AXIS A1601 Network Door Controller

Podręcznik użytkownika

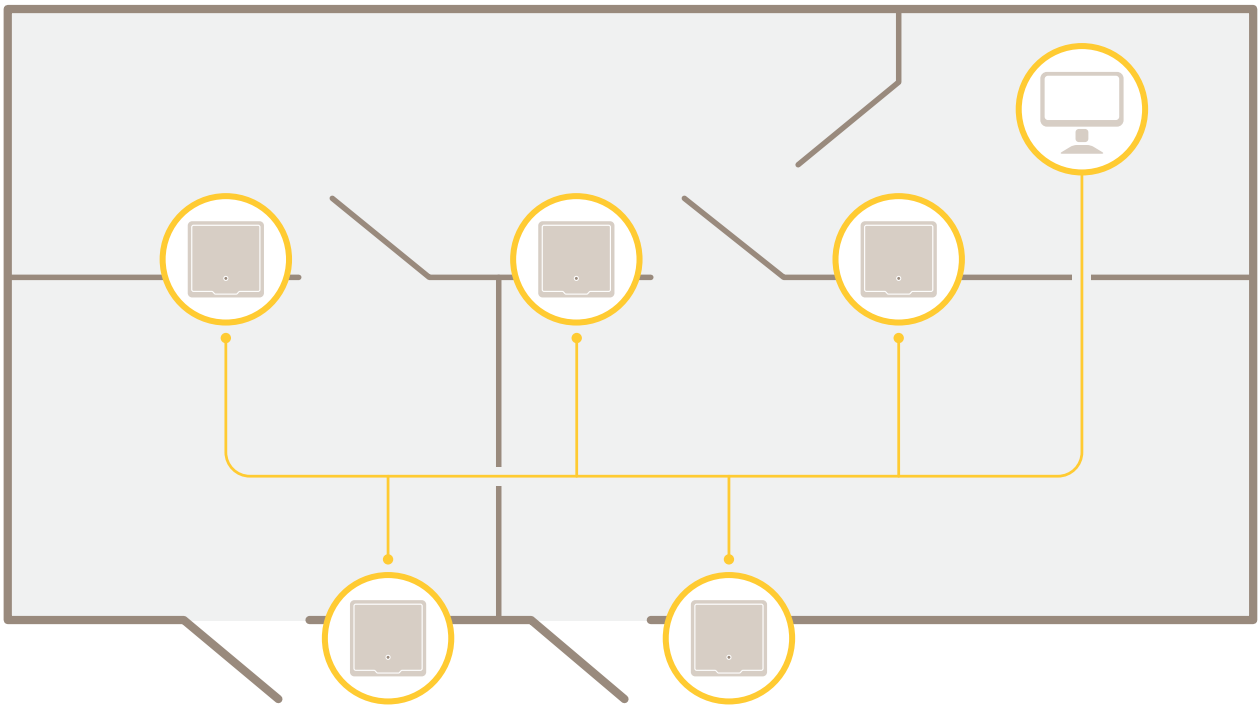
Spis treści

Informacje o rozwiązaniu....5
Przegląd produktów....6
Wyszukiwanie urządzenia w sieci....7
Dostęp do urządzenia....7
Uzyskiwanie dostępu do produktu przez internet....7
Bezpieczne hasła....7
Ustawianie hasła root....8
Strona Informacje ogólne....8
Konfiguracja systemu....9
Konfiguracja – krok po kroku....9
Wybór języka....9
Ustawianie daty i godziny....9
Pobieranie daty i godziny z serwera sieciowego protokołu synchronizacji czasu (NTP)....10
Ręczne ustawianie daty i godziny....10
Pobieranie daty i godziny z komputera....10
Konfiguracja ustawień sieciowych....10
Konfigurowanie sprzętu....10
Importowanie pliku konfiguracji sprzętowej....11
Tworzenie nowej konfiguracji sprzętowej....11
Tworzenie nowej konfiguracji sprzętowej bez urządzeń peryferyjnych....11
Tworzenie nowej konfiguracji sprzętowej zamków bezprzewodowych....14
Tworzenie nowej konfiguracji sprzętowej ze sterowaniem windą (AXIS A9188)....15
Dodawanie i konfiguracja sieciowych urządzeń peryferyjnych....16
Zweryfikuj połączenia ze sprzętem....16
Zarządzanie weryfikacją drzwi....16
Zarządzanie weryfikacją pięter....17
Skonfiguruj karty i formaty....17
Opisy formatu karty....18
Format karty....18
Mapy pól....19
Konfiguracja usług....20
SmartIntego....20
Profil LED OSDP....21
Instrukcje konserwacji....22
Konfiguracja zdarzeń....23
Wyświetlanie dziennika zdarzeń....23
Filtry dziennika zdarzeń....23
Konfigurowanie dziennika zdarzeń....23
Opcje dziennika zdarzeń....23
Konfigurowanie reguł akcji....23
Dodawanie odbiorców....24
Jak stworzyć harmonogram....25
Konfiguracja powtórzeń....25
Informacje zwrotne z czytnika....25
Opcje systemu....27
Bezpieczeństwo....27
Użytkownicy....27
ONVIF....27
Filtr adresów IP....27
HTTPS....27
IEEE 802.1X....28
Certyfikaty....28
Sieć....29

Podstawowe ustawienia TCP/IP 29
Zaawansowane ustawienia TCP/IP 30
SOCKS 32
QoS (Quality of Service) 33
SNMP 33
UPnP 33
Bonjour 34
Porty i urządzenia 34
Porty we/wy 34
Status portu 34
Konserwacja 34
Wsparcie 35
Informacje ogólne o pomocy technicznej 35
Przegląd systemu 35
Dzienniki i raporty 35
Zaawansowane 35
Używanie skryptów 35
Przesyłanie plików 36
Rozwiązywanie problemów 37
Przywracanie domyślnych ustawień fabrycznych 37
Sprawdzanie bieżącej wersji oprogramowania sprzętowego 37
Jak dokonać aktualizacji oprogramowania sprzętowego 37
Objawy, możliwe przyczyny i sposoby naprawy 38
Specyfikacje 40
..... 40
Wskaźniki LED 40
Przyciski 40
Przycisk kontrolny 40
Złącza 40
Złącze sieciowe 40
Złącze czytnika 41
Złącze drzwi 42
Złącze przekaźnikowe 43
Złącze pomocnicze 44
Złącze zewnętrzne 45
Złącze zasilania 45
Złącze wejścia zapasowego akumulatora 46
Informacje dotyczące bezpieczeństwa 47
Poziomy zagrożenia 47
Inne poziomy komunikatów 47
Interfejs WWW 48
..... 48
Status 48
Urządzenie 49
Alarmy 49
Urządzenia peryferyjne 50
Czytniki 50
Zamki bezprzewodowe 51
Uaktualnianie 51
System 51
Czas i lokalizacja 51
Sieć 53
Bezpieczeństwo 57
Konta 61
MQTT 62
Akcesoria 65

Dzienniki 65
Konserwacja 68

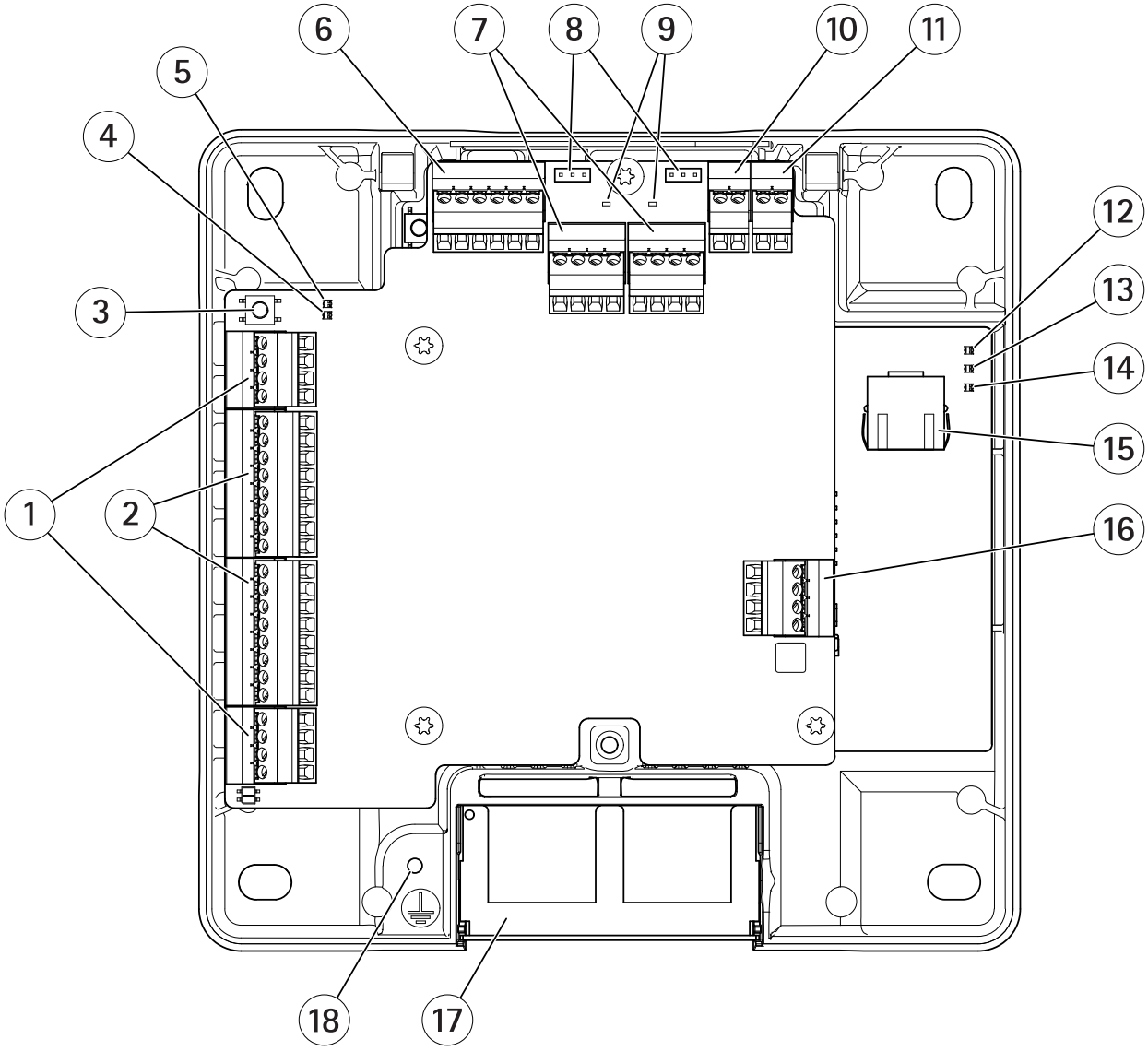
Informacje o rozwiązaniu



Sieciowy kontroler drzwi można łatwo podłączyć do istniejącej sieci IP i zasilać go z niej z bez konieczności prowadzenia dodatkowego okablowania.

Każdy sieciowy kontroler drzwi to inteligentne urządzenie, które można łatwo zamontować w pobliżu drzwi. Może ono zasilać i kontrolować maksymalnie cztery czytniki.

Przegląd produktów



1 *Złącze drzwi, on page 42 (2x)*
2 *Złącze czytnika, on page 41 (2x)*
3 *Przycisk kontrolny, on page 40*
4 *Wskaźnik LED nadprądu czytnika*
5 *Wskaźnik LED nadprądu przekaźnika*
6 *Złącze pomocnicze, on page 44*
7 *Złącze przekaźnikowe, on page 43 (2x)*
8 *Zworka przekaźnika (2x)*
9 *Wskaźnik LED przekaźnika (2x)*
10 *Złącze wejścia zapasowego akumulatora, on page 46*
11 *Złącze zasilania, on page 45*
12 *Wskaźnik LED zasilania*
13 *Dioda stanu*
14 *Wskaźnik LED sieci*
15 *Złącze sieciowe, on page 40*
16 *Złącze zewnętrzne, on page 45*
17 *Odwracalna osłona kabla*
18 *Położenie uziemienia*

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. 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*.

Dostęp do urządzenia

1. Otwórz przeglądarkę i wprowadź adres IP lub nazwę hosta urządzenia Axis.
   Jeśli nie znasz adresu IP, użyj narzędzia AXIS IP Utility lub AXIS Device Manager, aby zlokalizować urządzenie w sieci.
2. Wprowadź nazwę użytkownika oraz hasło. Jeżeli uzyskujesz dostęp do urządzenia po raz pierwszy, musisz ustawić hasło root. Zob. .
3. W przeglądarce zostanie otwarta strona internetowa urządzenia. Strona początkowa nosi nazwę Informacje ogólne.

Uzyskiwanie dostępu do produktu przez internet

Router sieciowy umożliwia produktom w sieci prywatnej (LAN) współdzielić jedno połączenie internetowe. Odbywa się to poprzez przekazanie ruchu sieciowego z sieci prywatnej do internetu.

Większość routerów jest wstępnie skonfigurowana tak, aby zatrzymać próby uzyskania dostępu do sieci prywatnej (LAN) z sieci publicznej (internetu).

Użyj opcji **NAT traversal**, gdy produkt Axis jest podłączony do intranetu (LAN) i chcesz go udostępnić po drugiej stronie (WAN) routera NAT. Po prawidłowym skonfigurowaniu NAT traversal cały ruch HTTP do zewnętrznego portu HTTP w routerze NAT jest przekazywany do produktu.

Włączanie funkcji NAT traversal

- Przejdź do menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Network (Sieć) > TCP/IP > Advanced (Zaawansowane)**.
- Kliknij przycisk **Włącz**.
- Ręcznie skonfiguruj router NAT, aby umożliwić dostęp przez internet.

Uwaga

- W tym kontekście router oznacza dowolne urządzenie działające jako router sieciowy, takie jak router NAT, router sieciowy, bramka internetowa, router szerokopasmowy, urządzenie do udostępniania szerokopasmowego lub oprogramowanie, takie jak zapora.
- Aby funkcja NAT traversal działała, produkt musi obsługiwać NAT traversal. Router musi również obsługiwać protokół UPnP®.

Bezpieczne hasła

Ważne

Aby ustawić hasło lub inne poufne konfiguracje przez sieć IP, należy korzystać z protokołu HTTPS (który jest domyślnie włączony). Protokół HTTPS umożliwia bezpieczne i szyfrowane połączenia sieciowe, chroniąc w ten sposób poufne dane takie jak hasła.

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.

Ustawianie hasła root

Aby uzyskać dostęp do produktu Axis, należy ustawić hasło dla domyślnego administratora **root**. Można to zrobić w oknie dialogowym **Skonfiguruj hasło root**, które zostanie otwarte przy pierwszym dostępie do produktu.

Aby uniknąć podsłuchów sieciowych, hasło root można ustawić za pomocą zaszyfrowanego połączenia HTTPS, wymagającego certyfikatu HTTPS. HTTPS (Hypertext Transfer Protocol over SSL) to protokół używany do szyfrowania ruchu pomiędzy przeglądarkami i serwerami. Certyfikat HTTPS zapewnia szyfrowaną wymianę informacji. Zob. *HTTPS, on page 27*.

Domyślna nazwa użytkownika dla administratora **root** jest stała i nie można jej usunąć. W razie utraty hasła dla użytkownika root należy przywrócić ustawienia fabryczne produktu. Zob. *Przywracanie domyślnych ustawień fabrycznych, on page 37*.

Aby ustawić hasło, wprowadź je bezpośrednio w oknie dialogowym.

Strona Informacje ogólne

Strona Informacje ogólne na stronie internetowej produktu zawiera informacje o nazwie kontrolera drzwi, adresie MAC, adresie IP i wersji oprogramowania sprzętowego. Umożliwia także identyfikację kontrolera drzwi w sieci.

Przy pierwszym dostępie do produktu Axis na stronie Informacje ogólne pojawi się monit o skonfigurowanie sprzętu, ustawienie daty i godziny oraz skonfigurowanie ustawień sieci. Więcej informacji na temat konfigurowania systemu: *Konfiguracja – krok po kroku, on page 9*.

Aby powrócić do strony Informacje ogólne na innych stronach internetowych produktu, kliknij opcję **Informacje ogólne** na pasku menu.

Konfiguracja systemu

Aby otworzyć strony konfiguracji produktu, kliknij opcję **Ustawienia** w prawym górnym rogu strony Informacje ogólne.

Produkt Axis może być konfigurowany przez administratorów. Więcej informacji dotyczących użytkowników i administratorów: *page 27*.

Konfiguracja – krok po kroku

Przed rozpoczęciem korzystania z systemu kontroli dostępu należy wykonać następujące etapy konfiguracji:

1. Jeśli na co dzień nie posługujesz się językiem angielskim, możesz wybrać inny język strony internetowej produktu. Zob. *Wybór języka, on page 9*.
2. Ustaw datę i godzinę. Zob. *page 9*.
3. Skonfiguruj ustawienia sieciowe. Zob. *page 10*.
4. Skonfiguruj kontroler drzwi i podłączone urządzenia, takie jak czytniki, zamki i urządzenia request to exit (REX). Zob. *Konfigurowanie sprzętu, on page 10*.
5. Zweryfikuj połączenia ze sprzętem. Zob. *page 16*.
6. Skonfiguruj karty i formaty. Zob. *page 17*.

Informacje dotyczące zaleceń w zakresie konserwacji: *Instrukcje konserwacji, on page 22*.

Wybór języka

Domyślnym językiem strony internetowej produktu jest angielski, ale możesz przełączyć się na dowolny język skonfigurowany w urządzeniu. Informacje na temat najnowszego dostępnego oprogramowania sprzętowego można znaleźć na stronie *www.axis.com*.

Możesz zmienić język na dowolnej stronie internetowej produktu.

Aby zmienić język, kliknij listę rozwijaną języków  i wybierz język. Wszystkie strony internetowe i strony pomocy produktu będą wyświetlane w wybranym języku.

Uwaga

- Po zmianie języka format daty zmienia się również na format powszechnie używany w wybranym języku. Poprawny format jest wyświetlany w polach danych.
- Jeśli zresetujesz urządzenie do domyślnych ustawień fabrycznych, strona internetowa produktu przełączy się z powrotem na angielski.
- Jeśli przywrócisz lub ponownie uruchomisz produkt albo zaktualizujesz oprogramowanie sprzętowe, strona internetowa produktu będzie nadal używać wybranego języka.

Ustawianie daty i godziny

Aby ustawić datę i godzinę produktu Axis, przejdź do menu **Ustawienia > Data i godzina**.

Datę i godzinę możesz ustawić w jeden z następujących sposobów:

- Pobieranie daty i godziny z serwera sieciowego protokołu synchronizacji czasu (NTP). Zob. *page 10*.
- Ręczne ustawianie daty i godziny. Zob. *page 10*.
- Pobieranie daty i godziny z komputera. Zob. *page 10*.

Aktualny czas kontrolera to aktualna data i godzina kontrolera drzwi (w formacie 24 h).

Te same opcje dla daty i godziny są również dostępne na stronach Opcji systemu. Przejdź do menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Date & Time (Data i godzina)**.

Pobieranie daty i godziny z serwera sieciowego protokołu synchronizacji czasu (NTP)

1. Przejdź do menu **Ustawienia > Data i godzina**.
2. Wybierz **Strefę czasową** z listy rozwijanej.
3. Jeśli w Twoim regionie stosowana jest zmiana czasu letniego, wybierz opcję **Dostosuj do zmiany czasu letniego**.
4. Wybierz opcję **Synchronizuj z NTP**.
5. Wybierz domyślny adres DHCP lub wprowadź adres serwera NTP.
6. Kliknij przycisk **Save (Zapisz)**.

