* lub zeskanuj poniższy QR Code®.

System iOS

Kliknij przycisk *Download (Pobierz)* lub zeskanuj poniższy QR Code.

Otwórz aplikację mobilną i zaloguj się, używając poświadczeń konta Axis.

Jeżeli nie masz konta My Axis, możesz je założyć, przechodząc na stronę *axis.com/my-axis*.

QRCode to zastrzeżony znak towarowy należący do Denso Wave Incorporated w Japonii i w innych krajach.

Rozpocznij korzystanie z aplikacji AXIS Camera Station

Dodawanie rejestratora

Uwaga

Po dodaniu rejestratora do nowego systemu AXIS Camera Station usuwa nagrania ze wszystkich poprzednich systemów.

1. Wybierz kolejno opcje **Configuration > Devices > Add devices (Konfiguracja > Urządzenia > Dodaj urządzenia)**.
2. Zaznacz rejestrator na liście i kliknij przycisk **Add (Dodaj)**. Jeżeli rejestratora nie ma na liście, poszukaj go ręcznie za pomocą opcji **Manual search (Wyszukiwanie ręczne)**.
3. Użyj ustawień domyślnych i kliknij przycisk **Dalej**.
4. Ustaw hasło szyfrujące pamięć masową. Kliknij przycisk **Dalej**. Hasło trzeba będzie podać w celu uzyskania dostępu do dysku twardego rejestratora poza aplikacją AXIS Camera Station oraz po przywróceniu fabrycznych ustawień rejestratora z interfejsu WWW urządzenia.
5. Wybierz kolejno opcje **Configuration > Devices > Other devices (Konfiguracja > Urządzenia > Inne urządzenia)** i sprawdź, czy rejestrator został dodany.
6. Wybierz kolejno opcje **Configuration > Storage > Management (Konfiguracja > Pamięć masowa > Zarządzanie)** i sprawdź, czy rejestrator został dodany do listy zasobów pamięci masowej.

Dodawanie urządzeń i wskazywanie rejestratora jako pamięci masowej nagrań

1. Wybierz kolejno opcje **Configuration > Devices > Add devices (Konfiguracja > Urządzenia > Dodaj urządzenia)**.
2. Zaznacz urządzenia na liście i kliknij przycisk **Add (Dodaj)**. Jeżeli urządzeń nie ma na liście, poszukaj ich ręcznie za pomocą opcji **Manual search (Wyszukiwanie ręczne)**.
3. Użyj ustawień domyślnych i kliknij przycisk **Dalej**.
4. Wybierz ręcznie rejestrator z listy rozwijanej **Recording storage (Pamięć masowa nagrywania)** i kliknij przycisk **Install (Zainstaluj)**.

Uwaga

W przypadku wybrania opcji **Automatic (Automatycznie)** rejestrator nie zostanie ustawiony jako pamięć masowa nagrań.

5. Wybierz kolejno opcje **Configuration > Storage > Selection (Konfiguracja > Zasób > Wybór)**. Kliknij urządzenia i sprawdź, czy rolę pamięci masowej nagrań pełni rejestrator.

Konfigurowanie nagrywania

1. Wybierz kolejno opcje **Configuration > Storage > Selection (Konfiguracja > Pamięć masowa > Wybór)** i zaznacz swoje urządzenie.
2. Skonfiguruj ustawienie **Czas przechowywania**.
   - Wybierz czas przechowywania **Bez ograniczeń**, aby nagrania pozostawały w pamięci masowej aż do jej zapełnienia.
   - Alternatywnie zaznacz opcję **Ograniczony** i ustaw maksymalną liczbę dni zachowywania nagrań.
3. Kliknij przycisk **Apply (Zastosuj)**.

Uwaga

Opcja Fallback recording (Zapis zawartości rezerwowej) jest domyślnie włączona, aby w razie utraty połączenia między aplikacją AXIS Camera Station a rejestratorem nagrania były zapisywane na rejestratorze. Zobacz *Fallback recording (Zapis zawartości rezerwowej)*.

Konfiguracja urządzenia

Przydziel moc

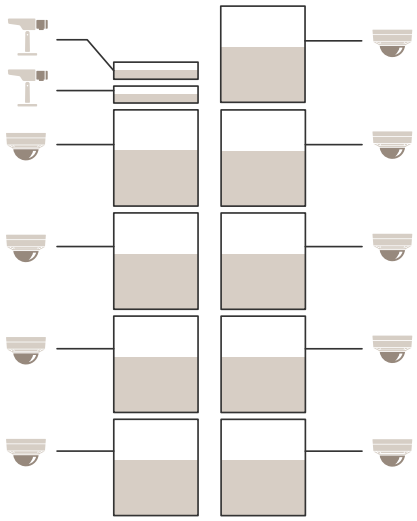
Rejestrator rezerwuje pewną ilość energii dla każdego portu. Łączna moc zarezerwowana nie może przekraczać łącznego budżetu zasilania. Port nie jest zasilany, jeśli rejestrator próbuje zarezerwować większą moc, niż jest dostępna. Dzięki temu można zapewnić, że wszystkie podłączone urządzenia będą zasilane.

Przykład:

W tym przykładzie:

- AXIS S3016 Recorder ma łączny budżet mocy 305 W.
- Urządzenie PoE klasy 3. Żąda mocy 15,5 W, ale faktycznie zużywa 7,5 W.
- Urządzenie PoE klasy 4. Żąda mocy 30 W, ale faktycznie zużywa 15 W.
- Zarezerwowana moc.
- Faktyczny pobór mocy.

Zarezerwowana moc



Faktyczny pobór mocy

- Każdy port rezerwuje moc zgodnie z klasą PoE urządzenia.
- Rejestrator może zasilać 9 urządzenia PoE klasy 4 i 3 urządzenia PoE klasy 2.
- Łączna zarezerwowana moc wynosi (9 x 30) + (2 x 15,5) = 301 W.
- Faktyczna moc wykorzystana wynosi (9 x 15) + (2 x 7,5) = 150 W.

Zmiana poziomu RAID

⚠UWAGA

Zmiana poziomu RAID powoduje ponowne sformatowanie systemu plików i wyczyszczenie dysków.

1. W interfejsie WWW urządzenia przejdź do menu **System > Storage (Zasób)**.
2. W menu **Tools (Narzędzia)** wybierz polecenie **Change RAID level (Zmień poziom RAID)** i kliknij **Use tool (Użyj narzędzia)**.
3. Wybierz poziom RAID i kliknij przycisk **Next (Dalej)**.
4. Wybierz polecenie **Encrypt the disk (Zaszyfruj dysk)** i wpisz hasło. Kliknij przycisk **Dalej**.
5. Kliknij **Tak**.
6. W prawym górnym rogu zostanie wyświetlony komunikat o stanie. Zanim zamkniesz tę stronę, poczekaj na zakończenie operacji i wyświetlenie komunikatu `RAID configured (Skonfigurowano RAID)`.

Wymień dysk twardy

Uwaga

W celu zapobiegania wyładowaniom elektrostatycznym w trakcie pracy przy komponentach systemu używaj maty elektrostatycznej i paska elektrostatycznego.

1. Odkręć śruby po lewej i prawej stronie osłony i zdejmij ją.
2. Znajdź uszkodzony dysk twardy (ze wskaźnikiem LED świecącym na czerwono).

   W przypadku awarii RAID wszystkie wskaźniki LED świecą na czerwono. Aby znaleźć uszkodzony dysk twardy, przejdź do interfejsu WWW urządzenia i otwórz menu **System > Storage > Hard drive status (System > Zasób > Stan dysku twardego)**.
3. Odkręć śrubę mocującą szyny dysku twardego (T10).
4. Wysuń szynę dysku twardego z wnęki.
5. Odkręć cztery śruby dysku twardego (T8).
6. Wyjmij dysk twardy z szyny.
7. Włóż nowy dysk twardy do szyny.
8. Przykręć cztery śruby dysku twardego.
9. Włóż i wsuń szynę dysku twardego do wnęki.
10. Przykręć śrubę szyny dysku twardego. Zaczekaj, aż dioda LED zaświeci się na zielono.
11. Zamocuj osłonę i przykręć śruby po lewej i prawej stronie.

Utwórz nową macierz RAID

⚠UWAGA

Nowa macierz RAID jest tworzona tylko w przypadku błędu RAID. Utworzenie nowej macierzy RAID powoduje usunięcie wszystkich danych z dysków twardych.

1. Wymień uszkodzone dyski twarde. Patrz *Wymień dysk twardy na stronie 10*.
2. Skonfiguruj macierz RAID. Patrz *Zmiana poziomu RAID na stronie 9*.
3. Skonfiguruj nagrania w swoim VMS. Patrz *Rozpocznij na stronie 4* i *Rozpocznij korzystanie z aplikacji AXIS Camera Station na stronie 7*.

Twarde resetowanie rejestratora

Ważne

Gdy rejestrator jest włączony, należy go przesuwać bardzo ostrożnie. Gwałtowne ruchy lub wstrząsy mogą uszkodzić dysk twardy.

Uwaga

- Twardy reset spowoduje zresetowanie wszystkich ustawień, w tym adresu IP.
- Twardy reset nie powoduje usunięcia nagrań.

1. Wyłącz rejestrator:

   Naciśnij przycisk zasilania znajdujący się z przodu rejestratora i przytrzymaj przez 4–5 sekund, aż usłyszysz sygnał dźwiękowy.

2. Poczekaj na wyłączenie rejestratora, a następnie obróć go, aby uzyskać dostęp do przycisku kontrolnego.

3. Naciśnij i przytrzymaj przycisk kontrolny. Naciśnij i zwolnij przycisk zasilania, aby uruchomić rejestrator. Zwolnij przycisk kontrolny po 15–30 sekundach, kiedy wskaźnik LED zacznie migać na bursztynowo.

4. Ostrożnie odłóż rejestrator na miejsce.

5. Proces zostanie zakończony, gdy wskaźnik LED stanu zmieni kolor na zielony. Produkt zostanie zresetowany do domyślnych ustawień fabrycznych. Jeśli w sieci brak serwera DHCP, domyślny adres IP to `192.168.0.90`

6. Jeżeli dysk twardy jest zaszyfrowany, należy go zamontować ręcznie po zresetowaniu rejestratora:

   6.1 Przejdź do interfejsu WWW urządzenia.

   6.2 Przejdź do menu **System** > **Storage (Zasób)** i kliknij przycisk **Mount (Montaż)**.

   6.3 Wprowadź hasło użyte podczas szyfrowania dysku twardego.

Interfejs WWW

Aby przejść do interfejsu WWW urządzenia, wpisz adres IP urządzenia w przeglądarce internetowej.