Podczas synchronizacji z serwerem NTP data i godzina są aktualizowane w sposób ciągły, ponieważ dane są wysyłane z serwera NTP. Informacje dotyczące ustawień NTP: *Konfiguracja NTP, on page 31*.
W przypadku używania nazwy hosta dla serwera NTP należy skonfigurować serwer DNS. Zob. *Konfiguracja DNS, on page 30*.

Ręczne ustawianie daty i godziny

1. Przejdź do menu **Ustawienia > Data i godzina**.
2. Jeśli w Twoim regionie stosowana jest zmiana czasu letniego, wybierz opcję **Dostosuj do zmiany czasu letniego**.
3. Wybierz polecenie **Ustaw datę i godzinę ręcznie**.
4. Wprowadź żądaną datę i godzinę.
5. Kliknij przycisk **Save (Zapisz)**.

W przypadku ręcznego ustawiania daty i godziny data i godzina zostaną ustawione jednorazowo i nie będą automatycznie aktualizowane. Oznacza to, że jeśli będzie wymagana aktualizacja daty lub godziny, zmiany muszą zostać wprowadzone ręcznie, ponieważ nie ma połączenia z zewnętrznym serwerem NTP.

Pobieranie daty i godziny z komputera

1. Przejdź do menu **Ustawienia > Data i godzina**.
2. Jeśli w Twoim regionie stosowana jest zmiana czasu letniego, wybierz opcję **Dostosuj do zmiany czasu letniego**.
3. Wybierz polecenie **Ustaw datę i godzinę ręcznie**.
4. Kliknij przycisk **Zsynchronizuj i zapisz**.

Podczas korzystania z czasu komputera data i godzinę są synchronizowane z komputerem raz i nie będą aktualizowane automatycznie. Oznacza to, że zmiana daty i godziny w komputerze, który służy do zarządzania systemem, wymaga ponownej synchronizacji z urządzeniem.

Konfiguracja ustawień sieciowych

Aby skonfigurować podstawowe ustawienia sieciowe, przejdź do menu **Ustawienia > Ustawienia sieciowe** lub **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Podstawowe**.

Aby uzyskać więcej informacji o ustawieniach sieciowych, p. sekcja *Sieć, on page 29*.

Konfigurowanie sprzętu

Przed zakończeniem konfiguracji sprzętowej możesz podłączyć czytniki, blokady i inne urządzenia do produktu Axis. Jednak łatwiej będzie podłączyć urządzenia, jeśli najpierw zakończysz konfigurację sprzętową, ponieważ schemat styków sprzętu będzie dostępny po zakończeniu konfiguracji. Schemat styków sprzętu jest przewodnikiem po podłączaniu urządzeń do pinów i może służyć jako arkusz referencyjny do konserwacji. Instrukcje dotyczące konserwacji, p. *page 22*.

Jeśli konfigurujesz sprzęt po raz pierwszy, wybierz jedną z następujących metod:

- Importowanie pliku konfiguracji sprzętowej. Zob. *page 11*.
- Tworzenie nowej konfiguracji sprzętowej. Zob. *page 11*.

Uwaga

Jeśli sprzęt danego produktu nie został uprzednio skonfigurowany lub został usunięty, opcja **Konfiguracja sprzętowa** będzie dostępna w panelu powiadomień na stronie Informacje ogólne.

Importowanie pliku konfiguracji sprzętowej

Konfigurację sprzętową produktu Axis można wykonać szybciej, importując plik konfiguracji sprzętowej.

Po wyeksportowaniu pliku z jednego produktu i zaimportowaniu go do innych można wykonać wiele kopii tej samej konfiguracji sprzętowej bez powtarzania tych samych kroków. Można także przechowywać eksportowane pliki jako kopie zapasowe i używać ich do przywracania poprzedniej konfiguracji sprzętowej. Aby uzyskać dodatkowe informacje, zob. *Eksportowanie pliku konfiguracji sprzętowej, on page 11*.

Importowanie pliku konfiguracji sprzętowej:

1. Przejdź do menu **Ustawienia > Konfiguracja sprzętowa**.
2. Kliknij przycisk **Importuj konfigurację sprzętową** lub, jeśli konfiguracja sprzętowa już istnieje, **Zresetuj i zaimportuj konfigurację sprzętową**.
3. W wyświetlonym oknie dialogowym przeglądarki plików znajdź i wybierz plik konfiguracji sprzętowej (*.json) na swoim komputerze.
4. Kliknij **OK**.

Eksportowanie pliku konfiguracji sprzętowej

Konfigurację sprzętową produktu Axis można wyeksportować w celu wielokrotnego skopiowania tej samej konfiguracji sprzętowej. Można także przechowywać eksportowane pliki jako kopie zapasowe i używać ich do przywracania poprzedniej konfiguracji sprzętowej.

Uwaga

Konfiguracji sprzętowej pięter nie można wyeksportować.

Ustawienia zamków bezprzewodowych nie są uwzględniane podczas eksportowania konfiguracji sprzętowej.

Aby wyeksportować plik konfiguracji sprzętowej:

1. Przejdź do menu **Ustawienia > Konfiguracja sprzętowa**.
2. Kliknij polecenie **Eksportuj konfigurację sprzętową**.
3. W zależności od przeglądarki konieczne może być przejście do okna dialogowego w celu dokończenia eksportu.
   Jeśli nie określono inaczej, wyeksportowany plik (*.json) zostanie zapisany w domyślnym folderze pobierania. Folder pobierania można wybrać w ustawieniach użytkownika przeglądarki internetowej.

Tworzenie nowej konfiguracji sprzętowej

Postępuj zgodnie z instrukcjami według wymogów:

- *Tworzenie nowej konfiguracji sprzętowej bez urządzeń peryferyjnych, on page 11*
- *Tworzenie nowej konfiguracji sprzętowej zamków bezprzewodowych, on page 14*
- *Tworzenie nowej konfiguracji sprzętowej ze sterowaniem windą (AXIS A9188), on page 15*

Tworzenie nowej konfiguracji sprzętowej bez urządzeń peryferyjnych

1. Przejdź do menu **Ustawienia > Konfiguracja sprzętowa** i kliknij polecenie **Utwórz nową konfigurację sprzętową**.
2. Wprowadź nazwę produktu Axis.
3. Wybierz liczbę podłączonych drzwi i kliknij przycisk **Dalej**.

4. Skonfiguruj monitory drzwi (czujniki położenia drzwi) i zamki wedle potrzeby, a następnie kliknij przycisk **Dalej**. Więcej informacji na temat dostępnych opcji, p. *Konfiguracja monitorów drzwi i zamków, on page 12*.
5. Skonfiguruj używane czytniki i urządzenia REX, a następnie kliknij przycisk **Zakończ**. Więcej informacji na temat dostępnych opcji, p. *Konfiguracja czytników i urządzeń REX, on page 13*.
6. Kliknij przycisk **Zamknij** lub łącze prowadzące do schematu styków sprzętu.

Konfiguracja monitorów drzwi i zamków

Po wybraniu opcji drzwi podczas nowej konfiguracji sprzętowej możesz skonfigurować monitory drzwi i zamki.

1. Jeśli będzie używany monitor drzwi, wybierz **Monitor drzwi**, a następnie wybierz opcję odpowiadającą temu, jak obwody monitora drzwi będą połączone.
2. Jeśli zamek drzwi ma być blokowany natychmiast po otwarciu drzwi, wybierz **Anuluj czas dostępu po otwarciu drzwi**.
   Jeśli chcesz opóźnić ponowne zablokowanie, ustaw wartość czasu opóźnienia w milisekundach w opcji **Czas ponownego zablokowania**.
3. Określ opcje czasu monitorowania drzwi lub jeśli żaden monitor drzwi nie będzie używany – opcje czasu zamka.
4. Wybierz opcje odpowiadające temu, jak obwody monitora drzwi będą połączone.
5. Jeśli będzie używany monitor zamka, wybierz **Monitor zamka**, a następnie wybierz opcję odpowiadającą temu, jak obwody monitora drzwi będą połączone.
6. Jeśli połączenia wejściowe z czytników, urządzeń REX i monitorów drzwi będą nadzorowane, wybierz opcję **Włącz nadzorowane wejścia**.
   Aby uzyskać dodatkowe informacje, zob. *Używanie nadzorowanych wejść, on page 14*.

Uwaga

- Większość opcji blokady, monitora drzwi i czytnika można zmienić bez resetowania i uruchamiania nowej konfiguracji sprzętowej. Przejdź do menu **Ustawienia > Ponowna konfiguracja sprzętowa**.
- Możesz połączyć jeden monitor zamka na kontroler drzwi. Jeśli więc używasz drzwi z podwójnym zamkiem, tylko jeden z zamków może mieć monitor zamka. Jeśli dwie pary drzwi są połączone z tym samym kontrolerem drzwi, nie można używać monitorów zamka.

Informacje o monitorze drzwi i opcjach ustawień czasu

Dostępne są następujące opcje dla monitora drzwi:

- **Monitor drzwi** – wybierany domyślnie. Każde drzwi mają własny monitor drzwi, który sygnalizuje, jeśli drzwi otworzono siłą lub jeśli zbyt długo pozostawały otwarte. Odznacz, jeśli monitor drzwi nie będzie używany.

– **Obwód otwarty = Drzwi zablokowane** – wybierz, jeśli obwód monitora drzwi jest normalnie otwarty. Monitor drzwi wysyła sygnał odblokowanych drzwi, kiedy obwód jest zamknięty. Monitor drzwi wysyła sygnał zablokowanych drzwi, kiedy obwód jest otwarty.

– **Obwód otwarty = Drzwi odblokowane** – wybierz, jeśli obwód monitora drzwi jest normalnie zamknięty. Monitor drzwi wysyła sygnał odblokowanych drzwi, kiedy obwód jest otwarty. Monitor drzwi wysyła sygnał zablokowanych drzwi, kiedy obwód jest zamknięty.

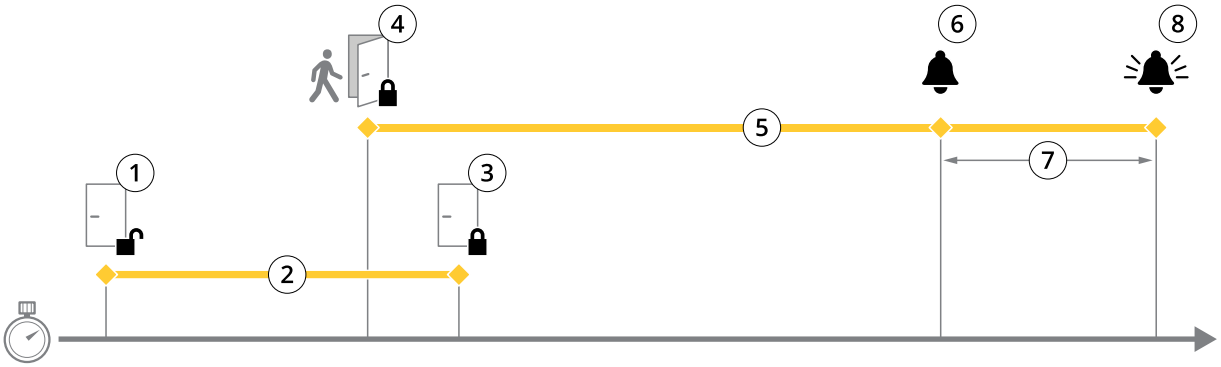
- **Anuluj czas dostępu po otwarciu drzwi** – wybierz, aby zapobiec nieautoryzowanemu wjazdowi/wejściu. Zamek zostanie zablokowany, jak tylko monitor drzwi wskaże, że drzwi są odblokowane.

Następujące opcje ustawień czasu dla drzwi są zawsze dostępne:

- **Czas dostępu** – podaj czas (w sekundach) odblokowania drzwi po uzyskaniu dostępu. Drzwi pozostaną odblokowane do momentu ich otwarcia lub upłynięcia ustawionego czasu. Drzwi zostaną zablokowane po zamknięciu niezależnie od tego, czy czas dostępu upłynął, czy nie.
- **Długi czas dostępu** – podaj czas (w sekundach) odblokowania drzwi po uzyskaniu dostępu. Długi czas dostępu nadpisuje wcześniej ustawiony czas dostępu i zostanie włączony w przypadku użytkowników, dla których wybrano długi czas dostępu.

Wybierz opcję **Monitor drzwi**, aby udostępnić następujące opcje ustawień czasu dla drzwi:

- **Otwarte zbyt długo** – podaj czas (w sekundach), przez jaki drzwi mogą być otwarte. Jeżeli po upłynięciu ustawionego czasu drzwi pozostają otwarte, wyzwalany jest alarm związany ze zbyt długim otwarciem drzwi. Ustaw regułę akcji, aby skonfigurować akcję, którą powinno wyzwolić zdarzenie zbyt długiego otwarcia drzwi.
- **Czas przed alarmem** – alarm wstępny to sygnał ostrzegawczy, wyzwalany po upłynięciu czasu ustawionego w opcji „Otwarte zbyt długo". Informuje on administratora i, w zależności od konfiguracji reguły akcji, ostrzega osobę wchodzącą przez drzwi, że drzwi należy zamknąć, aby uniknąć wyzwolenia alarmu. Podaj czas (w sekundach) przed wyzwoleniem alarmu związanego ze zbyt długim otwarciem drzwi, w którym system ma uruchomić sygnał ostrzegawczego alarmu wstępnego. Aby wyłączyć alarm wstępny, ustaw czas alarmu wstępnego jako 0.



1 Dostęp przyznany – zamek odblokowany
2 Czas dostępu
3 Nie podjęto żadnych działań – zamek zablokowany
4 Podjęto działanie (otwarto drzwi) – zamek zablokowany lub pozostaje odblokowany do momentu zamknięcia drzwi
5 Przekroczony czas otwarcia drzwi
6 Uruchamiany jest alarm wstępny
7 Czas alarmu wstępnego
8 Otwarte zbyt długo – uruchamiany jest alarm

Informacje o konfigurowaniu reguły akcji: *Konfigurowanie reguł akcji, on page 23*.

Informacje o opcjach zamków

Dostępne są następujące opcje obwodów zamków:

- **Przekaźnik** – można go użyć tylko dla jednego zamka na kontroler drzwi. Jeśli z kontrolerem połączone są dwie pary drzwi, przekaźnika można użyć tylko dla zamka drugiej pary drzwi.
- **Brak** – dostępne wyłącznie dla zamka nr 2. Zaznacz, jeśli będzie używany tylko jeden zamek.

Następujące opcje monitora zamka są dostępne dla konfiguracji z jedną parą drzwi:

- **Monitor zamka** – wybierz, aby udostępnić elementy sterowania monitorem zamka. Następnie wybierz zamek, który ma być monitorowany. Monitora zamka można używać tylko dla drzwi z podwójnym zamkiem, ale nie można go używać, jeśli dwie pary drzwi są połączone z kontrolerem drzwi.

– **Obwód otwarty = Drzwi zablokowane** – wybierz, jeśli obwód monitora drzwi jest normalnie zamknięty. Monitor zamka wysyła sygnał odblokowanych drzwi, kiedy obwód jest zamknięty. Monitor zamka wysyła sygnał zablokowanych drzwi, kiedy obwód jest otwarty.

– **Obwód otwarty = Odblokowany** – Wybierz, jeśli obwód monitora zamka jest normalnie otwarty. Monitor zamka wysyła sygnał odblokowanych drzwi, kiedy obwód jest otwarty. Monitor zamka wysyła sygnał zablokowanych drzwi, kiedy obwód jest zamknięty.

Konfiguracja czytników i urządzeń REX

Po przygotowaniu nowej konfiguracji sprzętowej monitorów drzwi i zamków można skonfigurować czytniki i urządzenia REX.

1. Jeżeli używany będzie czytnik, zaznacz pole wyboru i wybierz opcje pasujące do protokołu komunikacji czytnika.
2. Jeżeli używane będą takie urządzenia REX, jak przyciski, czujniki lub zamknięcia drążkowe, zaznacz pole wyboru i wybierz opcję pasującą do sposobu podłączenia obwodów urządzenia REX.
   Jeżeli sygnał REX nie wpływa na otwarcie drzwi (na przykład drzwi z mechanicznymi klamkami lub uchwytami drążkowymi), wybierz opcję **REX nie odblokowuje drzwi**.
3. Jeśli do kontrolera drzwi podłączasz więcej niż jeden czytnik/urządzenie REX, wykonaj powyższe czynności ponownie, tak aby każdy czytnik lub urządzenie REX miało poprawne ustawienia.

Informacje o opcjach czytnika i urządzenia REX

Dostępne są następujące opcje czytnika:

- **Wiegand** – wybierz dla czytników korzystających z protokołów Wiegand. Następnie wybierz kontrolkę LED obsługiwaną przez czytnik. Czytniki z pojedynczymi kontrolkami LED zwykle przełączają się między światłem czerwonym a zielonym. Czytniki z podwójnymi kontrolkami LED mają różne przewody dla czerwonych i zielonych diod LED. Oznacza to, że diody LED są sterowane niezależnie od siebie. Gdy obie diody LED są włączone, światło wydaje się pomarańczowe. Więcej informacji na temat tego, które kontrolki LED obsługuje czytnik, można znaleźć w instrukcji producenta.
- **OSDP, RS485 half duplex** – wybierz dla czytników RS485 z obsługą trybu half duplex (dwużyłowego). Więcej informacji na temat tego, które protokoły obsługuje czytnik, można znaleźć w instrukcji producenta.

Dostępne są następujące opcje urządzenia REX:

- **Aktywny niski** – wybierz, jeśli aktywacja urządzenia REX zamyka obwód.
- **Aktywny wysoki** – wybierz, jeśli aktywacja urządzenia REX otwiera obwód.
- **Sygnał REX nie odblokowuje drzwi** – wybierz, jeżeli sygnał REX nie wpływa na otwarcie drzwi (na przykład drzwi z mechanicznymi klamkami lub uchwytami drążkowymi). Jeżeli użytkownik otworzy drzwi w przewidzianym czasie dostępu, nie zostanie wyzwolony alarm „drzwi wyważone". Anuluj wybór, jeśli drzwi powinny automatycznie odblokowywać się, gdy użytkownik uruchomi urządzenie REX.

Uwaga

Większość opcji blokady, monitora drzwi i czytnika można zmienić bez resetowania i uruchamiania nowej konfiguracji sprzętowej. Przejdź do menu **Ustawienia > Ponowna konfiguracja sprzętowa**.

Używanie nadzorowanych wejść

Nadzorowane wejścia informują o statusie połączenia między kontrolerem drzwi a monitorami drzwi. Jeśli połączenie zostanie przerwane, zostanie aktywowane zdarzenie.

Aby użyć nadzorowanych wejść:

1. Zamontuj rezystory końca linii na wszystkich używanych nadzorowanych wejściach. Schemat połączeń: *page 42*.
2. Przejdź do menu **Ustawienia > Ponowna konfiguracja sprzętowa** i wybierz opcję **Włącz nadzorowane wejścia**. Możesz także włączyć nadzorowane wejścia podczas konfiguracji sprzętowej.

Informacje o zgodności wejść nadzorowanych

Następująca funkcja obsługuje wejścia nadzorowane:

- Monitor drzwi. Zob. *Złącze drzwi, on page 42*.