Uwaga

Obsługa funkcji i ustawień opisanych w tym rozdziale różni się w zależności od urządzenia. Ikona wskazuje, że funkcja lub ustawienie są dostępne tylko w niektórych urządzeniach.

Wyświetl/ukryj menu główne. Wyświetl informacje o wersji. Uzyskaj dostęp do pomocy dotyczącej produktu. Zmień język. Ustaw jasny lub ciemny motyw. Menu użytkownika zawiera opcje:

- Informacje o zalogowanym użytkowniku.
- **Change account (Zmień konto)**: Wyloguj się z bieżącego konta i zaloguj się na nowe konto.
- **Log out (Wyloguj się)**: Wyloguj się z bieżącego konta.

Menu kontekstowe zawiera opcje:

- **Analytics data (Dane analityczne)**: Zaakceptuj, aby udostępniać nie osobiste dane przeglądarki.
- **Feedback (Opinia)**: Ta opcja pozwala wystawiać opinie, by pomagać nam w poprawianiu funkcjonalności produktów i usług.
- **Legal (Informacje prawne)**: Wyświetl informacje o plikach cookie i licencjach.
- **About (Informacje)**: Tutaj znajdziesz informacje o urządzeniu, w tym wersję systemu AXIS OS i numer seryjny.

Status

Informacje o urządzeniu

Tutaj znajdziesz informacje o urządzeniu, w tym wersję systemu AXIS OS i numer seryjny.

Upgrade AXIS OS (Aktualizacja AXIS OS): umożliwia zaktualizowanie oprogramowania urządzenia. Ta opcja pozwala przejść do strony Maintenance (Konserwacja), gdzie można wykonać aktualizację.

Stan synchronizacji czasu

Pokazuje informacje o synchronizacji z usługą NTP, w tym czy urządzenie jest zsynchronizowane z serwerem NTP oraz czas pozostały czas do następnej synchronizacji.

NTP settings (Ustawienia NTP): umożliwia wyświetlenie i zaktualizowanie ustawień NTP. Ta opcja pozwala przejść do strony **Time and location (Czas i lokalizacja)**, gdzie można zmienić ustawienia usługi NTP.

Bezpieczeństwo

Pokazuje, jakiego rodzaju dostęp do urządzenia jest aktywny, które protokoły szyfrowania są używane oraz, czy dozwolone jest korzystanie z niepodpisanych aplikacji. Zalecane ustawienia bazują na przewodniku po zabezpieczeniach systemu operacyjnego AXIS.

Hardening guide (Przewodnik po zabezpieczeniach): Kliknięcie spowoduje przejście do *przewodnika po zabezpieczeniach systemu operacyjnego AXIS OS*, gdzie można się dowiedzieć więcej o stosowaniu najlepszych praktyk cyberbezpieczeństwa.

Porty sieciowe

Wskazuje stan portów sieciowych i informacje o zasilaniu, w tym o przydzielonej mocy i całkowitym zużyciu PoE. **Network ports settings (Ustawienia portów sieciowych)**: Kliknij tę opcję, aby przejść do strony Network ports (Porty sieciowe), gdzie można zmienić ustawienia.

Przechowywanie

Wskazuje status zasobu wraz z informacjami, takimi jak wolna przestrzeń i temperatura dysku. **Storage settings (Ustawienia zasobu)**: Kliknij, aby przejść do strony Onboard storage (Zasób pokładowy), gdzie można zmienić ustawienia.

Podłączone klienty

Pokazuje liczbę połączeń i połączonych klientów.

View details (Wyświetl szczegóły): Wyświetla i aktualizuje listę połączonych klientów. Na liście widać adres IP, protokół, port, stan i PID/proces każdego połączenia.

Trwające zapisy

Ta opcja wyświetla trwające nagrania i zasób pamięci, w którym mają być zapisane.

Nagrania: pozwala wyświetlić trwające i przefiltrowane nagrania oraz ich źródła. Więcej informacji: *Nagrania na stronie 13*

Pokazuje lokalizację zapisu nagrania w zasobie.

Nagrania

Odtwórz nagranie. Zatrzymaj odtwarzanie nagrania. Wyświetl lub ukryj informacje i opcje nagrania.**Set export range (Ustaw zakres eksportu)**: Jeżeli chcesz wyeksportować tylko część nagrania, określ zakres czasu.**Encrypt (Szyfruj)**: ta opcja pozwala skonfigurować hasło do eksportowanych nagrań. Podanie ustawionego hasła będzie konieczne do otworzenia eksportowanego pliku. Kliknij, aby usunąć nagranie.**Export (Eksportuj)**: pozwala wyeksportować całe nagranie lub jego fragment.

Kliknij, aby filtrować nagrania.**From (Od)**: Pokazuje nagrania wykonane po określonym momencie w czasie.**To (Do)**: Pokazuje nagrania wykonane przed określonym momentem w czasie.**Source (Źródło)** : Pokazuje nagrania z podziałem na źródła. Źródło odnosi się do czujnika.**Event (Zdarzenie)**: Pokazuje nagrania z podziałem na zdarzenia.**Pamięć masowa**: Pokazuje nagrania z podziałem na typy zasobów.

Aplikacje

Add app (Dodaj aplikację): umożliwia zainstalowanie nowej aplikacji.**Find more apps (Znajdź więcej aplikacji)**: pozwala znaleźć więcej aplikacji do zainstalowania. Nastąpi przekierowanie na stronę z opisem aplikacji Axis.**Allow unsigned apps (Zezwalaj na niepodpisane aplikacje)** : włączenie tej opcji umożliwi instalowanie niepodpisanych aplikacji.**Allow root-privileged apps (Zezwalaj na aplikacje z uprawnieniami roota)** : włączenie tej opcji umożliwi aplikacjom z uprawnieniami roota pełny dostęp do urządzenia. Wyświetl aktualizacje zabezpieczeń w aplikacjach AXIS OS i ACAP.

Uwaga

Korzystanie z kilku aplikacji jednocześnie może wpływać na wydajność urządzenia.

Aby włączyć lub wyłączyć aplikację, użyj przełącznika znajdującego się obok jej nazwy.**Open (Otwórz)**: umożliwia uzyskanie dostępu do ustawień aplikacji. Dostępne ustawienia zależą od aplikacji. W niektórych aplikacjach nie ma żadnych ustawień.
Menu kontekstowe może zawierać jedną lub kilka z następujących opcji:

- **Open-source license (Licencja open source)**: pozwala wyświetlić informacje o licencjach open source używanych w aplikacji.
- **App log (Dziennik aplikacji)**: pozwala wyświetlić dziennik zdarzeń aplikacji. Dziennik jest pomocny podczas kontaktowania się z pomocą techniczną.
- **Activate license with a key (Aktywuj licencję kluczem)**: Jeżeli aplikacja wymaga licencji, konieczne jest jej aktywowanie. Z tej opcji należy korzystać, jeżeli urządzenie nie ma dostępu do Internetu.
  Jeśli nie masz klucza licencji, przejdź na stronę *axis.com/products/analytics*. Do wygenerowania klucza potrzebny będzie kod licencyjny oraz numer seryjny produktu Axis.
- **Activate license automatically (Aktywuj licencję automatycznie)**: Jeżeli aplikacja wymaga licencji, konieczne jest jej aktywowanie. Z tej opcji należy korzystać, jeżeli urządzenie ma dostęp do Internetu. Do aktywowania licencji konieczny jest kod.
- **Deactivate the license (Dezaktywuj licencję)**: Aby zastąpić obecną licencję inną licencją, np. w przypadku przejścia z wersji próbnej na pełną, musisz wyłączyć obecną licencję. Jeśli dezaktywujesz licencję, zostanie ona również usunięta z urządzenia.
- **Ustawienia**: Ta opcja umożliwia konfigurowanie parametrów.
- **Usuń**: Ta opcja powoduje trwałe usunięcie aplikacji z urządzenia. Jeśli najpierw nie dezaktywujesz licencji, pozostanie ona aktywna.

System

Czas i lokalizacja

Data i godzina

Format czasu zależy od ustawień językowych przeglądarki internetowej.

Uwaga

Zalecamy zsynchronizowanie daty i godziny urządzenia z serwerem NTP.

Synchronization (Synchronizacja): pozwala wybrać opcję synchronizacji daty i godziny urządzenia.

- **Automatyczna data i godzina (ręczne serwery NTS KE)**: Synchronizacja z serwerami bezpiecznych kluczy NTP podłączonym do serwera DHCP.
  - **Ręczne serwery NTS KE**: Opcja ta umożliwia wprowadzenie adresu IP jednego lub dwóch serwerów NTP. W przypadku używania dwóch serwerów NTP urządzenie jest zsynchronizowane i dostosowuje czas według danych wejściowych z obu serwerów.
  - **Max NTP poll time (Maks. czas zapytania NTP)**: Wybierz maksymalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.
  - **Min NTP poll time (Min czas zapytania NTP)**: Wybierz minimalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.
- **Automatyczna data i godzina (serwery NTP z protokołem DHCP)**: Synchronizacja z serwerami NTP podłączonymi do serwera DHCP.
  - **Zapasowe serwery NTP**: Wprowadź adres IP jednego lub dwóch serwerów zapasowych.
  - **Max NTP poll time (Maks. czas zapytania NTP)**: Wybierz maksymalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.
  - **Min NTP poll time (Min czas zapytania NTP)**: Wybierz minimalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.
- **Automatyczna data i godzina (ręczne serwery NTP)**: Opcja ta umożliwia synchronizowanie z wybranymi serwerami NTP.
  - **Ręczne serwery NTP**: Opcja ta umożliwia wprowadzenie adresu IP jednego lub dwóch serwerów NTP. W przypadku używania dwóch serwerów NTP urządzenie jest zsynchronizowane i dostosowuje czas według danych wejściowych z obu serwerów.
  - **Max NTP poll time (Maks. czas zapytania NTP)**: Wybierz maksymalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.

- **Min NTP poll time (Min czas zapytania NTP)**: Wybierz minimalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.

- **Custom date and time (Niestandardowa data i godzina)**: Ustaw datę i godzinę ręcznie. Kliknij polecenie **Get from system (Pobierz z systemu)** w celu pobrania ustawień daty i godziny z komputera lub urządzenia przenośnego.

Strefa czasowa: Wybierz strefę czasową. Godzina zostanie automatycznie dostosowana względem czasu letniego i standardowego.

- **DHCP**: Stosuje strefę czasową serwera DHCP. Aby można było wybrać tę opcję, urządzenie musi być połączone z serwerem DHCP.
- **Manual (Ręcznie)**: Wybierz strefę czasową z listy rozwijanej.

Uwaga

System używa ustawień daty i godziny we wszystkich nagraniach, dziennikach i ustawieniach systemowych.

Sieć

IPv4

Przypisz automatycznie IPv4: wybierz, aby router sieciowy automatycznie przypisywał adres IP do urządzenia. Zalecamy korzystanie z funkcji automatycznego przydzielania adresu IP (DHCP) dla większości sieci.**Adres IP**: wprowadź unikatowy adres IP dla urządzenia. Statyczne adresy IP można przydzielać losowo w sieciach izolowanych, pod warunkiem że adresy są unikatowe. Aby uniknąć występowania konfliktów, zalecamy kontakt z administratorem sieci przed przypisaniem statycznego adresu IP.**Maska podsieci**: Otwórz maskę podsieci, aby określić adresy w sieci lokalnej. Wszystkie adresy poza siecią lokalną przechodzą przez router.**Router**: wprowadź adres IP domyślnego routera (bramki) używanego do łączenia z urządzeniami należącymi do innych sieci i segmentów sieci.**Fallback to static IP address if DHCP isn't available (Jeśli DHCP jest niedostępny, zostanie ono skierowane do statycznego adresu IP)**: Wybierz, czy chcesz dodać statyczny adres IP, który ma być używany jako rezerwa, jeśli usługa DHCP jest niedostępna i nie można automatycznie przypisać adresu IP.

Uwaga

Jeśli protokół DHCP jest niedostępny, a urządzenie korzysta z adresu rezerwowego dla adresu statycznego, adres statyczny jest skonfigurowany w zakresie ograniczonym.

IPv6

Przypisz IPv6 automatycznie: Włącz IPv6, aby router sieciowy automatycznie przypisywał adres IP do urządzenia.

Nazwa hosta

Przypisz automatycznie nazwę hosta: Wybierz, aby router sieciowy automatycznie przypisywał nazwę hosta do urządzenia.**Nazwa hosta**: Wprowadź ręcznie nazwę hosta, aby zapewnić alternatywny dostęp do urządzenia. W raporcie serwera i dzienniku systemowym jest używana nazwa hosta. Używaj tylko dozwolonych znaków: A-Z, a-z, 0-9 i -.**Włącz aktualizacje dynamiczne DNS**: Zezwól urządzeniu na automatyczną aktualizację rekordów serwera nazw domen, gdy zmieni się jego adres IP.**Register DNS name (Zarejestruj nazwę DNS)**: Wprowadź unikatową nazwę domeny, która wskazuje na adres IP urządzenia. Używaj tylko dozwolonych znaków: A-Z, a-z, 0-9 i -.**TTL**: Ustawienie TTL (Time to Live) określa, jak długo rekord DNS pozostaje ważny, zanim trzeba go zaktualizować.

Serwery DNS

Przypisz automatycznie DNS: Wybierz ustawienie, aby serwer DHCP automatycznie przypisywał domeny wyszukiwania i adresy serwerów DNS do urządzenia. Zalecamy korzystanie z funkcji automatycznego przydzielania adresów DNS (DHCP) dla większości sieci.**Przeszukaj domeny**: jeżeli używasz nazwy hosta, która nie jest w pełni kwalifikowana, kliknij **Add search domain (Dodaj domenę wyszukiwania)** i wprowadź domenę, w której ma być wyszukiwana nazwa hosta używana przez urządzenie.**Serwery DNS**: kliknij polecenie **Add DNS server (Dodaj serwer DNS)** i wprowadź adres IP podstawowego serwera DNS. Powoduje to przełożenie nazw hostów na adresy IP w sieci.

Protokoły wykrywania sieci

Bonjour®: Włącz, aby umożliwić automatyczne wykrywanie urządzeń w sieci.**Nazwa Bonjour**: wprowadź przyjazną nazwę, która będzie widoczna w sieci. Nazwa domyślna składa się z nazwy urządzenia i jego adresu MAC.**UPnP**®: Włącz, aby umożliwić automatyczne wykrywanie urządzeń w sieci.**Nazwa UPnP**: wprowadź przyjazną nazwę, która będzie widoczna w sieci. Nazwa domyślna składa się z nazwy urządzenia i jego adresu MAC.**WS-Discovery**: Włącz, aby umożliwić automatyczne wykrywanie urządzeń w sieci.**LLDP and CDP (LLDP i CDP)**: Włącz, aby umożliwić automatyczne wykrywanie urządzeń w sieci. Wyłączenie funkcji LLDP and CDP może wpływać na negocjowanie zasilania z PoE. Aby rozwiązać ewentualne problemy negocjowania zasilania z PoE, należy skonfigurować przełącznik PoE tylko do sprzętowej negocjacji zasilania PoE.

Globalne serwery proxy

Http proxy (Serwer proxy HTTP): Określ hosta lub adres IP globalnego serwera proxy, używając dozwolonego formatu.**Https proxy (Serwer proxy HTTPS)**: Określ hosta lub adres IP globalnego serwera proxy, używając dozwolonego formatu.
Dozwolone formaty serwerów proxy HTTP i HTTPS:

- **http(s)://host:port**
- **http(s)://użytkownik@host:port**
- **http(s)://użytkownik:pass@host:port**

Uwaga

Uruchom urządzenie ponownie, aby zastosować ustawienia globalnych serwerów proxy.

No proxy (Brak serwera proxy): Użyj opcji **No proxy (Brak serwera proxy)**, aby pominąć globalne serwery proxy. Wprowadź jedną z opcji na liście lub kilka opcji rozdzielonych przecinkami:

- Pozostaw puste
- Określ adres IP
- Określ adres IP w formacie CIDR
- Określ nazwę domeny, na przykład: **www.<nazwa domeny>.com**
- Określ wszystkie poddomeny w określonej domenie, na przykład **.<nazwa domeny>.com**

One-click cloud connection (Łączenie w chmurze jednym kliknięciem)

Usługa One-Click Cloud Connect (O3C) w połączeniu z systemem AVHS zapewnia łatwe i bezpieczne połączenie z internetem w celu uzyskania dostępu do obrazów wideo w czasie rzeczywistym oraz zarejestrowanych obrazów z dowolnej lokalizacji. Więcej informacji: *axis.com/end-to-end-solutions/hosted-services*.

Allow O3C (Zezwalaj na O3C):

- **Jednym kliknięciem**: Jest to domyślne ustawienie. Naciśnij i przytrzymaj przycisk Control na urządzeniu, aby połączyć się z usługą O3C przez Internet. Urządzenie należy zarejestrować w serwisie O3C w ciągu 24 godzin od naciśnięcia przycisku kontrolnego. W przeciwnym razie urządzenie zakończy połączenie z usługą O3C. Po zarejestrowaniu urządzenia opcja **Always (Zawsze)** jest włączona, a urządzenie zostaje połączone z usługą O3C.
- **Zawsze**: Urządzenie stale próbuje połączyć się z usługą O3C przez Internet. Po zarejestrowaniu urządzenie zostaje połączone z usługą O3C. Opcji tej należy używać wtedy, gdy przycisk kontrolny na urządzeniu jest niedostępny.
- **Nie**: wyłącza usługę O3C.

Proxy settings (Ustawienia proxy): W razie potrzeby należy wprowadzić ustawienia proxy, aby połączyć się z serwerem proxy.**Host**: Wprowadź adres serwera proxy.**Port**: wprowadź numer portu służącego do uzyskania dostępu.**Login** i **Hasło**: W razie potrzeby wprowadź nazwę użytkownika i hasło do serwera proxy.**Authentication method (Metoda uwierzytelniania)**:

- **Zwykła**: Ta metoda jest najbardziej zgodnym schematem uwierzytelniania HTTP. Jest ona mniej bezpieczna niż metoda **Digest (Szyfrowanie)**, ponieważ nazwa użytkownika i hasło są wysyłane do serwera w postaci niezaszyfrowanej.
- **Szyfrowanie**: ta metoda jest bezpieczniejsza, ponieważ zawsze przesyła hasło w sieci w formie zaszyfrowanej.
- **Automatycznie**: ta opcja umożliwia urządzeniu wybór metody uwierzytelniania w zależności od obsługiwanych metod. Priorytet ma metoda **Szyfrowanie**; w dalszej kolejności stosowana jest metoda **Zwykła**.

Owner authentication key (OAK) (Klucz uwierzytelniania właściciela (OAK)): Kliknij **Get key (Uzyskaj klucz)**, aby pobrać klucz uwierzytelniania właściciela. Warunkiem jest podłączone urządzenia do Internetu bez użycia zapory lub serwera proxy.

SNMP

Protokół zarządzania urządzeniami sieciowymi Simple Network Management Protocol (SNMP) umożliwia zdalne zarządzanie urządzeniami sieciowymi.

SNMP: Wybierz wersję SNMP.

- **v1 and v2c (v1 i v2c)**:
  - **Read community (Społeczność odczytu)**: wprowadź nazwę społeczności, która ma dostęp tylko do odczytu do wszystkich obsługiwanych obiektów SNMP. Wartość domyślna to **publiczna**.
  - **Write community (Społeczność zapisu)**: wprowadź nazwę społeczności, która ma dostęp do odczytu/zapisu do wszystkich obsługiwanych obiektów SNMP (poza obiektami tylko do odczytu). Wartość domyślna to **zapis**.
  - **Activate traps (Uaktywnij pułapki)**: włącz, aby uaktywnić raportowanie pułapek. Urządzenie wykorzystuje pułapki do wysyłania do systemu zarządzania komunikatów o ważnych zdarzeniach lub zmianach stanu. W interfejsie WWW urządzenia można skonfigurować pułapki dla SNMP v1 i v2c. Pułapki są automatycznie wyłączane w przypadku przejścia na SNMP v3 lub wyłączenia SNMP. Jeśli używasz SNMP v3, możesz skonfigurować pułapki za pomocą aplikacji do zarządzania SNMP v3.
  - **Trap address (Adres pułapki)**: Wprowadzić adres IP lub nazwę hosta serwera zarządzania.
  - **Trap community (Społeczność pułapki)**: Wprowadź nazwę społeczności używanej, gdy urządzenie wysyła komunikat pułapki do systemu zarządzającego.
  - **Traps (Pułapki)**:
  - **Cold start (Zimny rozruch)**: wysyła komunikat pułapkę po uruchomieniu urządzenia.
  - **Ciepły rozruch**: wysyła komunikat pułapkę w przypadku zmiany ustawienia SNMP.
  - **Link up (Łącze w górę)**: wysyła komunikat pułapkę po zmianie łącza w górę.
  - **Niepowodzenie uwierzytelniania**: wysyła komunikat pułapkę po niepowodzeniu próby uwierzytelnienia.