Tworzenie nowej konfiguracji sprzętowej zamków bezprzewodowych

1. Przejdź do menu **Ustawienia > Konfiguracja sprzętowa** i kliknij polecenie **Utwórz nową konfigurację sprzętową**.
2. Wprowadź nazwę produktu Axis.
3. Z listy urządzeń peryferyjnych wybierz producenta bramki bezprzewodowej.

4. Jeśli chcesz podłączyć drzwi przewodowe, zaznacz pole wyboru **1 Drzwi** i kliknij przycisk **Dalej**. Jeżeli nie dołączono drzwi, kliknij przycisk **Zakończ**.
5. W zależności od producenta zamków, postępuj zgodnie z jednym z punktów:
   - **ASSA Aperio**: Kliknij łącze, aby wyświetlić schemat styków sprzętu lub kliknij przycisk **Close (Zamknij)** i przejdź do menu **Setup > Hardware Reconfiguration (Ustawienia > Ponowna konfiguracja sprzętowa)**, aby zakończyć konfigurację; patrz *Dodawanie drzwi i urządzeń Assa Aperio™, on page 15*
   - **SmartIntego**: Kliknij łącze, aby wyświetlić schemat styków sprzętu lub kliknij przycisk **Kliknij tutaj, aby wybrać bramkę bezprzewodową i skonfigurować drzwi**, aby zakończyć konfigurację; patrz *Informacje na temat konfiguracji SmartIntego, on page 20*.

Dodawanie drzwi i urządzeń Assa Aperio™

Przed dodaniem drzwi bezprzewodowych do systemu należy sparować je z podłączonym koncentratorem komunikacyjnym Assa Aperio, używając narzędzia Aperio PAP (do programowania aplikacji Aperio).

Aby dodać drzwi bezprzewodowe:

1. Przejdź do menu **Ustawienia** > **Ponowna konfiguracja sprzętowa**.
2. W menu Drzwi i urządzenia bezprzewodowe kliknij opcję **Dodaj drzwi**.
3. W polu **Nazwa drzwi**: Wprowadź nazwę opisową.
4. W polu **ID** w menu **Zablokuj**: wprowadź sześcioznakowy adres urządzenia, które chcesz dodać. Adres urządzenia jest wydrukowany na etykiecie produktu.
5. Opcjonalnie w menu **Czujnik położenia drzwi**: Wybierz opcję **Wbudowany czujnik położenia drzwi** lub **Czujnik położenia drzwi zewnętrznych**.

Uwaga

Jeśli korzystasz z zewnętrznego czujnika położenia drzwi (DPS), upewnij się, że urządzenie blokujące Aperio obsługuje wykrywanie stanu klamki drzwi przed jego skonfigurowaniem.

6. Opcjonalnie, w polu **ID** w menu **Czujnik położenia drzwi**: wprowadź sześcioznakowy adres urządzenia, które chcesz dodać. Adres urządzenia jest wydrukowany na etykiecie produktu.
7. Kliknij **Dodaj**.

Tworzenie nowej konfiguracji sprzętowej ze sterowaniem windą (AXIS A9188)

Ważne

Przed utworzeniem konfiguracji sprzętowej należy dodać użytkownika w module przekaźnikowym AXIS 9188 Network I/O Relay Module. Przejdź do interfejsu www A9188 > **Preferencje > Dodatkowa konfiguracja urządzenia > Ustawienia podstawowe > Użytkownicy > Dodaj > Ustawienia użytkownika**.

Uwaga

Z każdym kontrolerem Axis Network Door Controller można połączyć maksymalnie dwa moduły przekaźnikowe AXIS 9188 Network I/O Relay Module.

1. Na stronie internetowej kontrolera przejdź do menu **Ustawienia > Konfiguracja sprzętowa** i kliknij polecenie **Utwórz nową konfigurację sprzętową**.
2. Wprowadź nazwę produktu Axis.
3. Na liście urządzeń peryferyjnych wybierz **Sterowanie windą**, aby dołączyć moduł przekaźnikowy AXIS A9188 Network I/O Relay Module, a następnie kliknij przycisk **Dalej**.
4. Wprowadź nazwę podłączonego czytnika.
5. Wybierz używany protokół czytnika i kliknij przycisk **Zakończ**.
6. Kliknij opcję **Network Peripherals (Sieciowe urządzenia peryferyjne)**, aby zakończyć konfigurację, patrz *Dodawanie i konfiguracja sieciowych urządzeń peryferyjnych , on page 16*, lub kliknij łącze, aby przejść do schematu styków.

Dodawanie i konfiguracja sieciowych urządzeń peryferyjnych

Ważne

- Przed skonfigurowaniem sieciowych urządzeń peryferyjnych należy dodać użytkownika AXIS A9188 Network I/O Relay Module. Przejdź do interfejsu www AXIS A9188 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Preferencje > Dodatkowa konfiguracja urządzenia > Ustawienia podstawowe > Użytkownicy > Dodaj > Ustawienia użytkownika)**.
- Nie należy dodawać kolejnego kontrolera AXIS A1001 Network Door Controller jako sieciowego urządzenia peryferyjnego.

1. Przejdź do menu **Ustawienia > Sieciowe urządzenia peryferyjne**, aby dodać urządzenie.
2. Znajdź swoje urządzenie w części **Wykryte urządzenia**.
3. Kliknij **Dodaj to urządzenie**.
4. Wprowadź nazwę urządzenia
5. Wprowadź nazwę użytkownika i hasło produktu AXIS A9188.
6. Kliknij **Dodaj**.

Uwaga

Sieciowe urządzenia peryferyjne możesz dodać ręcznie, wprowadzając adres MAC lub adres IP w oknie dialogowym **Dodaj urządzenie ręcznie**.

Ważne

Jeżeli chcesz usunąć harmonogram, upewnij się, że nie jest on używany przez sieciowy moduł przekaźnikowy I/O.

Konfigurowanie portów I/O oraz przekaźników w sieciowych urządzeniach peryferyjnych

Ważne

Przed skonfigurowaniem sieciowych urządzeń peryferyjnych należy dodać użytkownika AXIS A9188 Network I/O Relay Module. Przejdź do interfejsu www AXIS A9188 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Preferencje > Dodatkowa konfiguracja urządzenia > Ustawienia podstawowe > Użytkownicy > Dodaj > Ustawienia użytkownika)**.

1. Przejdź do menu **Setup > Network Peripherals (Ustawienia > Sieciowe urządzenia peryferyjne)** i kliknij wiersz **Added devices (Dodane urządzenia)**.
2. Wybierz porty I-O i przekaźniki do ustawienia jako piętro.
3. Kliknij przycisk **Ustaw jako piętro** i wprowadź nazwę.
4. Kliknij **Dodaj**.

Zweryfikuj połączenia ze sprzętem

Po zakończeniu instalacji i konfiguracji sprzętu, a także w dowolnym momencie podczas eksploatacji kontrolera drzwi, można sprawdzić działanie podłączonych monitorów drzwi, sieciowych modułów przekaźnikowych I/O, zamków i czytników.

Aby zweryfikować konfigurację i przejść do elementów zarządzania weryfikacją, przejdź do menu **Ustawienia > Weryfikacja połączeń ze sprzętem**.

Zarządzanie weryfikacją drzwi

- **Status drzwi** – zweryfikuj bieżący status monitora drzwi, alarmów drzwi i zamków. Kliknij przycisk **Odczytaj bieżący status**.
- **Zablokuj** – ręcznie uruchom blokadę. Będzie to miało wpływ zarówno na zamki główne, jak i dodatkowe, jeśli są. Kliknij przycisk **Zablokuj** lub **Odblokuj**.
- **Zablokuj** – ręcznie uruchom blokadę, aby przyznać dostęp. Dotyczy to tylko zamków głównych. Kliknij **Access (Dostęp)**.

- **Reader: Feedback (Czytnik: informacje zwrotne)** – sprawdź informacje zwrotne z czytnika, na przykład dźwięki i sygnały LED, dla różnych poleceń. Wybierz polecenie i kliknij przycisk **Testuj**. Dostępne rodzaje informacji zwrotnych zależą od czytnika. Aby uzyskać dodatkowe informacje, zob. *Informacje zwrotne z czytnika, on page 25*. Patrz także instrukcje producenta.
- **Reader: Tampering (Czytnik: sabotaż)** – uzyskaj informacje o ostatniej próbie ingerencji. Po zamontowaniu czytnika zostanie zarejestrowana pierwsza próba ingerencji. Kliknij opcję **Odczytaj ostatnią ingerencję**.
- **Reader: Card swipe (Czytnik: przeciągnięcie karty)** – uzyskaj informacje na temat ostatniej przeciągniętej karty lub innego tokenu użytkownika zaakceptowanego przez czytnik. Kliknij opcję **Odczytaj ostatnie uprawnienia**.
- **REX** – uzyskaj informacje o ostatnim naciśnięciu przycisku żądania wyjścia (REX). Kliknij **Pobierz ostatni REX**.

Zarządzanie weryfikacją pięter

- **Status piętra** – zweryfikuj bieżący status dostępów do piętra. Kliknij przycisk **Odczytaj bieżący status**.
- **Blokada i odblokowanie piętra** – ręcznie wyzwalaj dostęp do piętra. Będzie to miało wpływ zarówno na zamki główne, jak i dodatkowe, jeśli są. Kliknij przycisk **Zablokuj** lub **Odblokuj**.
- **Dostęp do piętra** – ręczne udzielanie tymczasowego dostępu do piętra. Dotyczy to tylko zamków głównych. Kliknij **Access (Dostęp)**.
- **Elevator Reader: Feedback (Czytnik windy: informacje zwrotne)** – sprawdź informacje zwrotne z czytnika, na przykład dźwięki i sygnały LED, dla różnych poleceń. Wybierz polecenie i kliknij przycisk **Testuj**. Dostępne rodzaje informacji zwrotnych zależą od czytnika. Aby uzyskać dodatkowe informacje, zob. *Informacje zwrotne z czytnika, on page 25*. Patrz także instrukcje producenta.
- **Elevator Reader: Tampering (Czytnik windy: sabotaż)** – uzyskaj informacje o ostatniej próbie ingerencji. Po zamontowaniu czytnika zostanie zarejestrowana pierwsza próba ingerencji. Kliknij opcję **Odczytaj ostatnią ingerencję**.
- **Elevator Reader: Card swipe (Czytnik windy: przeciągnięcie karty)** – uzyskaj informacje na temat ostatniej przeciągniętej karty lub innego tokenu użytkownika zaakceptowanego przez czytnik. Kliknij opcję **Odczytaj ostatnie uprawnienia**.
- **REX** – uzyskaj informacje o ostatnim naciśnięciu przycisku żądania wyjścia (REX). Kliknij **Pobierz ostatni REX**.

Skonfiguruj karty i formaty

Kontroler drzwi ma kilka wstępnie zdefiniowanych często stosowanych formatów kart, które można wykorzystać lub zmodyfikować według potrzeb. Można również tworzyć niestandardowe formaty kart. Każdy format karty ma inny zestaw reguł, mapy pól, sposób uporządkowania informacji przechowywanych na karcie. Dzięki zdefiniowaniu formatu karty system będzie wiedział, jak interpretować informacje, które kontroler pobiera z czytnika. Więcej informacji na temat tego, które formaty kart obsługuje czytnik, można znaleźć w instrukcji producenta.

Aby włączyć formaty kart:

1. Przejdź do menu **Ustawienia > Konfiguracja kart i formatów**.
2. Wybierz jeden lub więcej formatów kart, które pasują do formatu karty używanego przez podłączone czytniki.

Aby utworzyć nowe formaty kart:

1. Przejdź do menu **Ustawienia > Konfiguracja kart i formatów**.
2. Kliknij polecenie **Add card format (Dodaj format karty)**.
3. W oknie dialogowym **Dodaj format karty** wprowadź nazwę, opis i długość bitową formatu karty. Zob. *Opisy formatu karty, on page 18*.
4. Kliknij polecenie **Dodaj mapę pola** i wprowadź wymagane informacje w polach. Zob. *Mapy pól, on page 19*.

5. Aby dodać wiele map pól, powtórz poprzedni krok.

Aby rozwinąć element na liście **Card formats (Formaty kart)** i wyświetlić opisy formatów kart i mapy pól, kliknij ▶.

Aby edytować format karty, kliknij ,255mm,sfx)="graphics:graphic547F89EF9AD2F8699BCC306AD83605C5" i w razie potrzeby zmień opisy formatów kart i mapy pól. Następnie kliknij przycisk **Zapisz**.

Aby usunąć mapę pola, w oknie dialogowym **Edit card format (Edytuj format karty)** lub **Add card format (Dodaj format karty)**, kliknij ,255mm,sfx)="graphics:graphicC8BD4DE53987F8726B1B16D61921EB37"

Aby usunąć format karty, kliknij ,255mm,sfx)="graphics:graphicC8BD4DE53987F8726B1B16D61921EB37".

Ważne

- Możesz włączać i wyłączać formaty kart tylko wtedy, gdy kontroler drzwi w systemie został skonfigurowany z przynajmniej jednym czytnikiem. Zob. *Konfigurowanie sprzętu, on page 10* i *Konfiguracja czytników i urządzeń REX, on page 13*.
- Dwa formaty kart o tej samej długości bitów nie mogą być aktywne w tym samym czasie. Na przykład, jeśli zdefiniowano dwa 32-bitowe formaty kart, „Format A" i"Format B", a następnie włączono „Format A", nie można włączyć formatu „Format B" bez uprzedniego wyłączenia „Formatu A".
- Jeśli nie włączono formatów kart, do identyfikacji karty i udzielenia dostępu można użyć typów identyfikacji **Tylko dane karty** i **Tylko dane karty i PIN**. Nie jest to jednak zalecane, ponieważ różni producenci czytników lub ustawienia czytników mogą generować różne dane surowe karty.

Opisy formatu karty

- **Nazwa** (wymagana) – wprowadź nazwę opisową.
- **Opis** – wprowadź dodatkowe informacje według potrzeby. Informacje te są widoczne wyłącznie w oknach dialogowych **Edytuj format karty** i **Dodaj format karty**.
- **Liczba bitów** (wymagana) – wprowadź liczbę bitów formatu karty. Musi to być liczba pomiędzy 1 a 1 000 000 000.

Format karty

Ta funkcja jest przeznaczona wyłącznie dla zaawansowanych użytkowników. Natychmiast po włączeniu funkcji **Card format (Format karty)**:

- Jeśli używasz poświadczenia 37-bitowego, zostaje usunięte ostatnie 5 bitów.
- Jeśli używasz poświadczenia 64-bitowego (kod QR), zostaje usunięta pierwsza sekwencja 24-bitowa.

Do wyświetlenia poświadczeń można użyć danych przykładowych albo czytnika kart.

1. Wybierz kolejno opcje **Advanced (Zaawansowane)** > **Card format (Format karty)**.
2. Zapoznaj się z ostrzeżeniem i kliknij **I understand (Rozumiem)**, aby włączyć funkcję **Card format (Format karty)**.
3. Wybierz swój czytnik z menu rozwijanego **Reader data visualization (Wizualizacja danych czytnika)**.
4. Kliknij opcję **Get reader data (Pobierz dane czytnika)** lub **Use sample data (Użyj danych przykładowych)**, aby wygenerować dane wyjściowe karty. Zostaną one zastosowane do wszystkich posiadaczy kart w urządzeniu.
5. Włącz opcję **Trim reader data (Przytnij dane czytnika)**, aby usunąć końcowe bity z poświadczeń kart.
6. Kliknij przycisk **Włącz**.

Mapy pól

- **Name (Nazwa)** (wymagana) – wprowadź nazwę mapy pola bez spacji, na przykład `OddParity`. Przykłady często stosowanych map pól:
  - `Parity` – bity parzystości są wykorzystywane do wykrywania błędów. Bity parzystości są zwykle dodawane na początku lub na końcu ciągu kodu binarnego i wskazują, czy liczba bitów jest parzysta, czy nieparzysta.
  - `EvenParity` – bity parzystości zapewniają parzystą liczbę bitów w ciągu. Wliczane są bity o wartości 1. Jeśli ich liczba jest już parzysta, wartość bitu parzystości jest ustawiana na 0. Jeśli ich liczba jest nieparzysta, wartość bitu parzystości jest ustawiana na 1, co sprawia, że łączna liczba staje się liczbą parzystą.
  - `OddParity` – bity nieparzystości zapewniają nieparzystą liczbę bitów w ciągu. Wliczane są bity o wartości 1. Jeśli ich liczba jest już nieparzysta, wartość bitu nieparzystości jest ustawiana na 0. Jeśli liczba jest parzysta, wartość bitu nieparzystości jest ustawiana na 1, co sprawia, że łączna liczba staje się liczbą nieparzystą.
  - `FacilityCode` – kody obiektu są czasem wykorzystywane w celu zweryfikowania, czy token jest zgodny z partią danych uwierzytelniających użytkownika końcowego. W starszych systemach kontroli dostępu kod obiektu był wykorzystywany do walidacji danych o obniżonej wartości, umożliwiając dostęp do danych każdego pracownika w partii danych uwierzytelniających, które zakodowano odpowiadającym kodem obiektu. Ta nazwa mapy pola, w której wielkość liter ma znaczenie, jest wymagana dla produktu, aby możliwa była walidacja kodu obiektu.
  - `CardNr` – numer karty lub ID użytkownika są najczęściej poddawane walidacji w systemach kontroli dostępu. Ta nazwa mapy pola, w której wielkość liter ma znaczenie, jest wymagana dla produktu, aby możliwa była walidacja numeru karty.
  - `CardNrHex` – dane binarne numeru karty są zakodowane w produkcie w postaci liczb heksadecymalnych (małymi literami). Służą one przede wszystkim do rozwiązywania problemu w przypadku nieotrzymania oczekiwanego numeru karty z czytnika.
- **Range** (wymagane) – wprowadź zakres bitów dla mapy pola, na przykład 1, 2–17, 18–33 i 34.
- **Encoding** (wymagane) – wybierz rodzaj kodowania dla każdej mapy pola.
  - **BinLE2Int** – dane binarne są kodowane jako liczby całkowite z kolejnością bitów little endian. Liczba całkowita oznacza, że nie może to być ułamek. Kolejność bitów little endian oznacza kolejność, w której pierwszy bit jest najmniejszy (najmniej znaczący).
  - **BinBE2Int** – dane binarne są kodowane jako liczby całkowite z kolejnością bitów big endian. Liczba całkowita oznacza, że nie może to być ułamek. Kolejność bitów big endian oznacza kolejność, w której pierwszy bit jest największy (najistotniejszy).
  - **BinLE2Hex** – dane binarne są kodowane w postaci liczb heksadecymalnych (małymi literami) w kolejności little endian. System szesnastkowy, zwany również heksadecymalnym, składa się z 16 niepowtarzalnych znaków: cyfr od 0 do 9 oraz liter od a do f. Kolejność bitów little endian oznacza, że pierwszy bit jest najmniejszy (najmniej znaczący).
  - **BinBE2Hex** – dane binarne są kodowane w postaci liczb heksadecymalnych (małymi literami) z kolejnością bitów big endian. System szesnastkowy, zwany również heksadecymalnym, składa się z 16 niepowtarzalnych znaków: cyfr od 0 do 9 oraz liter od a do f. Kolejność bitów big endian oznacza, że pierwszy bit jest największy (najbardziej znaczący).
  - **BinLEIBO2Int** – dane binarne są kodowane w ten sam sposób, jak w przypadku BinLE2Int, ale dane nieprzetworzone z karty są odczytywane w odwróconej kolejności bitów w sekwencji wielobitowej przed wyodrębnieniem map pola w celu ich zakodowania.
  - **BinBEIBO2Int** – dane binarne są kodowane w podobny sposób, jak w przypadku BinBE2Int, ale dane nieprzetworzone z karty są odczytywane w odwróconej kolejności bitów w sekwencji wielobitowej przed wyodrębnieniem map pola w celu ich zakodowania.