Uwaga

Wszystkie pułapki Axis Video MIB są włączone po włączeniu pułapek SNMP v1 i v2c. Więcej informacji: *AXIS OS Portal > SNMP*.

- **v3**: SNMP v3 to bezpieczniejsza wersja, zapewniająca szyfrowanie i bezpieczne hasła. Aby używać SNMP v3, zalecane jest włączenie protokołu HTTPS, który posłuży do przesłania hasła. Zapobiega to również dostępowi osób nieupoważnionych do niezaszyfrowanych pułapek SNMP v1 i v2c. Jeśli używasz SNMP v3, możesz skonfigurować pułapki za pomocą aplikacji do zarządzania SNMP v3.
  - **Password for the account "initial" (Hasło do konta „wstępnego")**: wprowadź hasło SNMP dla konta o nazwie „initial" (wstępne). Chociaż hasło może być wysłane bez aktywacji HTTPS, nie zalecamy tego. Hasło SNMP v3 można ustawić tylko raz i najlepiej tylko po aktywacji HTTPS. Po ustawieniu hasła pole hasła nie jest już wyświetlane. Aby zresetować hasło, należy zresetować urządzenie do ustawień fabrycznych.

Porty sieciowe

Zasilanie przez sieć Ethernet

- **Przydzielona moc**: Liczba aktualnie przydzielonych watów (W).
- **Łączny pobór PoE**: Liczba zużytych watów (W).
- **PoE aktywne podczas ponownego uruchomienia rejestratora**: Włącz, aby zapewnić zasilanie podłączonych urządzeń podczas ponownego uruchamiania rejestratora.

Kliknij tę opcję, aby wyświetlić lub ukryć obraz portów.

- Kliknij port na obrazie, aby wyświetlić jego dane na liście portów.

Lista portów

- **Port**: Numer portu.
- **PoE**: Umożliwia włączanie i wyłączanie PoE dla portu.
- **Network (Sieć)**: Umożliwia włączanie i wyłączanie sieci dla portu.
- **Status (Stan)**: Wskazuje, do danego portu jest podłączone urządzenie.
- **Friendly name (Przyjazna nazwa)**: Przyjazną nazwę można ustawić w zakładce **Network settings (Ustawienia sieci)**. Domyślna nazwa to połączenie modelu i adresu sterownika multimedialnego MAC (Media Access Control) podłączonego urządzenia.
- **Pobór energii**: Liczba watów (W) faktycznie zużywanych i przydzielanych przez podłączone urządzenie.

Bezpieczeństwo

Certyfikaty

Certyfikaty służą do uwierzytelniania urządzeń w sieci. Urządzenie obsługuje dwa typy certyfikatów:

- **Certyfikaty serwera/klienta**
  Certyfikat serwera/klienta potwierdza numer urządzenia i może mieć własny podpis lub podpis jednostki certyfikującej (CA). Certyfikaty z własnym podpisem oferują ograniczoną ochronę i można je wykorzystywać do momentu uzyskania certyfikatu CA.
- **Certyfikaty CA**
  Certyfikaty CA mogą służyć do uwierzytelniania innych certyfikatów, na przykład tożsamości serwera uwierzytelniającego w przypadku połączenia urządzenia z siecią zabezpieczoną za pomocą IEEE 802.1X. Urządzenie ma kilka zainstalowanych wstępnie certyfikatów CA.

Obsługiwane są następujące formaty:

- Formaty certyfikatów: .PEM, .CER i .PFX
- Formaty kluczy prywatnych: PKCS#1 i PKCS#12

Ważne

W przypadku przywrócenia na urządzeniu ustawień fabrycznych wszystkie certyfikaty są usuwane. Wstępnie zainstalowane certyfikaty CA są instalowane ponownie.

Add certificate (Dodaj certyfikat) : Kliknij, aby dodać certyfikat.

- **More (Więcej)** : Wyświetlanie dodatkowych pól do wypełnienia lub wybrania.
- **Secure keystore (Bezpieczny magazyn kluczy)**: Wybierz tę opcję, aby używać funkcji **Secure element (Zabezpieczony element)** lub **Trusted Platform Module 2.0 (Moduł TPM 2.0)** do bezpiecznego przechowywania klucza prywatnego. Aby uzyskać więcej informacji na temat bezpiecznego magazynu kluczy, odwiedź stronę *help.axis.com/en-us/axis-os#cryptographic-support*.
- **Key type (Typ klucza)**: Aby zabezpieczyć certyfikat, wybierz domyślny algorytm szyfrowania lub inny z listy rozwijanej.

Menu kontekstowe zawiera opcje:

- **Dane certyfikatu**: Wyświetl właściwości zainstalowanego certyfikatu.
- **Delete certificate (Usuń certyfikat)**: Umożliwia usunięcie certyfikatu.
- **Create certificate signing request (Utwórz żądanie podpisania certyfikatu)**: Umożliwia utworzenie żądanie podpisania certyfikatu w celu przekazania go do urzędu rejestracyjnego i złożenia wniosku o wydanie certyfikatu tożsamości cyfrowej.

Secure keystore (Bezpieczny magazyn kluczy) :

- **Bezpieczny element (CC EAL6+)**: Wybierz, aby używać bezpiecznego elementu do bezpiecznego magazynu kluczy.
- **Moduł TPM 2.0 (CC EAL4+, FIPS 140-2 poziom 2)**: Wybierz, aby używać modułu TPM 2.0 do bezpiecznego magazynu kluczy.

Kontrola dostępu do sieci i szyfrowanie

IEEE 802.1xIEEE 802.1x to standard IEEE dla kontroli dostępu sieciowego opartej na portach, zapewniający bezpieczne uwierzytelnianie przewodowych i bezprzewodowych urządzeń sieciowych. IEEE 802.1x jest oparty na protokole EAP (Extensible Authentication Protocol).Aby uzyskać dostęp do sieci zabezpieczonej IEEE 802.1x, urządzenia sieciowe muszą dokonać uwierzytelnienia. Do uwierzytelnienia służy serwer, zazwyczaj RADIUS, taki jak FreeRADIUS i Microsoft Internet Authentication Server.**IEEE 802.1AE MACsec**IEEE 802.1AE MACsec jest standardem IEEE dotyczącym adresu MAC, który definiuje bezpołączeniową poufność i integralność danych dla protokołów niezależnych od dostępu do nośników.**Certyfikaty**W przypadku konfiguracji bez certyfikatu CA, sprawdzanie poprawności certyfikatów serwera jest wyłączone, a urządzenie próbuje uwierzytelnić się niezależnie od tego, do jakiej sieci jest podłączone.Podczas korzystania z certyfikatu w instalacjach firmy Axis urządzenie i serwer uwierzytelniający używają do uwierzytelniania certyfikatów cyfrowych z użyciem EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).Aby zezwolić urządzeniu na dostęp do sieci chronionej za pomocą certyfikatów, w urządzeniu musi być zainstalowany podpisany certyfikat klienta.**Authentication method (Metoda uwierzytelniania)**: Wybierz typ protokołu EAP na potrzeby uwierzytelniania.**Client certificate (Certyfikat klienta)**: wybierz certyfikat klienta, aby użyć IEEE 802.1x. Serwer uwierzytelniania używa certyfikatu do weryfikacji tożsamości klienta.**Certyfikaty CA**: wybierz certyfikaty CA w celu potwierdzania tożsamości serwera uwierzytelniającego. Jeśli nie wybrano żadnego certyfikatu, urządzenie próbuje uwierzytelnić się niezależnie od tego, do jakiej sieci jest podłączone.**EAP identity (Tożsamość EAP)**: wprowadź tożsamość użytkownika powiązaną z certyfikatem klienta.**EAPOL version (Wersja protokołu EAPOL)**: wybierz wersję EAPOL używaną w switchu sieciowym.**Use IEEE 802.1x (Użyj IEEE 802.1x)**: wybierz, aby użyć protokołu IEEE 802.1 x.Te ustawienia są dostępne wyłącznie w przypadku korzystania z uwierzytelniania za pomocą **IEEE 802.1x PEAP-MSCHAPv2**:

- **Hasło**: Wprowadź hasło do tożsamości użytkownika.
- **Peap version (Wersja Peap)**: wybierz wersję Peap używaną w switchu sieciowym.

- **Etykieta**: 1 pozwala używać szyfrowania EAP klienta; 2 pozwala używać szyfrowania PEAP klienta. Wybierz etykietę używaną przez przełącznik sieciowy podczas korzystania z wersji 1 protokołu Peap.

Te ustawienia są dostępne wyłącznie w przypadku uwierzytelniania za pomocą **IEEE 802.1ae MACsec (klucz CAK/PSK)**:

- **Nazwa klucza skojarzenia łączności umowy klucza**: Wprowadź nazwę skojarzenia łączności (CKN). Musi to być od 2 do 64 (podzielnych przez 2) znaków szesnastkowych. CKN musi być ręcznie skonfigurowany w skojarzeniu łączności i musi być zgodny na obu końcach łącza, aby początkowo włączyć MACsec.
- **Klucz skojarzenia łączności umowy klucza**: Wprowadź klucz skojarzenia łączności (CAK). Musi mieć 32 lub 64 znaki szesnastkowe. CAK musi być ręcznie skonfigurowany w skojarzeniu łączności i musi być zgodny na obu końcach łącza, aby początkowo włączyć MACsec.

Zapora

Activate (Aktywuj): Włącz zaporę sieciową.
Domyślne ustawienia zasad: Wybierz stan domyślny zapory.

- **Allow (Zezwalaj):** Zezwala na wszystkie połączenia z urządzeniem. Jest opcja domyślna.
- **Deny: (Odrzuć)** Odrzuca wszystkie połączenia z urządzeniem.

Aby wprowadzić wyjątki od domyślnych zasad, można utworzyć reguły, które zezwalają lub nie zezwalają na łączenie się z urządzeniem z określonych adresów, protokołów i portów.

- **Adres**: Wprowadź adres w formacie IPv4/IPv6 lub CIDR, w przypadku którego dostęp ma być dozwolony lub niedozwolony.
- **Protocol (Protokół)**: Wybierz protokół, w przypadku którego dostęp ma być dozwolony lub niedozwolony.
- **Port**: Wprowadź numer portu, w przypadku którego dostęp ma być dozwolony lub niedozwolony. Podaj numer portu od 1 do 65535.
- **Policy (Zasada)**: Wybierz zasadę dla reguły.

: Kliknij, aby utworzyć nową regułę.
Add rules: (Dodaj reguły) Kliknij tę opcję, aby dodać zdefiniowane reguły.

- **Time in seconds: (Czas w sekundach)** Pozwala ustawić limit czasu testowania reguł. Domyślny limit czasu to **300** sekund. Jeśli chcesz od razu aktywować reguły, ustaw czas **0** sekund.
- **Confirm rules (Potwierdzenie reguł):** Potwierdź reguły i ich limit czasowy. W przypadku ustawienia limitu czasu dłuższego niż 1 sekunda reguły będą aktywne przez ten czas. Jeśli ustawiono czas **0**, reguły będą aktywowane od razu.

Pending rules (Oczekujące reguły): Omówienie ostatnio testowanych reguł, które jeszcze nie zostały potwierdzone.

Uwaga

Reguły z limitem czasu są widoczne w obszarze **Active rules (Aktywne reguły)**, aż upłynie czas ustawiony w czasomierzu lub nastąpi ich potwierdzenie. Jeśli nie zostaną potwierdzone, po upłynięciu czasu ustawionego w czasomierzu, pojawią się w menu **Pending rules (Oczekujące reguły)**, i zostaną przywrócone wcześniejsze ustawienia zapory. Jeśli reguły zostaną potwierdzone, zastąpią one bieżące aktywne reguły.

Confirm rules (Potwierdzenie reguł): Kliknięcie tej opcji aktywuje oczekujące reguły.**Active rules (Aktywne reguły)**: Omówienie reguł obecnie stosowanych w urządzeniu. : Kliknięcie tej opcji pozwala usunąć aktywną regułę. : Kliknięcie tej opcji pozwala usunąć wszystkie oczekujące i aktywne reguły.

Niestandardowy podpisany certyfikat systemu AXIS OS

Do zainstalowania w urządzeniu oprogramowania testowego lub innego niestandardowego oprogramowania Axis konieczny jest niestandardowy podpisany certyfikat systemu AXIS OS. Certyfikat służy do sprawdzenia, czy oprogramowanie jest zatwierdzone zarówno przez właściciela urządzenia, jak i przez firmę Axis. Oprogramowanie działa tylko na określonym urządzeniu z niepowtarzalnym numerem seryjnym i identyfikatorem procesora. Niestandardowe podpisane certyfikaty systemu AXIS OS mogą być tworzone tylko przez firmę Axis, ponieważ Axis posiada klucze do ich podpisywania.**Zainstaluj**: Kliknij przycisk Install (Instaluj), aby zainstalować certyfikat. Certyfikat musi zostać zainstalowany przed zainstalowaniem oprogramowania. Menu kontekstowe zawiera opcje:

- **Delete certificate (Usuń certyfikat)**: Umożliwia usunięcie certyfikatu.

Konta

Konta

Add account (Dodaj konto): Kliknij, aby dodać nowe konto. Można dodać do 100 kont.**Account (Konto)**: Wprowadź niepowtarzalną nazwę konta.**Nowe hasło**: wprowadzić hasło do konta. Hasło musi mieć 1–64 znaki. Dozwolone są tylko możliwe do wydrukowania znaki ASCII (kod od 32 do 126), na przykład litery, cyfry, znaki interpunkcyjne i niektóre symbole.**Repeat password (Powtórz hasło)**: Wprowadź ponownie to samo hasło.**Privileges (Przywileje)**:

- **Administrator**: Ma nieograniczony dostęp do wszystkich ustawień. Administrator może tez dodawać, aktualizować i usuwać inne konta.
- **Operator**: Ma dostęp do wszystkich ustawień poza:
  - Wszystkie ustawienia **System**.
- **Viewer (Dozorca)**: Może:
  - Oglądać strumienie wideo i robić z nich migawki.
  - Oglądać i eksportować nagrania.
  - Korzystać z funkcji obracania, pochylania i zoomowania, jeśli ma dostęp do **konta PTZ**.

Menu kontekstowe zawiera opcje:**Update account (Zaktualizuj konto)**: Pozwala edytować właściwości konta.**Delete account (Usuń konto)**: Pozwala usunąć konto. Nie można usunąć konta root.

Konta SSH

Add SSH account (Dodaj konto SSH): Kliknij, aby dodać nowe konto SSH.

- **Restrict root access (Ogranicz dostęp do konta root)**: Włącz, aby ograniczyć funkcjonalność wymagającą dostępu root.
- **Enable SSH (Włącz SSH)**: Włącz, aby korzystać z usługi SSH.

Account (Konto): Wprowadź niepowtarzalną nazwę konta.**Nowe hasło**: wprowadzić hasło do konta. Hasło musi mieć 1–64 znaki. Dozwolone są tylko możliwe do wydrukowania znaki ASCII (kod od 32 do 126), na przykład litery, cyfry, znaki interpunkcyjne i niektóre symbole.**Repeat password (Powtórz hasło)**: Wprowadź ponownie to samo hasło.**Uwaga**: Wprowadź komentarz (opcjonalnie). Menu kontekstowe zawiera opcje:**Update SSH account (Zaktualizuj konto SSH)**: Pozwala edytować właściwości konta.**Delete SSH account (Usuń konto SSH)**: Pozwala usunąć konto. Nie można usunąć konta root.

Virtual host (Host wirtualny)

Add virtual host (Dodaj host wirtualny): kliknięcie tej opcji pozwala dodać nowego wirtualnego hosta.**Włączony**: zaznaczenie tej opcji spowoduje używanie tego wirtualnego hosta.**Server name (Nazwa serwera)**: w tym polu można wpisać nazwę serwera. Używaj tylko cyfr 0-9, liter A-Z i łącznika (-).**Port**: w tym polu należy podać port, z którym jest połączony serwer.**Type (Typ)**: pozwala wybrać typ poświadczenia, które ma być używane. Dostępne są opcje **Basic (Podstawowe)**, **Digest (Szyfrowane)** oraz **Open ID (Otwarte ID)**. Menu kontekstowe zawiera opcje:

- **Update (Aktualizuj)**: Zaktualizuj wirtualnego hosta.
- **Usuń**: Usuń wirtualnego hosta.

Disabled (Wyłączono): Serwer jest wyłączony.

Zdarzenia

Reguły

Reguła określa warunki wyzwalające w urządzeniu wykonywanie danej akcji. Na liście znajdują się wszystkie reguły skonfigurowane w produkcie.

Uwaga

Można utworzyć maksymalnie 256 reguł akcji.

Add a rule (Dodaj regułę): Utwórz regułę.**Nazwa**: Wprowadź nazwę reguły.**Wait between actions (Poczekaj między działaniami)**: Wprowadź minimalny czas (w formacie gg:mm:ss), jaki musi upłynąć między aktywacjami reguły. Ustawienie to jest przydatne, gdy reguła jest aktywowana na przykład warunkami trybów dziennego i nocnego, ponieważ zapobiega niepożądanemu uruchamianiu reguły przez niewielkie zmiany natężenia światła podczas wschodu i zachodu słońca.**Condition (Warunek)**: Wybierz warunek z listy. Dopiero po spełnieniu tego warunku urządzenie wykona akcję. Jeśli określono wiele warunków, to do wyzwolenia działania konieczne jest spełnienie wszystkich z nich. Informacje na temat konkretnych warunków można znaleźć w części *Get started with rules for events (Reguły dotyczące zdarzeń)*.**Use this condition as a trigger (Użyj tego warunku jako wyzwalacza)**: Zaznacz tę opcję, aby ten pierwszy warunek działał tylko jako wyzwalacz początkowy. Oznacza to, że po aktywacji reguła pozostanie czynna przez cały czas, gdy są spełniane wszystkie pozostałe warunki, bez względu na stan pierwszego warunku. Jeżeli nie zaznaczysz tej opcji, reguła będzie aktywna po spełnieniu wszystkich warunków.**Invert this condition (Odwróć ten warunek)**: Zaznacz tę opcję, jeśli warunek ma być przeciwieństwem dokonanego przez Ciebie wyboru. **Add a condition (Dodaj warunek)**: Kliknij, aby dodać kolejny warunek. **Action (Akcja)**: Wybierz akcję z listy i wprowadź jej wymagane informacje. Informacje na temat konkretnych akcji można znaleźć w części *Get started with rules for events (Reguły dotyczące zdarzeń)*.

Odbiorcy

W urządzeniu można skonfigurować powiadamianie odbiorców o zdarzeniach lub wysyłanie plików.

Uwaga

W przypadku skonfigurowania urządzenia do korzystania z protokołu FTP lub SFTP nie należy zmieniać ani usuwać unikatowego numeru sekwencyjnego dodawanego do nazw plików. Jeśli zostało to zrobione, można wysłać tylko jeden obraz na zdarzenie.

Na liście wyświetlani są wszyscy odbiorcy skonfigurowani dla produktu, a także informacje dotyczące ich konfiguracji.

Uwaga

Można utworzyć maksymalnie 20 odbiorców.