Więcej informacji na temat tego, które mapy pól obsługuje dany format karty, można znaleźć w instrukcji producenta.

Konfiguracja usług

Opcja Skonfiguruj usługi na stronie Ustawienia służy do konfigurowania zewnętrznych usług dla kontrolera drzwi.

SmartIntego

SmartIntego to bezprzewodowe rozwiązanie zwiększające liczbę drzwi obsługiwanych przez kontroler drzwi.

Wymogi wstępne SmartIntego

Przed konfiguracją SmartIntego należy spełnić następujące wymogi wstępne:

- Należy utworzyć plik CSV. Plik CSV zawiera informacje o tym, które opcje GatewayNode i drzwi są używane w rozwiązaniu SmartIntego. Plik zostaje utworzony w autonomicznym oprogramowaniu dostarczonym przez partnera SimonsVoss.
- Jeśli przeprowadzono konfigurację sprzętową SmartIntego: *Tworzenie nowej konfiguracji sprzętowej zamków bezprzewodowych, on page 14*.

Uwaga

- Narzędzie do konfiguracji SmartIntego musi być w wersji 2.1.6452.23485, kompilacji 2.1.6452.23485 (8/31/2017 1:02:50 PM) lub nowszej.
- SmartIntego jest niekompatybilny z szyfrowaniem Advanced Encryption Standard (AES) i dlatego trzeba je wyłączyć w narzędziu do konfiguracji SmartIntego.

Informacje na temat konfiguracji SmartIntego

Uwaga

- Upewnij się, że spełniono podane wymogi wstępne.
- Aby stan akumulatora był lepiej widoczny, przejdź do menu **Ustawienia** > **Konfiguruj dzienniki zdarzeń i alarmów**, a następnie dodaj jako alarm opcje **Drzwi — alarm akumulatora** lub **IdPoint — alarm akumulatora**.
- Ustawienia monitorów drzwi pochodzą z zaimportowanego pliku CSV. W standardowej instalacji ustawienia tego nie trzeba zmieniać.

1. Kliknij przycisk **Przeglądaj...**, wybierz plik CSV i kliknij polecenie **Prześlij plik**.
2. Wybierz opcję GatewayNode i kliknij przycisk **Dalej**.
3. Zostanie wyświetlony podgląd nowej konfiguracji. W razie potrzeby wyłącz monitory drzwi.
4. Kliknij polecenie **Konfiguruj (Configure)**.
5. Zostanie wyświetlony podgląd drzwi w konfiguracji. Kliknij opcję **Ustawienia**, aby skonfigurować każde drzwi oddzielnie.

Informacje na temat ponownej konfiguracji SmartIntego

1. W menu górnym kliknij opcję **Ustawienia**.
2. Kliknij opcję **Konfiguracja usług** > **Ustawienia**.
3. Kliknij przycisk **Konfiguruj ponownie**.
4. Kliknij przycisk **Przeglądaj...**, wybierz plik CSV i kliknij polecenie **Prześlij plik**.
5. Wybierz opcję GatewayNode i kliknij przycisk **Dalej**.
6. Zostanie wyświetlony podgląd nowej konfiguracji. W razie potrzeby wyłącz monitory drzwi.

Uwaga

Ustawienia monitorów drzwi pochodzą z zaimportowanego pliku CSV. W standardowej instalacji ustawienia tego nie trzeba zmieniać.

7. Kliknij polecenie **Konfiguruj (Configure)**.
8. Zostanie wyświetlony podgląd drzwi w konfiguracji. Kliknij opcję **Ustawienia**, aby skonfigurować każde drzwi oddzielnie.

Profil LED OSDP

Można dostosować profile LED czytnika OSDP, aby zdefiniować sygnały świetlne i dźwiękowe wykorzystywane dla różnych zdarzeń. Pełną listę profili można znaleźć w sekcji *LED profiles (Profile LED)*.

Ustawianie poziomów światła i dźwięku

1. Przejdź do menu **Peripherals (Urządzenia peryferyjne)** > **Readers (Czytniki)** > **OSDP LED profile (Profil LED OSDP)**.
2. Rozwiń menu **Light and audio levels (Poziomy światła i dźwięku)**.
3. Wyreguluj jasność paska LED, podświetlenia LED oraz głośność za pomocą suwaka.
4. Kliknij przycisk **Save (Zapisz)**.

Uwaga

Po zmianie poziomów światła i dźwięku ustawienia te są aktualizowane dla wszystkich czytników podłączonych do kontrolera.

Testowanie ustawień LED czytnika OSDP:

Za pomocą menu **OSDP LED test (Test LED czytnika OSDP)** można sprawdzić ustawienia dźwięku i światła dla dowolnego profilu czytnika.

Aby przetestować ustawienia profili LED OSDP:

1. Przejdź do menu **Peripherals (Urządzenia peryferyjne)** > **Readers (Czytniki)** > **OSDP LED profile (Profil LED OSDP)**.
2. Rozwiń menu **OSDP LED test (Test LED OSDP)**.
3. Wybierz sygnalizację LED.
4. Wybierz czytnik, który chcesz przetestować.
5. Kliknij przycisk **Start (Rozpocznij)**.
6. Kliknij **Edit feedback (Edytuj sygnalizację)**, aby zmienić ustawienia światła i dźwięku dla swojego profilu.
   - Wybierz nowy kolor z menu rozwijanego **Color (Kolor)**.
   - W razie potrzeby wybierz częstotliwość dźwięku z menu rozwijanego **Audio**.
   - Można również zresetować ustawienia profilu, klikając opcję **Reset to default values (Przywróć wartości domyślne)**.
   - Kliknij przycisk **Save (Zapisz)**.

Zmiana ustawień profilu LED OSDP:

1. Przejdź do menu **Peripherals (Urządzenia peryferyjne)** > **Readers (Czytniki)** > **OSDP LED profile (Profil LED OSDP)**.
2. Przejdź do menu **OSDP LED profile (Profil LED OSDP)**.
3. Kliknij obok profilu, który chcesz zmienić.
4. Zmodyfikuj odpowiednie ustawienia:
   - Wybierz sposób działania diod LED z menu rozwijanego **Behavior (Zachowanie)**.
   - Wybierz kolor diod LED z menu rozwijanego **Color (Kolor)**.
   - Ustaw parametry **Duration on (Czas włączenia)** i **Duration off (Czas wyłączenia)** dla diod LED.

- Ustaw parametr **Recurrence (Powtarzanie)** dla diod LED.
- Z menu rozwijanego **Audio** wybierz parametry **Beep duration, on (Czas trwania sygnału dźwiękowego – włączony)** i **Beep duration, off (Czas trwania sygnału dźwiękowego – wyłączony)**, a następnie ustaw parametr **Recurrence (Powtarzanie)** dla sygnału dźwiękowego. Upewnij się, że parametry **Beep duration, on (Czas trwania sygnału dźwiękowego – włączony)** i **Beep duration, off (Czas trwania sygnału dźwiękowego – wyłączony)** mają taką samą wartość.

5. Kliknij przycisk **Save (Zapisz)**.

Importowanie istniejących ustawień z innego kontrolera

1. Przejdź do menu **Peripherals (Urządzenia peryferyjne)** > **Readers (Czytniki)** > **OSDP LED profile (Profil LED OSDP)**.
2. Kliknij **Import (Importuj)**.
3. Wybierz plik, który chcesz przesłać.
4. Kliknij **Import (Importuj)**.

Eksportowanie bieżących ustawień

1. Przejdź do menu **Peripherals (Urządzenia peryferyjne)** > **Readers (Czytniki)** > **OSDP LED profile (Profil LED OSDP)**.
2. Kliknij **Export (Eksportuj)**.
3. Wybierz lokalizację, w której chcesz zapisać plik json, i kliknij **Save (Zapisz)**.

Instrukcje konserwacji

Aby system kontroli dostępu działał poprawnie, firma Axis zaleca regularną konserwację systemu, w tym kontrolerów drzwi i podłączonych urządzeń.

Konserwację należy przeprowadzać przynajmniej raz w roku. Sugerowana procedura konserwacji obejmuje, ale nie ogranicza się do następujących kroków:

- Upewnij się, że wszystkie połączenia między kontrolerem drzwi a urządzeniami zewnętrznymi są zabezpieczone.
- Sprawdź wszystkie połączenia sprzętowe. Zob. *Zarządzanie weryfikacją drzwi, on page 16*.
- Sprawdź, czy system, w tym podłączone urządzenia zewnętrzne, działa poprawnie.

– Przeciągnij kartę i przetestuj czytniki, drzwi i zamki.

– Jeśli system zawiera urządzenia REX, czujniki lub inne urządzenia, również należy je przetestować.

– Jeśli alarm przeciwsabotażowy jest włączony, sprawdź go.

Jeśli w wyniku powyższych sprawdzeń stwierdzona zostanie awaria lub nieprzewidziane zachowanie:

– Sprawdź sygnały przewodów za pomocą odpowiedniego sprzętu i sprawdź, czy przewody lub kable nie są w jakikolwiek sposób uszkodzone.

– Wymień wszystkie uszkodzone lub wadliwe kable i przewody.

– Po wymianie kabli i przewodów sprawdź ponownie wszystkie połączenia sprzętowe. Zob. *Zarządzanie weryfikacją drzwi, on page 16*.

- Jeśli kontroler drzwi nie działa zgodnie z oczekiwaniami, więcej informacji możesz znaleźć w *Rozwiązywanie problemów, on page 37* i *Konserwacja, on page 34*.

Konfiguracja zdarzeń

Zdarzenia zachodzące w systemie, na przykład kiedy użytkownik przeciągnie kartę lub kiedy aktywuje się urządzenie REX, są rejestrowane w dzienniku zdarzeń.

- Wyświetlanie dziennika zdarzeń. Zob. *page 23*.
- Eksportowanie dziennika zdarzeń. Zob. .
- Konfigurowanie dziennika zdarzeń. Zob. *Konfigurowanie dziennika zdarzeń, on page 23*.

Wyświetlanie dziennika zdarzeń

Aby wyświetlić zarejestrowane zdarzenia, przejdź do opcji **Dziennik zdarzeń**.

Aby rozwinąć element w dzienniku zdarzeń i wyświetlić szczegóły zdarzeń, kliknij ▶.

Zastosowanie filtrów do dziennika zdarzeń ułatwia znalezienie określonych zdarzeń. Aby odfiltrować listę, wybierz jeden lub kilka filtrów zdarzeń i kliknij przycisk **Zastosuj filtry**. Aby uzyskać dodatkowe informacje, zob. *Filtry dziennika zdarzeń, on page 23*.

Jako administrator możesz bardziej interesować się szczególnymi typami zdarzeń. Możesz więc wybrać, które zdarzenia mają być rejestrowane. Aby uzyskać dodatkowe informacje, zob. *Opcje dziennika zdarzeń, on page 23*.

Filtry dziennika zdarzeń

Możesz zawęzić zakres dziennika zdarzeń, wybierając co najmniej jeden z następujących filtrów:

- Użytkownik – filtruje zdarzenia związane z wybranym użytkownikiem.
- Drzwi i piętro – filtruje zdarzenia związane z konkretnymi drzwiami lub piętrem.
- Temat – filtruje typy zdarzeń.
- Data i godzina – filtruje dziennik zdarzeń według przedziału dat i czasu.

Konfigurowanie dziennika zdarzeń

Strona Konfiguruj dziennik zdarzeń umożliwia określenie zdarzeń, które będą rejestrowane w dzienniku.

Opcje dziennika zdarzeń

By zdefiniować, jakie zdarzenia powinny znaleźć się w dzienniku zdarzeń, przejdź do menu **Ustawienia > Skonfiguruj dzienniki zdarzeń**.

Dostępne są następujące opcje rejestrowania zdarzeń:

- **Brak rejestracji** – wyłącz rejestrowanie zdarzeń. Zdarzenie nie zostanie zarejestrowane ani włączone do dziennika zdarzeń.
- **Rejestruj dla wszystkich źródeł** – włącz rejestrowanie zdarzeń. Zdarzenie zostanie zarejestrowane i uwzględnione w dzienniku zdarzeń.

Konfigurowanie reguł akcji

Na stronach zdarzeń można skonfigurować produkt Axis tak, aby wykonywał akcje po wystąpieniu różnych zdarzeń. Zestaw warunków określających, w jaki sposób i kiedy wyzwalana jest akcja, nazywamy regułą akcji. Jeśli określono wiele warunków, to do wyzwolenia działania konieczne jest spełnienie wszystkich z nich.

Więcej informacji dotyczących dostępnych wyzwalaczy i akcji znajduje się we wbudowanej pomocy produktu.

W poniższym przykładzie opisano, jak skonfigurować regułę akcji, aby po otwarciu drzwi siłą został aktywowany port wyjścia.

1. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Porty i urządzenia > Porty I/O**.

2. Wybierz **Wyjście** z listy rozwijanej **Typ portu I/O** i wprowadź nazwę w polu **Nazwa**.
3. Wybierz **Stan normalny** portu I/O i kliknij przycisk **Zapisz**.
4. Przejdź do menu **Zdarzenia > Reguły akcji** i kliknij przycisk **Dodaj**.
5. Z listy rozwijanej **Wyzwalacz** wybierz opcję **Drzwi**.
6. Wybierz **Alarm drzwi** z listy rozwijanej.
7. Wybierz żądane drzwi z listy rozwijanej.
8. Wybierz **DrzwiOtwarteSiłą** z listy rozwijanej.
9. Możesz opcjonalnie wybrać **Harmonogram** i **Dodatkowe warunki**. Szczegółowe informacje można znaleźć poniżej.
10. W poleceniu **Akcje** wybierz opcję **Port wyjścia** z listy rozwijanej **Typ**.
11. Wybierz żądany port wyjścia z listy rozwijanej **Port**.
12. Ustaw stan jako **Aktywne**.
13. Wybierz **Czas trwania** i wartość **Przejdź do przeciwnego stanu po**. Wprowadź żądany czas trwania akcji.
14. Kliknij **OK**.

Aby użyć więcej niż jednego wyzwalacza dla reguły akcji, wybierz opcję **Dodatkowe warunki** i kliknij przycisk **Dodaj**, aby dodać dodatkowe wyzwalacze. Jeśli określono wiele warunków, to do wyzwolenia akcji konieczne jest spełnienie wszystkich z nich.

Aby zapobiec wielokrotnemu wyzwalaniu akcji, możesz ustawić wartość opcji **Odczekaj przynajmniej**. Wprowadź w godzinach, minutach i sekundach czas, podczas którego wyzwalacz powinien zostać zignorowany przed ponowną aktywacją reguły akcji.

Więcej informacji znajduje się we wbudowanej pomocy produktu.

Dodawanie odbiorców

Produkt może wysyłać wiadomości w celu powiadamiania odbiorców o zdarzeniach i alarmach. Aby produkt mógł wysyłać powiadomienia, trzeba zdefiniować co najmniej jednego odbiorcę. Więcej informacji na temat dostępnych opcji: .

Aby dodać odbiorcę:

1. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Zdarzenia > Odbiorcy** i kliknij przycisk **Dodaj**.
2. Wprowadź nazwę opisową.
3. Wybierz **Typ** odbiorcy.
4. Wprowadź informacje potrzebne w przypadku danego typu odbiorcy.
5. Kliknij przycisk **Test**, aby przetestować połączenie z odbiorcą.
6. Kliknij **OK**.

Konfiguracja odbiorców wiadomości e-mail

Adresatów wiadomości e-mail można skonfigurować, wybierając jednego z wymienionych dostawców poczty e-mail lub określając serwer SMTP, port i metodę uwierzytelnienia używane na przykład przez firmowy serwer poczty e-mail.

Uwaga

Niektórzy dostawcy usług poczty elektronicznej stosują filtry bezpieczeństwa, uniemożliwiające odbiór lub przeglądanie dużych załączników, odbieranie wiadomości cyklicznych itp. Sprawdź zasady zabezpieczeń dostawcy poczty elektronicznej, aby uniknąć problemów z dostarczaniem e-maili i zablokowania konta.

Aby skonfigurować adresata wiadomości e-mail przy użyciu jednego z wymienionych dostawców:

1. Przejdź do menu **Zdarzenia > Odbiorcy** i kliknij przycisk **Dodaj**.

2. Wprowadź **Nazwę** i wybierz **E-mail** z listy **Typ**.
3. Wprowadź adresy e-mail, na które chcesz wysłać e-maile, w polu **Do**. Aby wprowadzić wiele adresów e-mail, oddziel je przecinkami.
4. Wybierz dostawcę poczty elektronicznej z listy **Dostawca**.
5. Wprowadź identyfikator użytkownika i hasło do konta e-mail.
6. Kliknij przycisk **Testuj**, aby wysłać testową wiadomość e-mail.

Aby skonfigurować adresata wiadomości e-mail przy użyciu na przykład firmowego serwera poczty e-mail, postępuj zgodnie z instrukcjami powyżej, ale wybierz **Użytkownik zdefiniowany** jako **Dostawca**. Wprowadź adres e-mail, który ma być wyświetlany jako adres nadawcy w polu **Od**. Wybierz **Ustawienia zaawansowane** i podaj adres serwera SMTP, port i metodę uwierzytelniania. Opcjonalnie wybierz opcję **Użyj szyfrowania**, aby wysyłać wiadomości e-mail przez połączenie szyfrowane. Certyfikat serwera można sprawdzić za pomocą certyfikatów dostępnych w produkcie Axis. Informacje na temat przesyłania certyfikatów: *Certyfikaty, on page 28*.

Jak stworzyć harmonogram

Harmonogramów można użyć jako dodatkowego warunku wyzwalania reguł akcji. Użyj jednego ze wstępnie zdefiniowanych harmonogramów lub utwórz nowy harmonogram zgodnie z opisem poniżej.

Aby utworzyć nowy harmonogram:

1. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Zdarzenia > Harmonogramy** i kliknij przycisk **Dodaj**.
2. Wprowadź nazwę opisową oraz informacje niezbędne w przypadku harmonogramu dziennego, tygodniowego, miesięcznego lub rocznego.
3. Kliknij **OK**.

Aby użyć harmonogramu w reguła akcji, wybierz harmonogram z listy rozwijanej **Harmonogram** na stronie Konfiguracja reguł akcji.

Konfiguracja powtórzeń

Powtórzenia służą do powtarzania wyzwalania reguł akcji, na przykład co pięć minut lub co godzinę.

Konfigurowanie powtórzenia:

1. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Zdarzenia > Powtórzenia** i kliknij przycisk **Dodaj**.
2. Wprowadź nazwę opisową i wzorzec powtórzenia.
3. Kliknij **OK**.

Aby użyć powtórzenia w regule akcji, wybierz najpierw opcje **Godzina** na liście rozwijanej **Wyzwalacz** na stronie Konfiguracja reguł akcji, a następnie wybierz powtórzenie z listy rozwijanej.

Aby zmodyfikować lub zmienić powtórzenie, wybierz je z listy **Lista powtórzeń** i kliknij przycisk **Zmień** lub **Usuń**.

Informacje zwrotne z czytnika

Czytniki używają diod LED i sygnałów dźwiękowych do przekazywania informacji zwrotnych użytkownikom (osobom uzyskującym lub próbującym uzyskać dostęp do drzwi). Kontroler drzwi może wyzwolić kilka komunikatów zwrotnych, a niektóre z nich są wstępnie skonfigurowane w kontrolerze drzwi i obsługiwane przez większość czytników.