Add a recipient (Dodaj odbiorcę): Kliknij, aby dodać odbiorcę. **Nazwa**: Wprowadź nazwę odbiorcy.**Type (Typ)**: Wybierz z listy:

- FTP
  - **Host**: Wprowadź adres IP lub nazwę hosta serwera. W przypadku wprowadzenia nazwy hosta upewnij się, że w ustawieniu **System > Network > IPv4 and IPv6 (System > Sieć > IPv4 i IPv6)** podano serwer DNS.
  - **Port**: Wprowadź numer portu wykorzystywanego przez serwer FTP. Domyślny port to 21.
  - **Folder**: Wprowadź ścieżkę dostępu do katalogu, w którym mają być przechowywane pliki. Jeśli nie ma takiego katalogu na serwerze FTP, podczas wczytywania plików zostanie wyświetlony komunikat o błędzie.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.
  - **Use temporary file name (Użyj tymczasowej nazwy pliku)**: Wybierz tę opcję, aby wczytywać pliki z tymczasowymi, automatycznie generowanymi nazwami plików. Po zakończeniu wczytywania nazwy plików zostaną zmienione na docelowe. W przypadku przerwania/wstrzymania wczytywania plików nie zostaną one uszkodzone. Pliki tymczasowe nadal pozostaną na dysku. Dzięki temu będzie wiadomo, że wszystkie pliki o danej nazwie są prawidłowe.
  - **Use passive FTP (Użyj pasywnego FTP)**: W normalnych warunkach produkt po prostu wysyła żądanie otwarcia połączenia do serwera FTP. Urządzenie inicjuje przesyłanie danych na serwer docelowy i kontrolę serwera FTP. Jest to zazwyczaj konieczne w przypadku zapory ogniowej pomiędzy urządzeniem a serwerem FTP.
- HTTP
  - **URL**: Wprowadź adres sieciowy serwera HTTP oraz skrypt obsługujący żądanie. Na przykład: http://192.168.254.10/cgi-bin/notify.cgi.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.

- **Proxy**: Włącz tę opcję i wpisz wymagane informacje, jeżeli konieczne jest dodanie serwera proxy w celu połączenia w serwerem HTTP.

- HTTPS
  - **URL**: Wprowadź adres sieciowy serwera HTTPS oraz skrypt obsługujący żądanie. Na przykład: https://192.168.254.10/cgi-bin/notify.cgi.
  - **Validate server certificate (Potwierdź certyfikat serwera)**: Zaznacz tę opcję, aby sprawdzić certyfikat utworzony przez serwer HTTPS.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.
  - **Proxy**: Włącz tę opcję i wpisz wymagane informacje, jeżeli konieczne jest dodanie serwera proxy w celu połączenia w serwerem HTTPS.

- **Sieciowa pamięć masowa**
  Umożliwia dodanie takiego zasobu sieciowego, jak NAS (sieciowy zasób dyskowy), i wykorzystywanie go jako odbiorcy plików. Pliki zapisywane są w formacie Matroska (MKV).
  - **Host**: Wprowadź adres IP lub nazwę hosta serwera pamięci sieciowej.
  - **Udział**: Podaj nazwę współdzielonego udziału na serwerze hosta.
  - **Folder**: Wprowadź ścieżkę dostępu do katalogu, w którym mają być przechowywane pliki.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.

- SFTP
  - **Host**: Wprowadź adres IP lub nazwę hosta serwera. W przypadku wprowadzenia nazwy hosta upewnij się, że w ustawieniu **System > Network > IPv4 and IPv6 (System > Sieć > IPv4 i IPv6)** podano serwer DNS.
  - **Port**: Wprowadź numer portu wykorzystywanego przez serwer SFTP. Domyślny port to 22.
  - **Folder**: Wprowadź ścieżkę dostępu do katalogu, w którym mają być przechowywane pliki. Jeśli nie ma takiego katalogu na serwerze SFTP, podczas wczytywania plików zostanie wyświetlony komunikat o błędzie.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.
  - **SSH host public key type (Typ klucza publicznego hosta SSH) (MD5)**: Wprowadź odcisk cyfrowy klucza publicznego zdalnego hosta (ciąg 32 cyfr w szesnastkowym systemie liczbowym). Klient SFTP obsługuje serwery SFTP stosujące SSH-2 i typy klucza hosta RSA, DSA, ECDSA i ED25519. RSA jest preferowaną metodą podczas negocjacji; następnie wykorzystywane są metody ECDSA, ED25519 i DSA. Upewnij się, że wprowadzono prawidłowy klucz hosta MD5 używany przez serwer SFTP. Urządzenie Axis obsługuje klucze szyfrowania MD5 i SHA-256, ale my zalecamy używanie klucza SHA-256, ponieważ jest bezpieczniejszy niż MD5. Więcej informacji o konfigurowaniu serwera SFTP dla urządzenia Axis można znaleźć w *portalu poświęconym systemowi AXIS OS*.
  - **SSH host public key type (Typ klucza publicznego hosta SSH) (SHA256)**: Wprowadź odcisk cyfrowy klucza publicznego zdalnego hosta (ciąg 43 cyfr w systemie kodowania Base64). Klient SFTP obsługuje serwery SFTP stosujące SSH-2 i typy klucza hosta RSA, DSA, ECDSA i ED25519. RSA jest preferowaną metodą podczas negocjacji; następnie wykorzystywane są metody ECDSA, ED25519 i DSA. Upewnij się, że wprowadzono prawidłowy klucz hosta MD5 używany przez serwer SFTP. Urządzenie Axis obsługuje klucze szyfrowania MD5 i SHA-256, ale my zalecamy używanie klucza SHA-256, ponieważ jest bezpieczniejszy niż MD5. Więcej informacji o konfigurowaniu serwera SFTP dla urządzenia Axis można znaleźć w *portalu poświęconym systemowi AXIS OS*.
  - **Use temporary file name (Użyj tymczasowej nazwy pliku)**: Wybierz tę opcję, aby wczytywać pliki z tymczasowymi, automatycznie generowanymi nazwami plików. Po zakończeniu wczytywania nazwy plików zostaną zmienione na docelowe. W przypadku przerwania/wstrzymania wczytywania plików nie zostaną one uszkodzone. Pliki tymczasowe nadal pozostaną na dysku. Dzięki temu będzie wiadomo, że wszystkie pliki o danej nazwie są prawidłowe.

- **SIP or VMS (SIP lub VMS)** :
  SIP: Wybierz w celu nawiązania połączenia SIP.
  VMS: Wybierz w celu nawiązania połączenia VMS.
  - **From SIP account (Z konta SIP)**: Wybierz z listy.
  - **To SIP address (Na adres SIP)**: Wprowadź adres SIP.
  - **Test (Testuj)**: Kliknij, aby sprawdzić, czy ustawienia połączeń działają prawidłowo.
- **E-mail**

- **Wyślij wiadomość e-mail do**: Wprowadź adresy odbiorców. Aby wprowadzić wiele adresów e-mail, oddziel je przecinkami.
- **Wyślij e-mail przez**: Wprowadź adres serwera nadawcy.
- **Username (Nazwa użytkownika)**: Wprowadź nazwę użytkownika serwera poczty. Jeżeli serwer nie wymaga uwierzytelnienia, nie wypełniaj tego pola.
- **Hasło**: Wprowadź hasło dostępu do serwera poczty. Jeżeli serwer nie wymaga uwierzytelnienia, nie wypełniaj tego pola.
- **Email server (SMTP) (Serwer poczty e-mail (SMTP))**: Wprowadź nazwę serwera SMTP, na przykład smtp.gmail.com, smtp.mail.yahoo.com.
- **Port**: wprowadź numer portu serwera SMTP, używając wartości z zakresu 0–65535. Wartość domyślna to 587.
- **Szyfrowanie**: Aby używać szyfrowania, wybierz opcję SSL lub TLS.
- **Validate server certificate (Potwierdź certyfikat serwera)**: Jeżeli używasz szyfrowania, zaznacz tę opcję, aby weryfikować tożsamość urządzenia. Certyfikat może mieć własny podpis lub podpis jednostki certyfikującej (CA).
- **POP authentication (Uwierzytelnianie POP)**: Włącz tę opcję i wprowadź nazwę serwera POP, na przykład pop.gmail.com.

Uwaga

Niektórzy dostawcy usług poczty elektronicznej stosują filtry bezpieczeństwa, uniemożliwiające odbiór lub przeglądanie dużej liczby załączników, odbieranie wiadomości cyklicznych itp. Aby zapobiec zablokowaniu konta lub usunięciu wiadomości, należy sprawdzić regulamin zabezpieczeń dostawcy usług.

- **TCP**
  - **Host**: Wprowadź adres IP lub nazwę hosta serwera. W przypadku wprowadzenia nazwy hosta upewnij się, że w ustawieniu **System > Network > IPv4 and IPv6 (System > Sieć > IPv4 i IPv6)** podano serwer DNS.
  - **Port**: Wprowadź numer portu dostępowego serwera.

Test (Testuj): Kliknij, aby przetestować konfigurację. ⋮ Menu kontekstowe zawiera opcje:**View recipient (Pokaż odbiorcę)**: Kliknij, aby wyświetlić wszystkie dane odbiorcy.**Copy recipient (Kopiuj odbiorcę)**: Kliknij, aby skopiować odbiorcę. Po skopiowaniu odbiorcy można wprowadzić zmiany w nowym wpisie odbiorcy.**Delete recipient (Usuń odbiorcę)**: Kliknij, aby trwale usunąć odbiorcę.

Harmonogramy

Harmonogramów i zdarzeń jednorazowych można użyć jako warunków reguł. Na liście wyświetlane są wszystkie harmonogramy i zdarzenia jednorazowe skonfigurowane dla produktu, a także informacje dotyczące ich konfiguracji. + **Add schedule (Dodaj harmonogram)**: Kliknij, aby utworzyć harmonogram lub impuls.

Wyzwalacze ręczne

Wyzwalacz manualny służy do ręcznego wyzwalania reguły. Wyzwalacza manualnego można na przykład użyć do walidacji akcji podczas instalacji i konfiguracji produktu.

Przechowywanie

Pamięć pokładowa

RAID

- **Free (Wolne)**: Ilość wolnego miejsca na dysku.
- **Status (Stan)**: Czy dysk jest zainstalowany.
- **System plików**: System plików używany przez dysk.
- **Zaszyfrowane**: Czy dysk jest zaszyfrowany.
- **Temperatura**: Bieżąca temperatura sprzętu.
- **Overall heath test (Ogólny test stanu)**: Wynik kontroli kondycji dysku.
- **RAID level (Poziom RAID)**: Poziom RAID używany na potrzeby zasobu. Obsługiwane poziomy RAID: 0, 1, 5, 6, 10.
- **RAID status (Stan RAID)**: Status RAID zasobu. Możliwe są wartości **Online**, **Degraded (Obniżono)**, **Syncing (Synchronizacja)** i **Failed (Błąd)**.

Narzędzia

Uwaga

Po uruchomieniu poniższych narzędzi zaczekaj na zakończenie operacji, zanim zamkniesz stronę.