Czytniki mają różne konfiguracje działania diod LED, ale zazwyczaj korzystają z różnych sekwencji stałego i migającego czerwonego, zielonego i bursztynowego światła.

Czytniki mogą również wykorzystywać sygnały dźwiękowe do przesyłania komunikatów, używając różnych sekwencji krótszych i dłuższych sygnałów.

Poniższa tabela zawiera zdarzenia wstępnie skonfigurowane w kontrolerze drzwi tak, aby wyzwolić komunikat zwrotny z czytnika i typowy sygnał informacji zwrotnej. Sygnały zwrotne czytników AXIS znajdują się w Instrukcji instalacji dostarczonej z czytnikiem AXIS.

Zdarzenie	Wiegand podwójna dioda LED	Wiegand pojedyncza dioda LED	OSDP	Wzorzec sygnału dźwiękowego	Stan
Oczekiwanie[1]	Wył.	Czerwony	Czerwony	Bez dźwięku	Normalny
WymagajPIN	Migający czerwony/ zielony	Migający czerwony/ zielony	Migający czerwony/ zielony	Dwa krótkie sygnały	Wymagany PIN
Przyznanodos-tęp	Zielony	Zielony	Zielony	Beep (Sygnał dźwiękowy)	Przyznano dostęp
Odmowadostę-pu	Czerwony	Czerwony	Czerwony	Beep (Sygnał dźwiękowy)	Odmowa dostępu

Komunikaty zwrotne inne niż wymienione powyżej należy skonfigurować przez klienta, na przykład system zarządzania dostępem, interfejs oprogramowania VAPIX® obsługujący tę funkcję i pracujący z czytnikami, które mogą dostarczyć wymagany sygnał. Więcej informacji znajduje się w informacjach o użytkownikach dostarczonych przez deweloperów systemu zarządzania dostępem i producenta czytnika.

1. *Stan bezczynności rozpoczyna się po zamknięciu drzwi i zablokowaniu zamka.*

Opcje systemu

Bezpieczeństwo

Użytkownicy

Kontrola dostępu użytkowników jest domyślnie włączona i można ją skonfigurować w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Zabezpieczenia > Użytkownicy**. Administrator może skonfigurować innych użytkowników, nadając im nazwy użytkowników i przydzielając hasła.

Lista użytkowników zawiera autoryzowanych użytkowników i grupy użytkowników (poziomy dostępu):

- **Administratorzy** mają nieograniczony dostęp do wszystkich ustawień. Administrator może dodawać, modyfikować i usuwać innych użytkowników.

Uwaga

Należy pamiętać, że po wybraniu opcji **Zaszyfrowane i niezaszyfrowane**, serwer WWW zaszyfruje hasło. Jest to domyślna opcja dla nowego urządzenia lub urządzenia zresetowanego do domyślnych ustawień fabrycznych.

W opcji **Ustawienia hasła HTTP/RTSP** wybierz typ dozwolonego hasła. Może być konieczne zezwolenie na używanie niezaszyfrowanych haseł, jeśli istnieją klienty, które nie obsługują szyfrowania, lub jeśli zaktualizowano oprogramowanie sprzętowe, a istniejące klienty obsługują szyfrowanie, ale konieczne jest ponowne zalogowanie i konfiguracja, aby można było użyć tej funkcji.

ONVIF

ONVIF to otwarte forum branżowe zapewniające i promujące standardowe interfejsy zapewniające skuteczne współdziałanie produktów bezpieczeństwa fizycznego opartych na protokole IP.

Utworzenie użytkownika powoduje automatyczne włączenie komunikacji ONVIF. Nazwy użytkownika i hasła należy używać podczas komunikacji ONVIF z urządzeniem. Więcej informacji znajduje się na stronie *www.onvif.org*

Filtr adresów IP

Filtrowanie adresów IP można włączyć w menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Security (Zabezpieczenia) > IP Address Filter (Filtr adresów IP)**. Po włączeniu tej funkcji adresy IP z listy mogą uzyskać dostęp do produktu Axis (lub otrzymać komunikat odmowy dostępu). Wybierz opcję **Zezwalaj** lub **Odmów** z listy i kliknij przycisk **Zastosuj**, aby włączyć filtrowanie adresów IP.

Administrator może dodać maksymalnie 256 adresów IP do listy (jeden wpis może zawierać wiele adresów IP).

HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer lub HTTP over SSL) to protokół sieciowy zapewniający szyfrowane przeglądanie. Protokół HTTPS może być również używany przez użytkowników i klienty w celu sprawdzenia, czy uzyskiwany jest dostęp do właściwego urządzenia. Poziom bezpieczeństwa zapewniany przez HTTPS jest uważany za odpowiedni dla większości komercyjnych wymian danych.

Produkt Axis można skonfigurować tak, aby wymagał protokołu HTTPS podczas logowania administratora.

Aby móc korzystać z protokołu HTTPS, najpierw trzeba zainstalować certyfikat HTTPS. Przejdź do menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Security (Zabezpieczenia) > Certificates (Certyfikaty)**. Zob. *Certyfikaty, on page 28*.

Aby włączyć HTTPS w produkcie Axis:

1. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Zabezpieczenia > HTTPS**.
2. Wybierz certyfikat HTTPS z listy zainstalowanych certyfikatów.

3. Możesz również kliknąć opcję **Szyfr** i wybrać algorytmy szyfrowania dla SSL.
4. Ustaw **Zasady połączenia HTTPS** dla różnych grup użytkowników.
5. Kliknij **Save (Zapisz)**, aby włączyć ustawienia.

Aby uzyskać dostęp do produktu Axis za pośrednictwem pożądanego protokołu, w polu adresu przeglądarki wpisz `https://` dla protokołu HTTPS i `http://` dla protokołu HTTP.

Port HTTPS można zmienić na stronie **Opcje systemu > Sieć >TCP/IP > Zaawansowane**.

IEEE 802.1X

IEEE 802.1X to standard 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 być uwierzytelnione. Do uwierzytelnienia służy serwer, zazwyczaj **RADIUS**, taki jak FreeRADIUS i Microsoft Internet Authentication Server.

W instalacjach firmy Axis urządzenia Axis i serwer uwierzytelniający używają do identyfikacji certyfikatów cyfrowych z użyciem EAP-TLS (Extensible Authentication Protocol - Transport Layer Security). Certyfikaty są dostarczane przez **jednostkę certyfikującą** (CA). Potrzebujesz:

- certyfikatu CA w celu uwierzytelnienia serwera uwierzytelniania;
- certyfikatu klienta podpisanego przez CA w celu uwierzytelnienia produktu Axis.

Aby utworzyć i zainstalować certyfikaty, przejdź do menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Security (Zabezpieczenia) > Certificates (Certyfikaty)**. Zob. *Certyfikaty, on page 28*.

Aby umożliwić produktowi dostęp do sieci chronionej przez IEEE 802.1X:

1. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Zabezpieczenia > IEEE 802.1X**.
2. Wybierz **Certyfikat CA** i **Certyfikat klienta** z list zainstalowanych certyfikatów.
3. W opcji **Ustawienia** wybierz wersję EAPOL i podaj tożsamość EAP powiązaną z certyfikatem klienta.
4. Zaznacz to pole, aby włączyć IEEE 802.1X i kliknij przycisk **Zapisz**.

Uwaga

Aby uwierzytelnianie działało prawidłowo, ustawienia daty i godziny w produkcie Axis powinny być zsynchronizowane z serwerem NTP. Zob. .

Certyfikaty

Certyfikaty służą do uwierzytelniania urządzeń w sieci. Typowe zastosowania certyfikatów obejmują szyfrowane przeglądanie stron internetowych (HTTPS), ochronę sieci za pośrednictwem IEEE 802.1X i wysyłanie powiadomień, na przykład pocztą e-mail. Urządzenia Axis mogą używać dwóch rodzajów certyfikatów:

Certyfikaty serwera/klienta – Służą do uwierzytelniania produktów Axis. Certyfikat **serwera/klienta** 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 te służą do uwierzytelniania innych certyfikatów, na przykład certyfikatu serwera uwierzytelniającego w przypadku podłączenia urządzenia Axis do sieci zabezpieczonej IEEE 802.1X. Urządzenia Axis mają kilka zainstalowanych wstępnie certyfikatów CA.

Uwaga

- Po przywróceniu fabrycznych ustawień domyślnych urządzenia usuwane są wszystkie certyfikaty, poza zainstalowanymi wstępnie certyfikatami CA.
- Po przywróceniu fabrycznych ustawień domyślnych urządzenia wstępnie zainstalowane certyfikaty CA, które usunięto, zostaną zainstalowane ponownie.

Tworzenie certyfikatu z własnym podpisem

1. Przejdź do menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Security (Zabezpieczenia) > Certificates (Certyfikaty)**.
2. Kliknij przycisk **Utwórz certyfikat z własnym podpisem** i podaj wymagane informacje.

Tworzenie i instalowanie certyfikatu z podpisem CA

1. Tworzenie certyfikatu z podpisem własnym: *Tworzenie certyfikatu z własnym podpisem, on page 29*.
2. Przejdź do menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Security (Zabezpieczenia) > Certificates (Certyfikaty)**.
3. Kliknij przycisk **Utwórz żądanie podpisania certyfikatu** i podaj wymagane informacje.
4. Skopiuj żądanie w formacie PEM i wyślij do wybranego organu certyfikującego (CA).
5. Po otrzymaniu podpisanego certyfikatu kliknij przycisk **Zainstaluj certyfikat** i wczytaj certyfikat.

Instalowanie dodatkowych certyfikatów CA

1. Przejdź do menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Security (Zabezpieczenia) > Certificates (Certyfikaty)**.
2. Kliknij polecenie **Instaluj certyfikat** i wczytaj certyfikat.

Sieć

Podstawowe ustawienia TCP/IP

Produkt Axis obsługuje wersję 4 IP (IPv4) i wersję 6 IP (IPv6).

Produkt Axis może uzyskać adres IP na następujące sposoby:

- **Dynamiczny adres IP** – domyślnie wybraną opcją jest **Uzyskaj adres IP przez DHCP**. Oznacza to, że produkt Axis jest ustawiony tak, aby uzyskiwać adres IP automatycznie za pośrednictwem protokołu Dynamic Host Configuration Protocol (DHCP).
  DHCP pozwala administratorom sieci zarządzać centralnie adresami IP i automatyzować ich przypisywanie.
- **Statyczny adres IP** – aby użyć statycznego adresu IP, wybierz opcję **Użyj następującego adresu IP** i podaj adres IP, maskę podsieci i domyślny router. Następnie kliknij przycisk **Zapisz**.

DHCP należy włączać tylko w razie używania powiadomień dynamicznych adresów IP lub wtedy, gdy DHCP może aktualizować serwer DNS, co umożliwia dostęp do produktu Axis według nazwy (nazwy hosta).

Jeśli włączono DHCP i nie można uzyskać dostępu do produktu, należy uruchomić narzędzie AXIS IP Utility, aby wyszukać w sieci podłączone produkty Axis, lub zresetować produkt do domyślnych ustawień fabrycznych, a następnie wykonać ponowną instalację. Informacje dotyczące przywracania domyślnych ustawień fabrycznych: *page 37*.

AXIS Video Hosting System (AVHS)

System AVHS w połączeniu z usługą AVHS zapewnia łatwe i bezpieczne połączenie z internetem w celu zarządzania kontrolerami i dziennikami z dowolnej lokalizacji. Aby uzyskać więcej informacji znaleźć lokalnego dostawcę usług AVHS, odwiedź stronę www.axis.com/hosting

Ustawienia AVHS można skonfigurować w menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Network (Sieć) > TCP/IP > Basic (Podstawowe)**. Możliwość połączenia z usługą AVHS jest włączona domyślnie. Aby ją wyłączyć, wyczyść pole **Włącz AVHS**.

Włączona obsługa jednym kliknięciem – Naciśnij i przytrzymaj przycisk Control produktu (zob. *Przegląd produktów, on page 6*) przez około 3 sekundy, aby połączyć się z usługą AVHS przez Internet. Po rejestracji funkcja **Zawsze** będzie włączona, a produkt Axis pozostanie podłączony do usługi AVHS. Jeśli produkt nie zostanie zarejestrowany w ciągu 24 godzin od naciśnięcia przycisku, produkt zostanie odłączony od usługi AVHS.

Zawsze – Produkt Axis stale próbuje połączyć się z usługą AVHS przez internet. Po zarejestrowaniu produkt pozostanie podłączony do usługi. Ta opcja może być używana, gdy produkt jest już zainstalowany i nie można korzystać z instalacji jednym kliknięciem lub jest to niewygodne.

Uwaga

Wsparcie AVHS zależy od dostępności subskrypcji od usługodawców.

Usługa AXIS Internet Dynamic DNS Service

Usługa AXIS Internet Dynamic DNS Service przypisuje nazwę hosta, aby umożliwić łatwy dostęp do produktu. Więcej informacji: *www.axiscam.net*

Aby zarejestrować produkt Axis w usłudze AXIS Internet Dynamic DNS Service, przejdź do menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Network (Sieć) > TCP/IP > Basic (Podstawowe)**. W menu **Usługi** kliknij przycisk **Ustawienia** usługi AXIS Internet Dynamic DNS Service (wymaga dostępu do Internetu). Nazwę domeny zarejestrowaną aktualnie w usłudze AXIS Internet Dynamic DNS Service dla danego produktu można w dowolnym momencie usunąć.

Uwaga

Usługa AXIS Internet Dynamic DNS Service wymaga protokołu IPv4.

Zaawansowane ustawienia TCP/IP

Konfiguracja DNS

Usługa DNS (Domain Name Service) zapewnia tłumaczenie nazw hostów na adresy IP. Ustawienia DNS można skonfigurować w menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Network (Sieć) > TCP/IP > Advanced (Zaawansowane)**.

Wybierz polecenie **Uzyskaj adres serwera DNS za pośrednictwem DHCP**, aby wykorzystać ustawienia DNS dostarczone przez serwer DHCP.

Aby wprowadzić ustawienia ręczne, wybierz **Użyj następującego adresu serwera DNS** i określ następujące ustawienia:

Nazwa domeny – Wprowadź domenę (domeny), aby wyszukać nazwę hosta używaną przez produkt Axis. Nazwy domen można oddzielić średnikami. Nazwa hosta jest zawsze pierwszą częścią pełnej nazwy domeny, na przykład `myserver` to nazwa hosta w pełnej nazwie domeny `myserver.mycompany.com`, gdzie `mycompany.com` jest nazwą domeny.

Podstawowy/dodatkowy serwer DNS – Wprowadź adresy IP podstawowego i dodatkowego serwera DNS. Dodatkowy serwer DNS jest opcjonalny i będzie używany, jeśli podstawowy jest niedostępny.

Konfiguracja NTP

Protokół NTP (Network Time Protocol) służy do synchronizacji czasu zegarów urządzeń w sieci. Ustawienia NTP można skonfigurować w menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Network (Sieć) > TCP/IP > Advanced (Zaawansowane)**.

Wybierz polecenie **Uzyskaj adres serwera NTP za pośrednictwem DHCP**, aby wykorzystać ustawienia NTP dostarczone przez serwer DHCP.

Aby wprowadzić ustawienia ręczne, wybierz opcję **Użyj następującego adresu serwera NTP** i wprowadź nazwę hosta lub adres IP serwera NTP.

Konfiguracja nazwy hosta

Dostęp do produktu Axis można uzyskać przy użyciu nazwy hosta zamiast adresu IP. Nazwa hosta jest zwykle taka sama jak przypisana nazwa DNS. Nazwę hosta można skonfigurować w menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Network (Sieć) > TCP/IP > Advanced (Zaawansowane)**.

Wybierz opcję **Uzyskaj nazwę hosta za pośrednictwem IPv4 DHCP**, aby używać nazwy hosta dostarczonej przez serwer DHCP bazujący na protokole IPv4.

Wybierz opcję **Użyj nazwy hosta**, aby ręcznie ustawić nazwę hosta.

Wybierz opcję **Włącz dynamiczne aktualizacje DNS**, aby dynamicznie aktualizować lokalne serwery DNS za każdym razem, gdy zmienia się adres IP produktu Axis. Więcej informacji można znaleźć w pomocy online.

Adres IPv4 lokalnego powiązania

Adres lokalnego powiązania jest domyślnie włączony i powoduje przypisanie produktowi Axis dodatkowego adresu IP, który może służyć do dostępu do produktu z innych hostów należących do tego samego segmentu sieci lokalnej. Produkt może mieć równocześnie adres IP lokalnego powiązania oraz adres statyczny i dynamiczny (DHCP).

Funkcję tę można wyłączyć w menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Network (Sieć) > TCP/IP > Advanced (Zaawansowane)**.

HTTP

Port HTTP używany przez produkt Axis można zmienić w menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Network (Sieć) > TCP/IP > Advanced (Zaawansowane)**. Oprócz ustawienia domyślnego (czyli 80) można używać dowolnego portu w zakresie 1024–65535.

HTTPS

Numer portu HTTPS używanego przez produkt Axis można zmienić w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Zaawansowane**. Oprócz ustawienia domyślnego (czyli 443) można używać dowolnego portu w zakresie 1024–65535.

Aby włączyć HTTPS, przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Zabezpieczenia > HTTPS**. Aby uzyskać dodatkowe informacje, zob. *HTTPS, on page 27*.

NAT traversal (mapowanie portów) dla IPv4.

Router sieciowy umożliwia urządzeniom w sieci prywatnej (LAN) współdzielić jedno połączenie internetowe. Odbywa się to poprzez przekazanie ruchu sieciowego z sieci prywatnej „na zewnątrz", czyli do internetu. Bezpieczeństwo w sieci prywatnej (LAN) jest większe, ponieważ większość routerów jest wstępnie skonfigurowana tak, aby zatrzymać próby uzyskania dostępu do sieci prywatnej (LAN) z sieci publicznej (internetu).

Użyj opcji **NAT traversal**, gdy produkt Axis jest podłączony do intranetu (LAN) i chcesz go udostępnić po drugiej stronie (WAN) routera NAT. Po prawidłowym skonfigurowaniu NAT traversal cały ruch HTTP do zewnętrznego portu HTTP w routerze NAT jest przekazywany do produktu.

Ustawienia NAT traversal można skonfigurować w menu **Setup (Ustawienia)> Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Network (Sieć) > TCP/IP > Advanced (Zaawansowane)**.

Uwaga

- Aby ta funkcja działała, produkt musi obsługiwać NAT traversal. Router musi również obsługiwać protokół UPnP®.
- W tym kontekście router oznacza dowolne urządzenie działające jako router sieciowy, takie jak router NAT, router sieciowy, bramka internetowa, router szerokopasmowy, urządzenie do udostępniania szerokopasmowego lub oprogramowanie, takie jak zapora.

Włącz/Wyłącz – Po włączeniu produkt Axis próbuje skonfigurować mapowanie portów w routerze NAT w sieci przy użyciu UPnP. Protokół UPnP musi być włączony w produkcie — zob. **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Network (Sieć) > UPnP**.

Korzystanie z ręcznie wybranego routera NAT – Wybierz tę opcję, aby ręcznie wybrać router NAT i wprowadź w polu adres IP routera. Jeśli nie zostanie określony router, urządzenie automatycznie wyszuka routery NAT w sieci. Jeśli zostanie wykryty więcej niż jeden router, wybrany zostanie domyślny router.

Alternatywny port HTTP – Wybierz tę opcję, aby ręcznie zdefiniować zewnętrzny port HTTP. Wprowadź numer portu z zakresu 1024–65535. Jeśli pole portu jest puste lub zawiera ustawienie domyślne, czyli 0, numer portu jest wybierany automatycznie po włączeniu NAT traversal.

Uwaga

- Alternatywny port HTTP może być używany lub aktywny, nawet wtedy, gdy opcja NAT traversal jest wyłączona. Jest to przydatne wtedy, gry router NAT nie obsługuje UPnP i trzeba ręcznie skonfigurować przekazywanie portów w routerze NAT.
- Jeśli spróbujesz ręcznie wprowadzić port, który jest już w użyciu, automatycznie wybrany zostanie inny dostępny port.
- Automatycznie wybrany port jest wyświetlany w tym polu. Aby to zmienić, wprowadź nowy numer portu i kliknij przycisk **Zapisz**.

FTP

Serwer FTP działający w produkcie Axis umożliwia przesyłanie nowego oprogramowania sprzętowego, aplikacji użytkownika itp. Serwer FTP można wyłączyć w menu **Setup (Ustawienia)> Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Network (Sieć) > TCP/IP > Advanced (Zaawansowane)**.

RTSP

Serwer RTSP produktu Axis umożliwia podłączającemu się klientowi przesyłanie zdarzeń strumieniowo. Numer portu RTSP można zmienić w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Zaawansowane**. Domyślny port to 554.

Uwaga

Przesyłanie zdarzeń strumieniowo nie będzie dostępne, jeśli serwer RTSP zostanie wyłączony.

SOCKS

SOCKS to protokół sieciowy serwera proxy. Produkt Axis można skonfigurować tak, do dostępu do sieci po drugiej stronie zapory lub serwera proxy używał serwera SOCKS. Funkcja ta jest przydatna, jeśli produkt Axis znajduje się w sieci lokalnej za zaporą, a do miejsca przeznaczenia spoza sieci lokalnej (na przykład internetu) konieczne jest przesyłanie powiadomień, plików, alarmów itp.

SOCKS konfiguruje się w menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Network (Sieć) > SOCKS**. Więcej informacji można znaleźć w pomocy online.

QoS (Quality of Service)

Protokół QoS (Quality of Service) gwarantuje określony poziom konkretnego zasobu na potrzeby wybranego ruchu w sieci. Sieć obsługująca protokół QoS nadaje priorytet ruchowi w sieci i zapewnia większą niezawodność dzięki kontrolowaniu przepustowości, jaką może wykorzystywać aplikacja.

Ustawienia QoS można skonfigurować w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > QoS**. Korzystając z wartości DSCP (Differentiated Services Codepoint), produkt Axis może oznaczać ruch związany ze zdarzeniem/alarmem i ruch związany z zarządzaniem.

SNMP

Protokół zarządzania urządzeniami sieciowymi Simple Network Management Protocol (SNMP) umożliwia zdalne zarządzanie urządzeniami sieciowymi. Społeczność SNMP to grupa urządzeń i stacja zarządzająca protokołem SNMP. Do identyfikacji grup używa się nazw społeczności.

Aby włączyć i skonfigurować SNMP w produkcie Axis, przejdź do strony **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Network (Sieć) > SNMP**.

Zależnie od wymaganego poziomu bezpieczeństwa wybierz wersję SNMP, której chcesz użyć.

Pułapki są wykorzystywane przez produkt Axis, aby wysyłać do systemu zarządzania komunikaty dotyczące ważnych zdarzeń i zmian stanu. Zaznacz pole **Włącz pułapki** i wprowadź adres IP lokalizacji, do której ma zostać przesłany komunikat pułapki oraz **Społeczność pułapki**, która powinna otrzymać komunikat.

Uwaga

Jeśli włączono HTTPS, SNMP v1 i SNMP v2c należy wyłączyć.

Pułapki dla SNMP v1/v2 są wykorzystywane przez produkt Axis, aby wysyłać do systemu zarządzania komunikaty dotyczące ważnych zdarzeń i zmian stanu. Zaznacz pole **Włącz pułapki** i wprowadź adres IP lokalizacji, do której ma zostać przesłany komunikat pułapki oraz **Społeczność pułapki**, która powinna otrzymać komunikat.

Dostępne są następujące pułapki:

- Zimny rozruch
- Ciepły rozruch
- Powiąż
- Uwierzytelnianie nie powiodło się

SNMP v3 zapewnia szyfrowanie i bezpieczne hasła. Aby można było korzystać z pułapek z SNMP v3, wymagana jest aplikacja do zarządzania SNMP v3.

Aby można było korzystać z SNMP v3, należy włączyć HTTPS — zob. *HTTPS, on page 27*. Aby włączyć SNMP v3, zaznacz pole i wprowadź wstępne hasło użytkownika.

Uwaga

Wstępne hasło można ustawić tylko raz. W przypadku utraty hasła produkt Axis należy zresetować do domyślnych ustawień fabrycznych — zob. *Przywracanie domyślnych ustawień fabrycznych, on page 37*.

UPnP

Produkt Axis obsługuje protokół UPnP®. Protokół UPnP jest domyślnie włączony, a produkt jest automatycznie wykrywany przez systemy operacyjny i klienty obsługujące ten protokół.

Protokół UPnP można wyłączyć w menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Network (Sieć) > UPnP**.

Bonjour

Produkt Axis obsługuje protokół Bonjour. Protokół Bonjour jest domyślnie włączony, a produkt jest automatycznie wykrywany przez systemy operacyjny i klienty obsługujące ten protokół.

Protokół Bonjour można wyłączyć w menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Network (Sieć) > Bonjour**.

Porty i urządzenia

Porty we/wy

Złącze pomocnicze ma cztery konfigurowalne porty wejścia i wyjścia do podłączania urządzeń zewnętrznych.

Złącze zewnętrzne ma dwa konfigurowalne porty wejścia i wyjścia do podłączania urządzeń zewnętrznych.

Porty I/O można skonfigurować w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Porty i urządzenia > Porty I/O**. Wybierz kierunek portu (**Wejście** lub **Wyjście**). Portom można nadać nazwy opisowe, a ich **Stany normalne** można skonfigurować jako **Obwód otwarty** lub **Obwód uziemienia**.

Status portu

Lista na stronie **Opcje systemu > Porty i urządzenia > Status portu** informuje o statusie portów wejścia i wyjścia produktu.

Konserwacja

Produkt Axis ma kilka funkcji służących do konserwacji. Są one dostępne w menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Maintenance (Konserwacja)**.

Gdy produkt Axis działa niezgodnie z oczekiwaniami, kliknij przycisk **Uruchom ponownie**, aby ponownie uruchomić produkt. Nie wpłynie to na żadne bieżące ustawienia.

Uwaga

Ponowne uruchomienie spowoduje skasowanie wszystkich wpisów w raporcie o serwerze.

Kliknij przycisk **Przywróć**, aby zresetować większość ustawień do domyślnych wartości fabrycznych. Nie ma to wpływu na następujące ustawienia:

- protokół uruchamiania (DHCP lub stały adres),
- stały adres IP,
- router domyślny,
- maska podsieci,
- czas systemowy,
- ustawienia 802.1X,

Kliknij przycisk **Domyślne**, aby zresetować większość ustawień, w tym adres IP, do domyślnych wartości fabrycznych. Tego przycisku należy używać z rozwagą. Produkt Axis można również przywrócić do domyślnych ustawień fabrycznych za pomocą przycisku Control — zob. *Przywracanie domyślnych ustawień fabrycznych, on page 37*.

Informacje dotyczące aktualizacji oprogramowania sprzętowego: *Jak dokonać aktualizacji oprogramowania sprzętowego, on page 37*.

Wsparcie

Informacje ogólne o pomocy technicznej

Jeśli potrzebujesz pomocy technicznej, na stronie **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Support (Pomoc techniczna) > Support Overview (Informacje ogólne o pomocy technicznej)** znajdują się informacje na temat rozwiązywania problemów i dane kontaktowe.

Zob. też *Rozwiązywanie problemów, on page 37*.

Przegląd systemu

Aby wyświetlić ogólny status produktu Axis i jego ustawienia, przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Pomoc techniczna > Przegląd systemu**. Można tutaj znaleźć takie informacje, jak wersja oprogramowania sprzętowego, adres IP, ustawienia sieci i zabezpieczeń, ustawienia zdarzeń i najnowsze wpisy do dziennika.

Dzienniki i raporty

Na stronie **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Support (Pomoc techniczna) > Logs & Reports (Dzienniki i raporty)** można wygenerować dzienniki i raporty ułatwiające analizę systemu oraz rozwiązywanie problemów. W przypadku kontaktu z działem wsparcia technicznego Axis należy dołączyć raport systemowy do zgłoszenia.

Dzienniki systemu – Zawiera informacje o zdarzeniach systemowych.

Dziennik dostępu – Zawiera wykaz wszystkich nieudanych prób dostępu do produktu. Dziennik dostępu można również skonfigurować tak, aby wyświetlić listę wszystkich połączeń z produktem (patrz poniżej).

Wyświetl raport o serwerze – Opcja ta służy do wyświetlenia statusu produktu w oknie wyskakującym. W raporcie o serwerze automatycznie umieszczany jest dziennik dostępu.

Pobierz raport o serwerze – Opcja ta służy do utworzenia pliku ZIP, który zawiera pełny raport o serwerze w pliku tekstowym w formacie UTF–8. Aby dołączyć zrzut ekranu ze strony podglądu na żywo produktu, wybierz opcję **Include snapshot from Live View (Dołącz ujęcie z podglądu na żywo)**. Plik ZIP należy zawsze dołączać do korespondencji z działem pomocy technicznej.

Lista parametrów – Wyświetla parametry produktów i ich bieżące ustawienia. Lista ta może być szczególnie przydatna podczas rozwiązywania problemów lub korespondencji z działem pomocy technicznej Axis.

Lista połączeń – Lista wszystkich klientów mających bieżący dostęp do strumieni mediów.

Raport o awarii – Opcja ta służy do generowania archiwum z informacjami o usuwaniu błędów. Wygenerowanie tego raportu trwa kilka minut.

Poziomy dzienników systemu i dostępu można ustawić w menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Support (Pomoc techniczna) > Logs & Reports (Dzienniki i raporty) > Configuration (Konfiguracja)**. Dziennik dostępu można skonfigurować tak, aby wyświetlić listę wszystkich połączeń z produktem (wybierz opcję Krytyczne, Ostrzeżenia i informacje).

Zaawansowane

Używanie skryptów

Dzięki skryptom doświadczeni użytkownicy mogą personalizować i wykorzystywać własne skrypty.

POWIADOMIENIE

Nieprawidłowe korzystanie z tej funkcji może spowodować nieoczekiwane zachowanie i utratę kontaktu z produktem Axis.

Axis stanowczo odradza korzystanie z tej funkcji użytkownikom, którzy nie rozumieją konsekwencji. Dział wsparcia technicznego Axis nie zapewnia pomocy w razie problemów ze spersonalizowanymi skryptami.

Aby otworzyć Edytor skryptów, przejdź do menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Advanced (Zaawansowane) > Scripting (Skrypty)**. Jeśli skrypt powoduje problemy, zresetuj produkt do domyślnych ustawień fabrycznych: *page 37*.

Więcej informacji: *www.axis.com/developer*

Przesyłanie plików

Pliki, na przykład strony internetowe i obrazy, można przesłać do produktu Axis i użyć jako opcji ustawień domyślnych. Aby przesłać plik, przejdź do menu **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > System Options (Opcje systemu) > Advanced (Zaawansowane) > File Upload (Przesyłanie plików)**.

Dostęp do przesłanych plików można uzyskać pod adresem `http://<ip address>/local/<user>/<file name>`, gdzie `<user>` to wybrana grupa użytkowników (administrator) przesłanego pliku.

Rozwiązywanie problemów

Przywracanie domyślnych ustawień fabrycznych

Ważne

Przywracanie ustawień fabrycznych powinno być dokonywane ze szczególną ostrożnością. Przywrócenie ustawień fabrycznych oznacza zresetowanie wszystkich ustawień, łącznie z adresem IP, do wartości fabrycznych.

Przywracanie domyślnych ustawień fabrycznych produktu:

1. Odłącz zasilanie produktu.
2. Naciśnij i przytrzymaj przycisk kontrolny i włącz zasilanie. Zob. *Przegląd produktów, on page 6*.
3. Przytrzymuj przycisk Control przez 25 sekund, aż wskaźnik LED stanu ponownie zmieni kolor na bursztynowy.
4. Zwolnij przycisk Control. Proces zostanie zakończony, gdy wskaźnik LED stanu zmieni kolor na zielony. Produkt zostanie zresetowany do domyślnych ustawień fabrycznych. Jeżeli w sieci nie jest dostępny serwer DHCP, domyślny adres IP to `192.168.0.90`.
5. Użyj narzędzi do instalacji i zarządzania, aby przypisać adres IP, ustawić hasło i uzyskać dostęp do produktu.

Parametry można również zresetować do domyślnych ustawień fabrycznych przez interfejs WWW. Wybierz kolejno **Setup (Ustawienia) > Additional Controller Configuration (Dodatkowa konfiguracja kontrolera) > Setup (Ustawienia) > System Options (Opcje systemowe) > Maintenance (Konserwacja)** i kliknij **Default (Domyślne)**.

Sprawdzanie bieżącej wersji oprogramowania sprzętowego

Oprogramowanie sprzętowe określa dostępne funkcje urządzeń sieciowych. Podczas rozwiązywanie problemów należy zawsze najpierw sprawdzić bieżącą wersję oprogramowani sprzętowego. Najnowsza wersja może zawierać poprawki, które rozwiążą problem.

Bieżąca wersja oprogramowania sprzętowego produktu Axis wyświetlana jest na stronie przeglądu systemu.

Jak dokonać aktualizacji oprogramowania sprzętowego

Ważne

- Sprzedawca zastrzega sobie prawo do naliczenia opłaty za wszelkie naprawy spowodowane nieprawidłowym przeprowadzeniem aktualizacji przez użytkownika.
- Wstępnie skonfigurowane i spersonalizowane ustawienia są zapisywane podczas aktualizacji oprogramowania sprzętowego (pod warunkiem że funkcje te są dostępne w nowym oprogramowaniu sprzętowym), choć Axis Communications AB tego nie gwarantuje.
- Po zainstalowaniu poprzedniej wersji oprogramowania sprzętowego trzeba przywrócić domyślne ustawienia fabryczne produktu.

Uwaga

- Po zakończeniu aktualizacji produkt automatycznie uruchomi się ponownie. Jeżeli będziesz uruchamiać produkt po aktualizacji ręcznie, odczekaj 5 minut, nawet jeśli podejrzewasz niepowodzenie aktualizacji.
- Pierwsze uruchomienie może potrwać kilka minut, ponieważ po aktualizacji oprogramowania sprzętowego następuje uaktualnienie bazy danych zawierającej użytkowników, grupy, poświadczenia i inne dane. Wymagany czas zależy od ilości danych.
- Aktualizacja produktu Axis do najnowszej wersji oprogramowania sprzętowego umożliwia uaktualnienie produktu o najnowsze funkcje. Przed aktualizacją oprogramowania sprzętowego zawsze należy przeczytać instrukcje dotyczące aktualizacji oraz informacje o wersji dostępne z każdą nową wersją.

1. Pobierz na komputer najnowszy plik oprogramowania sprzętowego dostępny bezpłatnie na stronie *www.axis.com/support*

2. Przejdź do strony internetowej produktu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Konserwacja**.
3. W opcji **Aktualizuj serwer** kliknij polecenie **Wybierz plik** i wyszukaj plik na komputerze.
4. Jeżeli produkt ma automatycznie przywrócić domyślne ustawienia fabryczne po aktualizacji, zaznacz pole wyboru **Domyślne**.
5. Kliknij **Aktualizuj**.
6. Odczekaj około 5 minut na aktualizację i ponowne uruchomienie produktu. Następnie wyczyść pamięć podręczną przeglądarki.
7. Uzyskaj dostęp do produktu.

Objawy, możliwe przyczyny i sposoby naprawy

Problemy z aktualizacją oprogramowania sprzętowego

Niepowodzenie podczas aktualizacji oprogramowania sprzętowego	Jeśli aktualizacja oprogramowania sprzętowego zakończy się niepowodzeniem, produkt załaduje ponownie poprzednią wersję oprogramowania sprzętowego. Sprawdź plik oprogramowania sprzętowego i spróbuj ponownie.

Problemy z ustawieniem adresu IP

Podczas korzystania z ARP/Ping	Spróbuj ponownej instalacji. Adres IP należy ustawić w ciągu dwóch minut po doprowadzeniu zasilania do produktu. Upewnij się, że długość sondy ping jest ustawiona na 408. Instrukcje można znaleźć w Przewodniku instalacji na stronie produktu pod adresem *axis.com*.
Produkt należy do innej podsieci	Jeśli adres IP przeznaczony dla danego produktu oraz adres IP komputera używanego do uzyskania dostępu do produktu należą do różnych podsieci, ustawienie adresu IP będzie niemożliwe. Skontaktuj się z administratorem sieci, aby uzyskać adres IP.
Adres IP jest używany przez inne urządzenie	Odłącz produkt Axis od sieci. Uruchom polecenie ping (w oknie polecenia/DOS wpisz `ping` oraz adres IP produktu): • Jeżeli zostanie zwrócony komunikat: `Reply from <IP address>: bytes=32; time=10...` (Odpowiedź z...), oznacza to, że adres IP może być zajęty przez inne urządzenie w sieci IP. Poproś administratora sieci o nowy adres IP i zainstaluj ponownie produkt. • Jeśli otrzymasz: `Request timed out`, oznacza to, że ten adres IP jest dostępny do wykorzystania przez produkt Axis. Sprawdź całe okablowanie i zainstaluj produkt ponownie.
Możliwy konflikt adresów IP z innym urządzeniem w tej samej podsieci	Zanim serwer DHCP ustawi adres dynamiczny, używany jest statyczny adres IP produktu Axis. Oznacza to, że jeśli ten sam domyślny statyczny adres IP jest używany także przez inne urządzenie, mogą wystąpić problemy podczas uzyskiwania dostępu do produktu.

Nie można uzyskać dostępu do produktu przez przeglądarkę

Nie można się zalogować	Jeśli protokół HTTPS jest włączony, należy upewnić się, że podczas logowania używany jest właściwy protokół (HTTP lub HTTPS). Może zajść konieczność ręcznego wpisania `http` lub `https` w polu adresu przeglądarki. W razie utraty hasła dla użytkownika root należy przywrócić ustawienia fabryczne produktu. Zob. *Przywracanie domyślnych ustawień fabrycznych, on page 37*.

Serwer DHCP zmienił adres IP	Adresy IP otrzymane z serwera DHCP są dynamiczne i mogą się zmieniać. Jeśli adres IP został zmieniony, użyj narzędzia AXIS IP Utility lub AXIS Device Manager, aby zlokalizować produkt w sieci. Znajdź produkt przy użyciu nazwy modelu lub numeru seryjnego produktu bądź nazwy DNS (jeśli skonfigurowano tę nazwę). W razie potrzeby można przydzielić samodzielnie statyczny adres IP. Instrukcje znajdują się w dokumencie Jak przypisać adres IP i uzyskać dostęp do urządzenia na stronie produktu w witrynie *axis.com*
Błąd certyfikatu podczas korzystania ze standardu IEEE 802.1X	Aby uwierzytelnianie działało prawidłowo, ustawienia daty i godziny w produkcie Axis powinny być zsynchronizowane z serwerem NTP. Zob. .