- **Check (Sprawdź)**: Sprawdza, czy urządzenie pamięci masowej jest wolne od błędów, i spróbuje je naprawić automatycznie.
- **Napraw**: Naprawia urządzenie pamięci masowej. Podczas naprawy zostaną wstrzymane aktywne nagrania. Naprawa urządzenia pamięci masowej może spowodować utratę danych.
- **Format (Formatuj)**: Usuń wszystkie zapisy i sformatuj urządzenie pamięci masowej. Wybierz system plików.
- **Encrypt (Szyfruj)**: Umożliwia zaszyfrowanie zapisanych danych. Wszystkie pliki w urządzeniu pamięci masowej zostaną wymazane.
- **Decrypt (Odszyfruj)**: Umożliwia odszyfrowanie zapisanych danych. Wszystkie pliki w urządzeniu pamięci masowej zostaną wymazane.
- **Change password (Zmień hasło)**: Zmień hasło szyfrowania dysków. Zmiana hasła nie zakłóca nagrywania.
- **Change RAID level (Zmiana poziomu RAID)**: Ta opcja umożliwia zmienienie poziom RAID dla zasobu.
- **Use tool (Użyj narzędzia)**: Kliknij tę opcję, aby uruchomić wybrane narzędzie.

Hard drive status (Wskaźnik LED stanu dysku twardego): Kliknij tę opcję, aby wyświetlić status, pojemność i nr seryjny dysku twardego.**Write protect (Zabezpieczenie przed zapisem)**: Włącz zabezpieczenie urządzenia pamięci masowej przed zapisem.

Dzienniki

Raporty i dzienniki

Raporty

- **Wyświetl raport serwera o urządzeniu**: Opcja ta pozwala wyświetlić informacje o stanie produktu w wyskakującym oknie. W raporcie o serwerze automatycznie umieszczany jest dziennik dostępu.
- **Download the device server report (Pobierz raport serwera o urządzeniu)**: Opcja ta powoduje utworzenie pliku ZIP, który zawiera pełny raport serwera w pliku tekstowym w formacie UTF–8 oraz migawkę bieżącego podglądu na żywo. Podczas kontaktowania się z pomocą techniczną zawsze dodawaj plik zip raportu serwera.
- **Download the crash report (Pobierz raport o awarii)**: Pobierz archiwum ze szczegółowymi informacjami o stanie serwera. Raport o awarii zawiera informacje znajdujące się w raporcie o serwerze oraz szczegółowe dane pomocne w usuwaniu błędów. W raporcie tym mogą się znajdować informacje poufne, np. ślady sieciowe. Wygenerowanie raportu może potrwać kilka minut.

Dzienniki

- **View the system log (Wyświetl dziennik systemu)**: Kliknij tutaj, aby wyświetlić informacje o zdarzeniach systemowych, takich jak uruchamianie urządzenia, ostrzeżenia i komunikaty krytyczne.
- **Wyświetl dziennik dostępu**: Kliknij tutaj, by wyświetlić wszystkie nieudane próby uzyskania dostępu do urządzenia, na przykład gdy użyto nieprawidłowego hasła logowania.

Zdalny dziennik systemu

Dziennik systemowy to standard rejestracji komunikatów. Umożliwia on oddzielenie oprogramowania, które generuje komunikaty, systemu przechowującego je i oprogramowania, które je raportuje i analizuje. Każdy komunikat jest oznaczany etykietą z kodem obiektu wskazującym typ oprogramowania, które wygenerowało komunikat, oraz przypisany poziom ważności.

Server (Serwer): Kliknij, aby dodać nowy serwer.**Host**: Wprowadź nazwę hosta lub adres IP serwera.**Format (Formatuj)**: Wybierz format komunikatu dziennika systemowego, który ma być używany.

- Axis
- RFC 3164
- RFC 5424

Protocol (Protokół): Wybierz protokołu, który ma być używany:

- UDP (port domyślny to 514)
- TCP (port domyślny to 601)
- TLS (port domyślny to 6514)

Port: Wpisywanie innego numeru portu w miejsce obecnego.**Severity (Ciężkość)**: Zdecyduj, które komunikaty będą wysyłane po wyzwoleniu.**CA certificate set (Certyfikat CA ustawiony)**: Umożliwia wyświetlenie aktualnych ustawień lub dodanie certyfikatu.

Konserwacja

Konserwacja

Restart (Uruchom ponownie): Uruchom ponownie urządzenie. Nie wpłynie to na żadne bieżące ustawienia. Uruchomione aplikacje zostaną ponownie uruchomione automatycznie.**Restore (Przywróć)**: Opcja ta umożliwia przywrócenie *większości* domyślnych ustawień fabrycznych. Następnie konieczne jest ponowne skonfigurowanie urządzeń i aplikacji, zainstalowanie aplikacji, które nie zostały wstępnie zainstalowane, a także ponowne utworzenie wszystkich zdarzeń i wstępnych ustawień.

Ważne

Operacja przywrócenia spowoduje, że będą zapisane tylko następujące ustawienia:

- protokół uruchamiania (DHCP lub stały adres),
- statyczny adres IP,
- Router domyślny
- Maska podsieci
- ustawienia 802.1X.
- Ustawienia O3C
- Adres IP serwera DNS

Ustawienia fabryczne: Przywróć *wszystkie* ustawienia do domyślnych wartości fabrycznych. Po zakończeniu tej operacji konieczne będzie zresetowanie adresu IP w celu uzyskania dostępu do urządzenia.

Uwaga

Wszystkie składniki oprogramowania urządzenia firmy Axis posiadają podpisy cyfrowe zapewniające, że na urządzeniu będzie instalowane wyłącznie zweryfikowane oprogramowanie. To dodatkowo zwiększa minimalny ogólny poziom cyberbezpieczeństwa urządzeń Axis. Więcej informacji znajduje się w oficjalnym dokumencie „Axis Edge Vault" dostępnym na *axis.com*.

Uaktualnianie systemu AXIS OS: Umożliwia uaktualnienie do nowej wersji AXIS OS. Nowe wersje mogą zawierać udoskonalenia działania i poprawki błędów oraz zupełnie nowe funkcje. Zalecamy, aby zawsze korzystać z najnowszej wersji systemu AXIS OS. Aby pobrać najnowsza wersję, odwiedź stronę *axis.com/support*.
Po uaktualnieniu masz do wyboru trzy opcje:

- **Standard upgrade (Aktualizacja standardowa)**: Umożliwia uaktualnienie do nowej wersji systemu AXIS OS.
- **Ustawienia fabryczne**: Umożliwia uaktualnienie i przywrócenie ustawień do domyślnych wartości fabrycznych. Jeżeli wybierzesz tę opcję, po uaktualnieniu nie będzie możliwości przywrócenia poprzedniej wersji systemu AXIS OS.
- **Autorollback (Automatyczne przywrócenie wersji)**: Uaktualnij i potwierdź uaktualnienie w ustawionym czasie. Jeżeli nie potwierdzisz, w urządzeniu zostanie przywrócona poprzednia wersja systemu AXIS OS.

Przywracanie systemu AXIS OS: Przywróć poprzednio zainstalowaną wersję systemu AXIS OS.

Rozwiązywanie problemów

Ping: Aby sprawdzić, czy określony adres jest osiągalny dla urządzenia, wprowadź nazwę lub adres IP hosta, do którego chcesz wysłać polecenie ping, i kliknij **Start (Uruchom)**.**Port check (Sprawdzenie portu)**: Aby zweryfikować łączność urządzenia z określonym adresem IP i portem TCP/UDP, wprowadź nazwę hosta lub adres IP i numer portu, które chcesz sprawdzić, a następnie kliknij **Start (Uruchom)**.**Ślad sieciowy**

Ważne

Plik śladu sieciowego może zawierać dane poufne, takie jak certyfikaty lub hasła.

Plik śladu sieciowego, rejestrujący aktywność w sieci, może pomóc w rozwiązywaniu problemów. **Trace time (Czas śledzenia)**: Wybierz czas trwania śledzenia w sekundach lub minutach i kliknij przycisk **Download (Pobierz)**.

Więcej informacji

Cyberbezpieczeństwo

Informacje na temat cyberbezpieczeństwa dotyczące poszczególnych produktów można znaleźć w opisie produktu na stronie Axis.com.

Aby uzyskać szczegółowe informacje na temat cyberbezpieczeństwa w systemie AXIS OS, zapoznaj się z *przewodnikiem po zabezpieczeniach systemu operacyjnego AXIS OS*.

Podpisany system operacyjny

Podpisany system operacyjny jest wdrażany przez dostawcę oprogramowania podpisującego obraz systemu AXIS OS za pomocą klucza prywatnego. Po dołączeniu podpisu do systemu operacyjnego urządzenie sprawdzi poprawność oprogramowania przed jego zainstalowaniem. Jeżeli urządzenie wykryje naruszenie integralności oprogramowania, aktualizacja systemu AXIS OS zostanie odrzucona.

Bezpieczny start

Bezpieczny start to proces składający się z nieprzerwanego łańcucha oprogramowania zweryfikowanego kryptograficznie, rozpoczynający się w pamięci niezmiennej (rozruchowej pamięci ROM). Dzięki wykorzystaniu podpisanego systemu operacyjnego bezpieczny rozruch gwarantuje uruchomienie urządzenia wyłącznie z autoryzowanym oprogramowaniem.

Axis Edge Vault

Axis Edge Vault to sprzętowa platforma cyberbezpieczeństwa chroniąca urządzenie Axis. Zawiera funkcje gwarantujące tożsamość i integralność urządzenia oraz ochronę poufnych informacji przed nieuprawnionym dostępem. Rozwiązanie to bazuje na mocnych podstawach zapewnianych przez kryptograficzne moduły obliczeniowe (bezpieczny element i TPM) oraz zabezpieczenia procesora SoC (TEE i bezpieczny start), a także na specjalistycznej wiedzy z zakresu bezpieczeństwa urządzeń brzegowych.

Moduł TPM

Moduł TPM (Trusted Platform Module) to składnik udostępniający funkcje kryptograficzne umożliwiające ochronę informacji przed nieupoważnionym dostępem. Aplikacja jest zawsze aktywna i nie ma ustawień, które można zmienić.