Dostęp do produktu można uzyskać lokalnie, ale nie z zewnątrz

Konfiguracja routera	Aby skonfigurować router i umożliwić przesyłanie danych do produktu Axis, włącz funkcję NAT-traversal (przechodzenie portów), która spróbuje automatycznie skonfigurować router, umożliwiając dostęp do produktu Axis; zob. *NAT traversal (mapowanie portów) dla IPv4., on page 31*. Router musi obsługiwać protokół UPnP®.
Zapora	Poproś administratora sieci, aby sprawdził, czy problemem nie jest zapora internetowa.
Wymagane domyślne routery	Sprawdź, czy należy skonfigurować ustawienia routera w menu **Ustawienia > Ustawienia sieciowe** lub **Konfiguracji > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Podstawowe**.

Specyfikacje

Tekst oznaczony jako **UL** dotyczy tylko instalacji UL 293 lub UL 294.

Wskaźniki LED

LED	Kolor	Wskazanie
Sieć	Zielony	Stałe światło przy podłączeniu do sieci 100 Mbit/s. Miga w przypadku wystąpienia aktywności sieciowej.
	Bursztynowy	Stałe światło przy podłączeniu do sieci 10 Mbit/s. Miga w przypadku wystąpienia aktywności sieciowej.
	Wyłączona	Brak połączenia z siecią.
Status	Zielony	Stałe zielone światło przy normalnym działaniu.
	Bursztynowy	Stałe światło podczas uruchamiania i odtwarzania ustawień.
	Czerwony	Powolne miganie w przypadku niepowodzenia aktualizacji.
Zasilanie	Zielony	Normalne działanie.
	Bursztynowy	Miga na zielono/bursztynowo podczas aktualizacji oprogramowania sprzętowego.
Nadprąd przekaźnika	Czerwony	Stałe światło po zwarciu lub wykryciu nadprądu.
	Wyłączona	Normalne działanie.
Nadprąd czytnika	Czerwony	Stałe światło po zwarciu lub wykryciu nadprądu.
	Wyłączona	Normalne działanie.
Przekaźnik	Zielony	Przekaźnik aktywny.[2]
	Wyłączona	Przekaźnik nieaktywny.

Uwaga

- Wskaźnik LED stanu można skonfigurować tak, by podczas aktywnego zdarzenia migał.
- Wskaźnik LED stanu można skonfigurować tak, by migał po rozpoznaniu jednostki. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Konserwacja**.

Przyciski

Przycisk kontrolny

Przycisk kontrolny ma następujące zastosowania:

- Przywracania domyślnych ustawień fabrycznych produktu. Zob. *Przywracanie domyślnych ustawień fabrycznych, on page 37*.

Złącza

Złącze sieciowe

Złącze RJ45 Ethernet z zasilaniem Power over Ethernet Plus (PoE+).

UL: Zasilanie Power over Ethernet (PoE) dostarczane przez Power Injector Power over Ethernet IEEE 802.3af/802.3at typ 1 klasa 3 (UL 294) lub Power over Ethernet Plus (PoE+) IEEE 802.3at typ 2 klasa 4 z ograniczeniem

2. *Przekaźnik jest aktywny po podłączeniu COM do NO.*

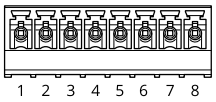
mocy, dostarczający zasilanie 44–57 V DC, 15,4 W / 30 W. Power over Ethernet (PoE) ocenione przez UL z zasilaczem midspan AXIS T8133 Midspan 30 W 1-port.

Złącze czytnika

Dwa 8-pinowe bloki złączy obsługujące protokoły RS485 i Wiegand do komunikacji z czytnikiem.

Podane wartości mocy wyjściowej są współdzielone między dwoma portami czytnika. Oznacza to, że 486 mA przy 12 V DC jest zarezerwowane dla wszystkich czytników podłączonych do kontrolera drzwi.

Na stronie internetowej produktu wybierz odpowiedni protokół, którego chcesz używać.



Konfiguracja na potrzeby RS485

Funkcja	Pin	Uwaga	Specyfikacje
Masa DC (GND)	1		0 V DC
Wyjście DC (+12 V)	2	Dostarcza zasilanie do czytnika.	12 V DC, maks. 486 mA do obu czytników łącznie
RX/TX	3-4	Pełny dupleks: RX. Half duplex: RX/TX.	
TX	5–6	Pełny dupleks: TX.	
Konfigurowalne (wejście lub wyjście)	7–8	Wejście cyfrowe — podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	Od 0 do maks. 30 V DC
		Wyjście cyfrowe – w przypadku stosowania z obciążeniem indukcyjnym, np. przekaźnikiem, konieczne jest szeregowe podłączenie diody w celu zabezpieczenia przed stanami przejściowymi napięcia.	Od 0 do maks. 30 V DC, otwarty dren maks. 100 mA

Ważne

- Gdy czytnik jest zasilany przez kontroler, dopuszczalna długość kabla wynosi do 200 m (656 stopy).
- Gdy czytnik nie jest zasilany przez kontroler, dopuszczalna długość kabla dla danych czytnika wynosi do 1000 m (3280,8 ft), jeśli spełnione są następujące wymagania dotyczące kabla: 1 skrętka ekranowana, AWG 24, impedancja 120 omów.

Konfiguracja na potrzeby Wiegand

Funkcja	Pin	Uwaga	Specyfikacje
Masa DC (GND)	1		0 V DC
Wyjście DC (+12 V)	2	Dostarcza zasilanie do czytnika.	12 V DC, maks. 486 mA do obu czytników łącznie

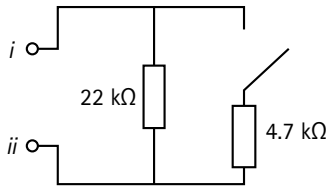
D0	3		
D1	4		
O	5–6	Wyjście cyfrowe, otwarty dren	
Konfigurowalne (wejście lub wyjście)	7–8	Wejście cyfrowe — podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	Od 0 do maks. 30 V DC
		Wyjście cyfrowe – w przypadku stosowania z obciążeniem indukcyjnym, np. przekaźnikiem, konieczne jest szeregowe podłączenie diody w celu zabezpieczenia przed stanami przejściowymi napięcia.	Od 0 do maks. 30 V DC, otwarty dren maks. 100 mA

Ważne

- Gdy czytnik jest zasilany przez kontroler, dopuszczalna długość kabla wynosi do 150 m (500 stopy).
- Gdy czytnik nie jest zasilany przez kontroler, dopuszczalna długość kabla dla danych czytnika wynosi do 150 m (500 ft), jeśli spełnione jest następujące wymaganie dotyczące kabla: AWG 22.

Nadzorowane wejścia

Aby móc korzystać z nadzorowanych wejść, zamontuj rezystory końca linii zgodnie ze schematem poniżej.



i Wejście

ii 0 V DC (-)

UL: nadzorowane wejścia nie były oceniane przez UL w przypadkach włamań. Wyłącznie monitor drzwi i REX obsługują nadzorowanie przy użyciu rezystorów końca linii.

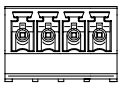
Uwaga

Zaleca się korzystanie ze skrętek ekranowanych. Podłącz ekranowanie do 0 V DC.

Złącze drzwi

Dwa 4-pinowe bloki złączy do urządzeń monitorujących drzwi (wejście cyfrowe).

Monitor drzwi obsługuje nadzorowanie przy użyciu rezystorów końca linii. Alarm wyzwalany jest po przerwaniu połączenia. Aby móc korzystać z nadzorowanych wejść, zamontuj rezystory końca linii. Dla wejść nadzorowanych użyj schematu połączeń. Zob. .



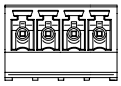
Funkcja	Pin	Uwagi	Specyfikacje
Masa DC	1, 3		0 V DC
Wejście	2, 4	Do komunikacji z monitorem drzwi. Wejście cyfrowe lub wejście nadzorowane — podłącz odpowiednio do styku 1 lub 3, aby aktywować, lub pozostaw rozłączone, aby dezaktywować.	od 0 do maks. 30 V DC

Ważne

Dopuszczalna długość kabla wynosi do 200 m (656 ft), jeśli spełnione jest następujące wymaganie dotyczące kabla: AWG 24.

Złącze przekaźnikowe

Dwa 4-pinowe bloki zacisków dla przekaźników typu C, które mogą być używane na przykład do sterowania zamkiem lub interfejsem do bramy.



Funkcja	Pin	Uwagi	Specyfikacje
Masa DC (GND)	1		0 V DC
NO	2	Normalnie otwarte. Do podłączania urządzeń przekaźnikowych. Podłącz bezpieczną blokadę między masą NO i DC. Dwa styki przekaźnika są galwanicznie oddzielone od reszty obwodu, jeśli zworki nie są używane.	Maks. prąd = 2 A na przekaźnik Maks. napięcie = 30 V DC
COM	3	Wspólny	
NC	4	NC (normalnie zamknięty). Do podłączania urządzeń przekaźnikowych. Podłącz bezpieczną blokadę między masą NC i DC. Dwa styki przekaźnika są galwanicznie oddzielone od reszty obwodu, jeśli zworki nie są używane.	

Zworka zasilania przekaźnika

Po podłączeniu zworki zasilania przekaźnika łączy ona 12 V DC lub 24 V DC z stykiem COM przekaźnika.

Można jej użyć do połączenia zamka między stykami GND i NO lub GND i NC.

Źródło prądu	Maksymalna moc przy 12 V DC[3]	Maksymalna moc przy 24 V DC[3]
DC IN	1600 mA	800 mA
PoE	800 mA	400 mA

POWIADOMIENIE

Jeśli zamek nie jest spolaryzowany, zalecamy dodanie zewnętrznej diody typu flyback.

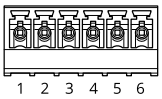
Złącze pomocnicze

Złącze pomocnicze służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wykrywaniem ruchu, wyzwalaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe) złącze pomocnicze zapewnia interfejs do:

Wejście cyfrowe – Do podłączenia urządzeń, które mogą przełączać się pomiędzy obwodem zamkniętym i otwartym, na przykład czujników PIR, czujników okiennych lub drzwiowych oraz czujników wykrywania zbicia szyby.

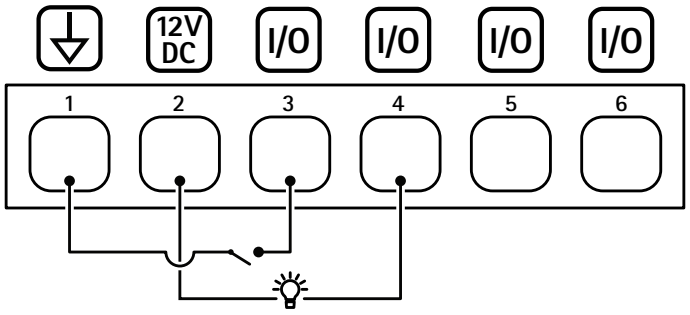
Wyjście cyfrowe – Do podłączenia urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączonymi urządzeniami można zarządzać poprzez API VAPIX® lub stronę internetową produktu.

6-pinowego bloku złączy



Funkcja	Pin	Uwagi	Specyfikacje
Masa DC	1		0 V DC
Wyjście DC	2	Może być wykorzystywane do zasilania dodatkowego sprzętu. Uwaga: ten styk może być używany tylko jako wyjście zasilania.	12 V DC Maks. obciążenie = 50 mA na każde WE/WY
Konfigurowalne (wejście lub wyjście)	3–6	Wejście cyfrowe — podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	od 0 do maks. 30 V DC
		Wyjście cyfrowe — podłączone wewnętrznie do styku 1 (masa DC), gdy aktywne i niepodłączone, gdy nieaktywne. W przypadku stosowania z obciążeniem indukcyjnym, np. przekaźnikiem, konieczne jest szeregowe podłączenie diody w celu zabezpieczenia przed stanami przejściowymi napięcia. Każde I/O może przyjąć zewnętrzne obciążenie 12 V DC, 50 mA (maks.)m jeśli użyto wewnętrznego wyjścia 12 V DC (styk 2). W przypadku podłączeń z otwartym drenem w połączeniu z zewnętrznym źródłem zasilania I/O mogą otrzymywać zasilanie DC 0–30 V DC, 100 mA.	Od 0 do maks. 30 V DC, otwarty dren maks. 100 mA

3. Zasilanie jest dzielone między dwa przekaźniki i wejście/wyjście AUX 12 V DC.

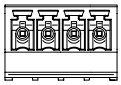


1 *Masa DC*
2 *Wyjście DC 12 V*
3 *We/Wy skonfigurowane jako wejście*
4 *We/Wy skonfigurowane jako wyjście*
5 *Konfigurowalne We/Wy*
6 *Konfigurowalne We/Wy*

Złącze zewnętrzne

4-pinowy blok złączy umożliwiający podłączenie urządzeń zewnętrznych, na przykład detektorów wybicia szyby lub czujników pożaru.

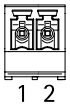
UL: Złącze nie zostało ocenione przez UL pod kątem użytkowania jako alarm antywłamaniowy/pożarowy.



Funkcja	Pin	Uwagi	Specyfikacje
Masa DC	1, 3		0 V DC
Konfigurowalne (wejście lub wyjście)	2, 4	Wejście cyfrowe – podłącz do styku 1 lub 3, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	od 0 do maks. 30 V DC
		Wyjście cyfrowe –podłącz do styku 1 lub 3, aby aktywować lub pozostaw rozłączone, aby dezaktywować. W przypadku stosowania z obciążeniem indukcyjnym, np. przekaźnikiem, konieczne jest szeregowe podłączenie diody w celu zabezpieczenia przed stanami przejściowymi napięcia.	Od 0 do maks. 30 V DC, otwarty dren maks. 100 mA

Złącze zasilania

2-stykowy zespół zacisków na wejście zasilania DC. Używaj urządzenia LPS zgodnego z SELV z nominalną mocą wyjściową ograniczoną do ≤100 W lub nominalnym prądem wyjściowym ograniczonym do ≤5 A.



Funkcja	Pin	Uwagi	Specyfikacje
0 V DC (-)	1		0 V DC
Wejście DC	2	Do zasilania kontrolera, gdy nie jest używane zasilanie Power over Ethernet. Uwaga: ten styk może być używany tylko jako wejście zasilania.	10,5–28 V (prąd stały), maks. 36 W

UL: zasilanie prądem stałym dostarczane z zasilaczem w standardzie UL 294, UL 293 lub UL 603, w zależności od oprogramowania, o odpowiednich parametrach.

Złącze wejścia zapasowego akumulatora

Do podłączenia zapasowego akumulatora z wbudowaną ładowarką. Wejście 12 V DC.

UL: Złącze nie zostało ocenione przez UL.

Ważne

Podczas korzystania z wejścia akumulatora należy włączyć szeregowo w obwód zewnętrzny bezpiecznik 3 A.



Funkcja	Pin	Uwagi	Specyfikacje
0 V DC (-)	1		0 V DC
Wejście akumulatora	2	Do zasilania kontrolera drzwi, gdy nie są dostępne inne źródła zasilania. Uwaga: ten styk może być używany tylko jako wejście zasilania z akumulatora. Tylko do łączenia z UPS.	11–13,7 V DC, maks. 36 W

Informacje dotyczące bezpieczeństwa

Poziomy zagrożenia

⚠ NIEBEZPIECZEŃSTWO
Wskazuje zagrożenie, które spowoduje zgon lub ciężkie obrażenia.

⚠ OSTRZEŻENIE
Wskazuje zagrożenie, które może spowodować zgon lub ciężkie obrażenia.

⚠ UWAGA
Wskazuje zagrożenie, które może spowodować niewielkie lub umiarkowane obrażenia.

POWIADOMIENIE
Wskazuje zagrożenie, które może spowodować uszkodzenie mienia.

Inne poziomy komunikatów

Ważne
Wskazuje istotne informacje niezbędne do poprawnego działania produktu.

Uwaga
Wskazuje przydatne informacje, które ułatwiają wykorzystanie możliwości produktu.

Interfejs WWW

Uwaga

Ta sekcja dotyczy tylko AXIS A1601 Network Door Controller z oprogramowaniem układowym AXIS Camera Station Secure Entry.

: Przełączaj się między przeglądem **Device settings (Ustawienia urządzenia)** a **Analytics (Dane analityczne)**.

: Wyświetl/ukryj menu główne.

Pomoc: Uzyskaj dostęp do pomocy dotyczącej produktu, informacji o wersji oraz przewodnika po cyklu życia produktu.

Information (Informacje):

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

Administrator:

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

Status

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, a także status PTP.

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

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.

Urządzenie

Alarmy

Device motion (Ruch urządzenia): Włączenie tej opcji powoduje wyzwalanie alarmu w systemie po wykryciu ruchu urządzenia.

Otwarcie obudowy: Włączenie tej opcji powoduje wyzwalanie alarmu w systemie, gdy zostanie wykryte otwarcie obudowy kontrolera drzwi. Wyłącz to ustawienie dla kontrolerów drzwi typu barebone.

Sabotaż od zewnątrz: Jej włączenie spowoduje emitowanie alarmu w systemie w reakcji na wykrycie zewnętrznej próby ingerencji. Na przykład po otwarciu lub zamknięciu zewnętrznej szafki.

- **Normal state (Stan normalny)**: Kliknij opcję  w przypadku obwodu otwartego i  w przypadku obwodu zamkniętego.
- **Nadzorowane wejście**: Włączenie tej opcji spowoduje monitorowanie stanu wejścia i umożliwi skonfigurowanie rezystorów końca linii.
  - Aby używać pierwszego połączenia równoległego, wybierz opcję **Pierwsze połączenie równoległe z 22 kΩ opornikiem równoległym i 4,7 kΩ opornikiem szeregowym**.
  - Aby używać pierwszego połączenia szeregowego, select zaznacz opcję **Serial first connection (Pierwsze połączenie szeregowe)**, a następnie z listy rozwijanej **Resistor values (Wartości oporników)** wybierz wartość rezystora.

Urządzenia peryferyjne

Czytniki

Dodaj: Kliknij, aby dodać czytnik.

Axis network readers (Czytniki sieciowe Axis): Do kontrolera można dodać maksymalnie 16 czytników Bluetooth, bez konieczności posiadania licencji.

- **Name (Nazwa)**: Wprowadź nazwę czytnika.
- **Czytnik**: Wybierz czytnik z listy rozwijanej.
- **Adres IP**: Ręcznie wprowadź adres IP czytnika.
- **Username (Nazwa użytkownika)**: Wprowadź nazwę użytkownika czytnika.
- **Password (Hasło)**: Wprowadź hasło czytnika.
- **Ignore server certificate verification (Ignoruj weryfikację certyfikatu serwera)**: Włącz, aby ignorować weryfikację.
- **I/O ports and relays (Porty WE/WY i przekaźniki)**: Rozwiń, aby skonfigurować porty WE/WY i przekaźniki.
  - **Port**: Wyświetla nazwę portu.
  - **Direction (Kierunek)**: Wskazuje, że jest to port wejścia lub wyjścia.
  - **Normal state (Stan normalny)**: Kliknij opcję  w przypadku obwodu otwartego i  w przypadku obwodu zamkniętego.

Interkomy sieciowe Axis (konieczna jest ponowna konfiguracja w AXIS Camera Station)

- **Name (Nazwa)**: Wprowadź nazwę czytnika.
- **Czytnik**: Wybierz czytnik z listy rozwijanej.
- **Adres IP**: Ręcznie wprowadź adres IP czytnika.
- **Username (Nazwa użytkownika)**: Wprowadź nazwę użytkownika czytnika.
- **Password (Hasło)**: Wprowadź hasło czytnika.
- **Ignore server certificate verification (Ignoruj weryfikację certyfikatu serwera)**: Włącz, aby ignorować weryfikację.