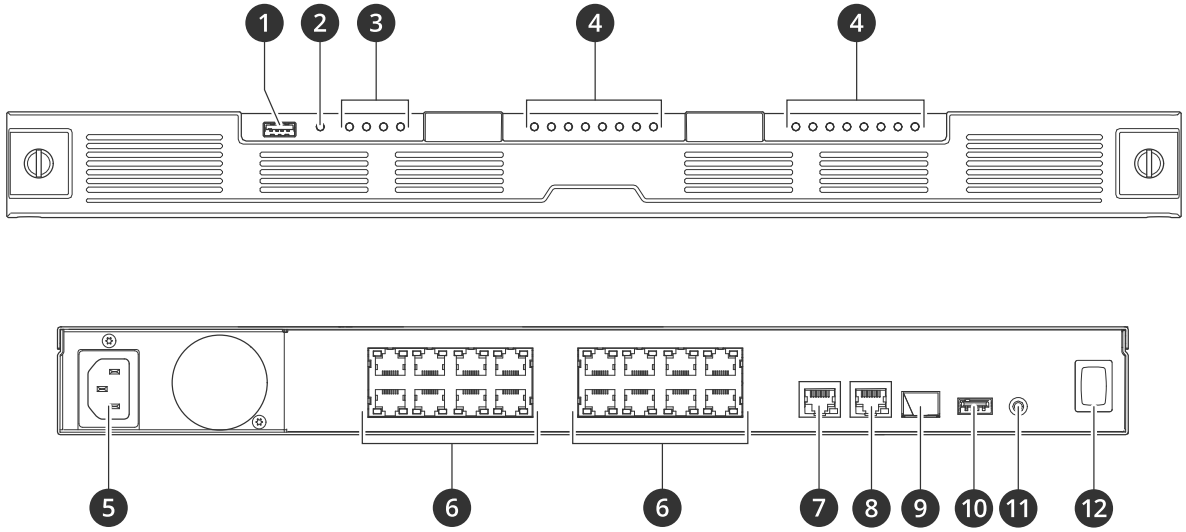
Identyfikator urządzenia axis

możliwość zweryfikowania pochodzenia urządzenia jest kluczowa z perspektywy wiarygodności tożsamości urządzenia. Podczas produkcji urządzenia z rozwiązaniem Axis Edge Vault mają przypisywany unikatowy fabryczny i zgodny ze standardem IEEE 802.1AR certyfikat znany jako identyfikator urządzenia Axis. Jest on swego rodzaju paszportem, który potwierdza pochodzenie urządzenia. Identyfikator urządzenia jest bezpiecznie i trwale przechowywany w bezpiecznym magazynie kluczy w postaci certyfikatu podpisanego za pomocą certyfikatu głównego Axis. ID urządzenia może być wykorzystywany przez infrastrukturę IT klienta do zautomatyzowanego bezpiecznego wdrażania urządzeń i bezpiecznej identyfikacji urządzeń.

Aby dowiedzieć się więcej o funkcjach cyberbezpieczeństwa stosowanych w urządzeniach Axis, przejdź do strony *axis.com/learning/white-papers* i poszukaj według hasła „cybersecurity".

Specyfikacje

Przegląd produktów



1 *Port USB 3.0*
2 *Dioda LED statusu produktu*
3 *Diody LED statusu dysków twardych*
4 *Diody LED statusu sieci/PoE*
5 *Złącze zasilania*
6 *Porty PoE*
7 *Port AUX RJ45*
8 *Port LAN RJ45*
9 *Port LAN SFP*
10 *Port USB 2.0*
11 *Przycisk kontrolny*
12 *Przycisk zasilania*

Specyfikacje

Przednie diody LED

dioda LED	Kolor	Wskazanie
Status produktu	Zielony	Rejestrator jest włączony, a stan to OK.
	Bursztynowy	Rejestrator jest uruchamiany lub trwa aktualizacja oprogramowania sprzętowego. Zaczekaj, aż dioda LED zaświeci się na zielono.
	Czerwony	Może to oznaczać, że budżet PoE został przekroczony. Jeśli urządzenie zostało dopiero połączone z rejestratorem, spróbuj je usunąć.
Stan dysku twardego	Zielony	Dysk jest w trybie online.
	Bursztynowy	Ten dysk jest w trybie online, ale inny dysk jest uszkodzony. Brak nadmiarowości macierzy RAID.
	Czerwony	Dysk jest uszkodzony.
	Wszystkie czerwone	Awaria RAID. System nie nagrywa. W razie awarii RAID otwórz interfejs WWW urządzenia i przejdź do menu **System > Storage > Hard drive status (System > Zasób > Stan dysku twardego)**, aby znaleźć uszkodzony dysk twardy.
	Wył.	Brak dysku twardego.
Status PoE	Zielony	Urządzenie jest podłączone.
	Bursztynowy	PoE jest w użytku, ale brak połączenia sieciowego.
	Czerwony	Nie można uruchomić podłączonego urządzenia. Przekroczono budżet PoE. Awaria PoE.
	Wył.	Port nie jest używany lub został wyłączony.

Tylne wskaźniki LED

dioda LED	Kolor	Wskazanie
Port sieciowy	Miga na zielono	2,5 Gbit/s
	Miga na bursztynowo	1 Gbit/s
	Wył.	Brak sieci
portem PoE Lewy wskaźnik LED	Zielony	PoE jest w użyciu.
	Czerwony	Awaria PoE. Przekroczono budżet PoE.
	Wył.	Port nie jest używany lub został wyłączony.
portem PoE Prawy wskaźnik LED	Miga na zielono	1 Gbit/s
	Miga na bursztynowo	100 Mbit/s
	Wył.	Brak sieci

Przycisk zasilania

- Aby wyłączyć rejestrator, naciśnij przycisk zasilania i przytrzymaj, aż brzęczyk wyemituje krótki dźwięk.
- Aby wyciszyć brzęczyk, naciśnij i zwolnij przycisk zasilania.

Przycisk kontrolny

Przycisk ten służy do:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz *Twarde resetowanie rejestratora na stronie 10*.
- Nawiązywanie połączenia przez Internet z usługą łączenia w chmurze jednym kliknięciem (O3C). Aby połączyć się z usługą, naciśnij i przytrzymaj przycisk przez około trzy sekundy, aż dioda LED stanu zacznie migać na zielono.

Rozwiązywanie problemów –

Problemy techniczne, wskazówki i rozwiązania

Wydano	Rozwiązanie
Moje zapisy są niedostępne.	Przejdź do *Rozwiązywanie typowych problemów na stronie 31*.
Nie mogę połączyć się z kamerami.	Przejdź do *Rozwiązywanie typowych problemów na stronie 31*.
Otrzymuję powiadomienie o błędzie: „No contact" (Brak kontaktu).	Przejdź do *Rozwiązywanie typowych problemów na stronie 31*.
Moje lokalizacje nie są widoczne w aplikacji mobilnej.	Upewnij się, że masz wersję 4 aplikacji mobilnej AXIS Companion.

Rozwiązywanie typowych problemów

Przed ponownym uruchomieniem skonfiguruj lub zresetuj urządzenia.

1. Sprawdź, czy kamery i rejestrator są podłączone do zasilania.
2. Sprawdź, czy masz połączenie z Internetem.
3. Sprawdź, czy sieć działa prawidłowo.
4. Sprawdź, czy kamery są podłączone do tej samej sieci, w której znajduje się komputer, chyba że korzystasz z łączności zdalnej.

Nadal coś nie działa?

5. Upewnij się, że kamery, rejestrator i aplikacja komputerowa AXIS Companion mają zainstalowane najnowsze aktualizacje oprogramowania sprzętowego i oprogramowania.

   Zobacz *Aktualizuj oprogramowanie sprzętowe na stronie 31*.
6. Uruchom ponownie aplikację komputerową AXIS Companion.
7. Uruchom ponownie kamery i rejestrator.

Nadal coś nie działa?

8. Wykonaj twardy reset kamer i rejestratora, aby przywrócić w nich ustawienia fabryczne.

   Patrz *Twarde resetowanie rejestratora na stronie 10*.
9. Podobnie dodaj zresetowane kamery do lokalizacji.

Nadal coś nie działa?

10. Zaktualizuj kartę graficzną przy użyciu najnowszych sterowników.

Nadal coś nie działa?

11. Zapisz raport systemowy i skontaktuj się z działem wsparcia technicznego Axis.

    Patrz *Zapisywanie raportu systemowego na stronie 32*.

Aktualizuj oprogramowanie sprzętowe

Nowe aktualizacje oprogramowania sprzętowego zawierają najnowsze, ulepszone opcje, funkcje i zabezpieczenia.

1. Przejdź do interfejsu WWW urządzenia wiodącego.
2. Wybierz kolejno opcje **Maintenance > Firmware upgrade (Konserwacja > Aktualizacja oprogramowania sprzętowego)** > **Upgrade (Aktualizuj)**.
3. Postępuj zgodnie z instrukcjami na ekranie.

Nie mogę zalogować się w interfejsie WWW produktu

W przypadku ustawienia hasła dla produktu podczas konfiguracji, a następnie dodania tego produktu do lokalizacji, nie można zalogować się w interfejsie WWW produktu przy użyciu hasła, które zostało ustawione. Dzieje się tak dlatego, że oprogramowanie AXIS Companion zmienia hasła wszystkich urządzeń w lokalizacji.

Aby zalogować się do urządzenia w lokalizacji, wpisz nazwę użytkownika **root** i hasło dostępu do lokalizacji.

Jak usunąć wszystkie nagrania

1. W interfejsie WWW urządzenia przejdź do menu **System** > **Storage (Zasób)**.
2. Wybierz **Format** i kliknij **Use tool (Użyj narzędzia)**.

Uwaga

Spowoduje to usunięcie wszystkich nagrań z dysku twardego, ale konfiguracja rejestratora i lokalizacji nie ulega zmianie.

Zapisywanie raportu systemowego

1. W aplikacji AXIS Companion przejdź do obszaru  > **Save system report (Zapisz raport systemowy)**.
2. W aplikacji AXIS Camera Station przejdź do obszaru  **> Help (Pomoc) > System report (Raport systemowy)**.
3. W przypadku rejestracji nowego przypadku na stronie wsparcia technicznego Axis dołącz raport systemowy.

Potrzebujesz więcej pomocy?

Przydatne łącza

- *Instrukcja obsługi aplikacji AXIS Companion*
- *Instrukcja obsługi użytkownika AXIS Camera Station*

Kontakt z pomocą techniczną

Aby uzyskać pomoc, przejdź na stronę *axis.com/support*.

Podręcznik użytkownika
AXIS S3016 Recorder

Wer. M5.2
Data: Styczeń 2025
Nr katalogowy T10186767