AXIS License Plate Verifier (konieczna jest ponowna konfiguracja w AXIS Camera Station)

- **Name (Nazwa)**: Wprowadź nazwę czytnika.
- **API key (Klucz API)**: Wprowadź klucz API.
- **Generate (Wygeneruj)**: Kliknij, aby wygenerować klucz API.
- **Copy API-key (Kopiuj klucz API)**: Kliknij, aby skopiować klucz API i zapisz go w bezpiecznym miejscu.

AXIS Barcode Reader (konieczna jest ponowna konfiguracja w AXIS Camera Station)

- **Name (Nazwa)**: Wprowadź nazwę czytnika.
- **API key (Klucz API)**: Wprowadź klucz API.
- **Generate (Wygeneruj)**: Kliknij, aby wygenerować klucz API.
- **Copy API-key (Kopiuj klucz API)**: Kliknij, aby skopiować klucz API i zapisz go w bezpiecznym miejscu.

Edit (Edycja): Wybierz czytnik i kliknij **Edit (Edytuj)**, aby wprowadzić zmiany dla wybranego czytnika.

Usuń: Wybierz czytniki i kliknij **Delete (Usuń)**, aby usunąć wybrane czytniki.

Zamki bezprzewodowe

Za pomocą koncentratora komunikacyjnego AH30 można podłączyć do 16 zamków bezprzewodowych ASSA ABLOY Aperio. Do korzystania z zamka bezprzewodowego wymagana jest licencja.

Uwaga

Koncentrator komunikacyjny AH30 należy zainstalować po bezpiecznej stronie.

Connect communication hub (Połącz koncentrator komunikacyjny): Kliknij, aby podłączyć zamki bezprzewodowe.

Uaktualnianie

Upgrade readers (Uaktualnij czytniki): Kliknij, aby uaktualnić oprogramowanie czytnika. Możesz uaktualnić obsługiwane czytniki tylko wtedy, gdy są one w trybie online.

Upgrade converters (Uaktualnij konwertery): Kliknij, aby uaktualnić oprogramowanie konwertera. Możesz uaktualnić obsługiwane konwertery tylko wtedy, gdy są one w trybie online.

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.

- **Automatic date and time (PTP) Automatyczna data i godzina (PTP))**: Synchronizacja przy użyciu protokołu precyzyjnego czasu.
- **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.
  - **Trusted NTS KE CA certificates (Zaufane certyfikaty NTS KE CA)**: Wybierz zaufane certyfikaty urzędu certyfikacji (UC), które mają być używane do bezpiecznej synchronizacji czasu NTS KE, lub pozostaw opcję bez zaznaczenia.
  - **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 (v4 lub v6). Jeżeli dostępne są obie wersje, urządzenie preferuje strefy czasowe IANA zamiast POSIX oraz DHCPv4 zamiast DHCPv6.
  - DHCPv4 korzysta z opcji 100 w zakresie stref czasowych POSIX oraz opcji 101 w zakresie stref czasowych IANA.
  - DHCPv6 korzysta z opcji 41 w zakresie POSIX i opcji 42 w zakresie IANA.
- **Manual (Ręcznie)**: Wybierz strefę czasową z listy rozwijanej.

Uwaga

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

Time sync status (Stan synchronizacji czasu): Wyświetla informacje dotyczące synchronizacji NTP oraz stan PTP.

Network time synchronized capture (Przechwytywanie zsynchronizowane z czasem sieciowym): Włącz, aby umożliwić przechwytywanie obrazów jednocześnie przez wiele kamer.

Sieć

Sieć

IPv4

Przypisz automatycznie IPv4: Wybierz opcję „Przypisz automatycznie IPv4" (DHCP), aby sieć automatycznie przydzielała adres IP, maskę podsieci i router bez konieczności ręcznej konfiguracji. 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.

Hostname (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 automatyczne aktualizowanie rekordów serwera nazw domen, gdy zmieni się jego adres IP.

Zarejestruj nazwę DNS: Wprowadź unikatową nazwę domeny, która wskazuje adres IP urządzenia. Używaj tylko dozwolonych znaków: A-Z, a-z, 0-9 i -.

TTL: Time to Live (TTL) to ustawienie określające, jak długo rekord DNS zachowuje ważność, 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.

Uwaga

Jeśli protokół DHCP jest wyłączony, funkcje oparte na automatycznej konfiguracji sieci, takie jak nazwa hosta, serwery DNS, serwer NTP i inne, mogą przestać działać.

HTTP i HTTPS

HTTPS to protokół umożliwiający szyfrowanie żądań stron wysyłanych przez użytkowników oraz stron zwracanych przez serwer sieci Web. Zaszyfrowana wymiana informacji opiera się na użyciu certyfikatu HTTPS, który gwarantuje autentyczność serwera.

Warunkiem używania protokołu HTTPS w urządzeniu jest zainstalowanie certyfikatu HTTPS. Przejdź do menu **System > Zabezpieczenia**, aby utworzyć i zainstalować certyfikaty.

Zezwalaj na dostęp przez: wybierz, czy użytkownik może połączyć się z urządzeniem za pośrednictwem protokołów **HTTP**, **HTTPS** lub zarówno **HTTP, jak i HTTPS**.

Uwaga

W przypadku przeglądania zaszyfrowanych stron internetowych za pośrednictwem protokołu HTTPS może wystąpić spadek wydajności, zwłaszcza przy pierwszym żądaniu strony.

HTTP port (Port HTTP): wprowadź wykorzystywany port HTTP. urządzenie pozwala na korzystanie z portu 80 lub innego portu z zakresu 1024–65535. Jeżeli zalogujesz się jako administrator, możesz również wprowadzić dowolny port z zakresu 1–1023. Jeśli użyjesz portu z tego zakresu, otrzymasz ostrzeżenie.

HTTPS port (Port HTTPS): wprowadź wykorzystywany port HTTPS. urządzenie pozwala na korzystanie z portu 443 lub innego portu z zakresu 1024–65535. Jeżeli zalogujesz się jako administrator, możesz również wprowadzić dowolny port z zakresu 1–1023. Jeśli użyjesz portu z tego zakresu, otrzymasz ostrzeżenie.

Certificate (Certyfikat): wybierz certyfikat, aby włączyć obsługę protokołu HTTPS w tym urządzeniu.

Protokoły wykrywania sieci

Bonjour®: Zaznacz, 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®: Zaznacz, 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: Zaznacz, aby umożliwić automatyczne wykrywanie urządzeń w sieci.

LLDP and CDP (LLDP i CDP): Zaznacz, aby umożliwić automatyczne wykrywanie urządzeń w sieci. Jeśli protokoły LLDP i CDP są wyłączone, może to wpłynąć na negocjowanie zasilania z PoE. Aby rozwiązać ewentualne problemy negocjowania zasilania z PoE, należy skonfigurować przełącznik PoE tylko do sprzętowej negocjacji zasilania PoE.

Neighbors (Sąsiedzi): Kliknij, aby wyświetlić informacje o sąsiednich urządzeniach podłączonych do tej samej sieci.

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

Usługa One-Click Cloud Connection (O3C) w połączeniu z systemem O3C 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 opcja domyślna. Aby połączyć się z usługą O3C, naciśnij przycisk kontrolny na urządzeniu. W zależności od modelu urządzenia, naciśnij i zwolnij lub naciśnij i przytrzymaj, aż dioda stanu zacznie migać. Zarejestruj urządzenie w usłudze O3C w ciągu 24 godzin, aby uaktywnić opcję **Always** i pozostać połączonym. Jeśli nie zarejestrujesz urządzenia, zostanie ono odłączone od usługi O3C.
- **Zawsze**: Urządzenie stale próbuje połączyć się z usługą O3C przez Internet. Po zarejestrowaniu urządzenia pozostaje ono połączone. Opcji tej należy używać wtedy, gdy przycisk kontrolny jest niedostępny.
- **No (Nie)**: Odłącza 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.
    - **Link up (Łącze w górę)**: wysyła komunikat pułapkę po zmianie łącza w górę.
    - **Link down (Łącze w dół)**: wysyła komunikat pułapkę po zmianie łącza w dół.
    - **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.
  - **Privacy** (Prywatność): Wybierz rodzaj szyfrowania stosowanego do ochrony danych SNMP.
  - **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. Hasło musi być zgodne z zasadami dotyczącymi haseł, patrz *Konta, on page 61*.

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.

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 oraz .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. Zostanie otwarty przewodnik krok po kroku.

- **More** (Więcej): Wyświetlanie dodatkowych pól do wypełnienia lub wybrania.
- **Secure keystore (Bezpieczny magazyn kluczy)**: Wybierz tę opcję, aby używać funkcji **Trusted Execution Environment (SoC TEE)**, **Secure element (Bezpieczny 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/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):

- **Trusted Execution Environment (SoC TEE)**: Wybierz, aby używać SoC TEE do bezpiecznego magazynu kluczy.
- **Secure element (CC EAL6+, FIPS 140-3 poziom 3)**: 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 802.1x

IEEE 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.

CA certificates (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**:

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

Zapobiegaj atakom typu brute force

Blocking (Blokowanie): włącz, aby blokować ataki typu brute force Ataki typu brute-force wykorzystują metodę prób i błędów do odgadnięcia danych logowania lub kluczy szyfrowania.

Blocking period (Okres blokowania): Wprowadź liczbę sekund, w ciągu których ataki typu brute-force mają być blokowane.

Blocking conditions (Warunki blokowania): wprowadź dopuszczalną liczbę nieudanych prób uwierzytelnienia na sekundę przed rozpoczęciem blokowania. Liczbę dopuszczalnych niepowodzeń można ustawić zarówno na stronie, jak i w urządzeniu.

Zapora

Firewall (Zapora sieciowa): włącz, aby uaktywnić zaporę sieciową.

Domyślne ustawienia zasad: wybierz sposób, w jaki zapora ma obsługiwać żądania połączeń, które nie są objęte regułami.

- **ACCEPT** (Zezwalaj): zezwala na wszystkie połączenia z urządzeniem. Jest opcja domyślna.
- **DROP** (Odrzucaj): blokuje wszystkie próby połączeń z urządzeniem.

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

+ New rule (Dodaj nową regułę): Kliknij, aby utworzyć regułę.

Rule type (Rodzaj reguły):

- **FILTR**: Zaznacz, aby zezwolić lub zablokować połączenia z urządzeń spełniających kryteria określone w regule.
  - **Policy (Zasada)**: wybierz opcję **Accept** (Zezwalaj) lub **Drop** (Odrzucaj) dotyczącą reguły zapory sieciowej.
  - **IP range** (Zakres adresów IP): zaznacz, aby określić zakres adresów do zezwolenia lub zablokowania. Użyj IPv4 / IPv6 w pozycji **Start** (Początek) i **End** (Koniec).
  - **Adres IP**: wpisz adres, który ma być przepuszczany lub blokowany. Użyj IPv4 / IPv6 lub formatu CIDR.
  - **Protocol (Protokół)**: wybierz protokół sieciowy (TCP, UDP lub oba), który ma być dozwolony lub blokowany. Po wybraniu protokołu należy również określić port.
  - **MAC (Adres MAC)**: Wprowadź adres MAC urządzenia, które ma lub nie ma mieć dostępu.
  - **Port range** (Zakres portów): zaznacz, aby określić zakres portów do zezwolenia lub zablokowania. Dodaj je w pozycjach **Start** (Początek) i **End** (Koniec).
  - **Port**: wpisz numer portu, który ma być przepuszczany lub blokowany. Numery portów muszą zawierać się w przedziale od 1 do 65535.
  - **Traffic type** (Rodzaj ruchu): wybierz rodzaj ruchu, na który chcesz zezwolić lub który chcesz zablokować.
    - **UNICAST**: Ruch od jednego nadawcy do jednego odbiorcy.
    - **BROADCAST (TRANSMISJA)**: Ruch od jednego nadawcy do wszystkich urządzeń w sieci.
    - **MULTICAST**: Ruch od jednego lub więcej nadawców do jednego lub więcej odbiorców.
- **LIMIT (OGRANICZENIE)**: Wybierz, aby przyjmować połączenia z urządzeń spełniających kryteria określone w regule, ale stosować ograniczenia w celu zmniejszenia nadmiernego ruchu.
  - **IP range** (Zakres adresów IP): zaznacz, aby określić zakres adresów do zezwolenia lub zablokowania. Użyj IPv4 / IPv6 w pozycji **Start** (Początek) i **End** (Koniec).
  - **Adres IP**: wpisz adres, który ma być przepuszczany lub blokowany. Użyj IPv4 / IPv6 lub formatu CIDR.
  - **Protocol (Protokół)**: wybierz protokół sieciowy (TCP, UDP lub oba), który ma być dozwolony lub blokowany. Po wybraniu protokołu należy również określić port.
  - **MAC (Adres MAC)**: Wprowadź adres MAC urządzenia, które ma lub nie ma mieć dostępu.
  - **Port range** (Zakres portów): zaznacz, aby określić zakres portów do zezwolenia lub zablokowania. Dodaj je w pozycjach **Start** (Początek) i **End** (Koniec).
  - **Port**: wpisz numer portu, który ma być przepuszczany lub blokowany. Numery portów muszą zawierać się w przedziale od 1 do 65535.
  - **Unit** (Rodzaj połączenia): wybierz rodzaj połączeń, które mają być dozwolone lub blokowane.
  - **Period** (Okres): wybierz okres związany z pozycją **Amount**.
  - **Amount** (Liczba): ustaw maksymalną liczbę połączeń, jaką urządzenie może ustanowić w ustawionym okresie **Period**. Maksymalna wartość to 65535.

- **Burst** (Przekroczenie): wpisz liczbę połączeń, dla których dozwolone jest jednokrotne przekroczenie ustawionej liczby **Amount** w ustawionym okresie **Period**. Po osiągnięciu tej liczby dozwolona jest tylko ustalona liczba w ustalonym okresie.
- **Traffic type** (Rodzaj ruchu): wybierz rodzaj ruchu, na który chcesz zezwolić lub który chcesz zablokować.
  - **UNICAST**: Ruch od jednego nadawcy do jednego odbiorcy.
  - **BROADCAST (TRANSMISJA)**: Ruch od jednego nadawcy do wszystkich urządzeń w sieci.
  - **MULTICAST**: Ruch od jednego lub więcej nadawców do jednego lub więcej odbiorców.

Test rules (Reguły testu): kliknij tę opcję, aby przetestować zdefiniowane reguły.

- **Test time in seconds** (Czas testu w sekundach): Pozwala ustawić limit czasu testowania reguł.
- **Roll back (Przywróć poprzednią wersję)**: kliknij, aby przywrócić zaporę sieciową do stanu sprzed przetestowania reguł.
- **Apply rules** (Zastosuj reguły): kliknij, aby uaktywnić reguły bez testowania. Nie zaleca się wykonywania tej czynności.

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 może działać tylko na określonym urządzeniu, które jest identyfikowane za pomocą unikatowego numeru seryjnego i identyfikatora układu. Tylko Axis może tworzyć niestandardowe podpisane certyfikaty AXIS OS, ponieważ to Axis ma klucz 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 urządzeń

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)**: Nie może zmieniać ustawień.

Menu kontekstowe zawiera opcje:

Update account (Zaktualizuj konto): Pozwala edytować właściwości konta.

Delete account (Usuń konto): Pozwala usunąć konto. Nie można usunąć konta root.

MQTT

MQTT (przesyłanie telemetryczne usługi kolejkowania wiadomości) to standardowy protokół do obsługi komunikacji w Internecie rzeczy (IoT). Został zaprojektowany z myślą o uproszczeniu integracji IoT i jest wykorzystywany w wielu branżach do podłączania urządzeń zdalnych przy jednoczesnej minimalizacji objętości kodu i obciążenia sieci. Klient MQTT w oprogramowaniu urządzeń Axis może ułatwiać integrację danych i zdarzeń generowanych w urządzeniu z systemami, które nie są oprogramowaniem do zarządzania materiałem wizyjnym (VMS).

Konfiguracja urządzenia jako klienta MQTT. Komunikacja MQTT oparta jest na dwóch jednostkach, klientach i brokerze. Klienci mogą wysyłać i odbierać wiadomości. Broker odpowiedzialny jest za rozsyłanie wiadomości między klientami.

Więcej informacji o protokole MQTT znajdziesz w *bazie wiedzy na temat systemu AXIS OS*.

ALPN

ALPN to rozszerzenie TLS/SSL umożliwiające wybranie protokołu aplikacji na etapie uzgadniania połączenia między klientem a serwerem. Służy do włączania ruchu MQTT przez port używany przez inne protokoły, takie jak HTTP. Czasami może nie być dedykowanego portu otwartego dla komunikacji MQTT. W takich przypadkach pomocne może być korzystanie z ALPN do negocjowania użycia MQTT jako protokołu aplikacji na standardowym porcie akceptowanym przez zapory sieciowe.

Klient MQTT

Connect (Połącz): włącz lub wyłącz klienta MQTT.

Status (Stan): pokazuje bieżący status klienta MQTT.

Broker

Host: wprowadź nazwę hosta lub adres IP serwera MQTT.

Protocol (Protokół): Wybierz protokół, który ma być używany.

Port: Wprowadź numer portu.

- 1883 to wartość domyślna ustawienia **MQTT over TCP (MQTT przez TCP)**
- 8883 to wartość domyślna dla **MQTT przez SSL**
- 80 to wartość domyślna dla **MQTT przez WebSocket**
- 443 to wartość domyślna dla **MQTT przez WebSocket Secure**

ALPN protocol (Protokół ALPN): Wprowadź nazwę protokołu ALPN dostarczoną przez dostawcę brokera MQTT. Dotyczy to tylko ustawień MQTT przez SSL i MQTT przez WebSocket Secure.

Username (Nazwa użytkownika): należy tu wprowadzić nazwę użytkownika, która będzie umożliwiać klientowi dostęp do serwera.

Password (Hasło): wprowadzić hasło dla nazwy użytkownika.

Client ID (Identyfikator klienta): Wprowadź identyfikator klienta. Identyfikator klienta jest wysyłany do serwera, gdy klient nawiązuje z nim połączenie.

Clean session (Czysta sesja): steruje zachowaniem w czasie połączenia i czasie rozłączenia. Po wybraniu tej opcji informacje o stanie są odrzucane podczas podłączania i rozłączania.

HTTP proxy (Serwer proxy HTTP): Adres URL o maksymalnej długości 255 bajtów. Jeśli nie chcesz używać serwera proxy HTTP, możesz zostawić to pole puste.

HTTPS proxy (Serwer proxy HTTPS): Adres URL o maksymalnej długości 255 bajtów. Jeśli nie chcesz używać serwera proxy HTTPS, możesz zostawić to pole puste.

Keep alive interval (Przedział czasowy KeepAlive): Umożliwia klientowi detekcję, kiedy serwer przestaje być dostępny, bez konieczności oczekiwania na długi limit czasu TCP/IP.

Timeout (Przekroczenie limitu czasu): interwał czasowy (w sekundach) pozwalający na zakończenie połączenia. Wartość domyślna: 60

Prefiks tematu urządzenia: Używany w domyślnych wartościach tematu w komunikacie łączenia i komunikacie LWT na karcie **MQTT client (Klient MQTT)** oraz w warunkach publikowania na karcie **MQTT publication (Publikacja MQTT)**.

Reconnect automatically (Ponowne połączenie automatyczne): określa, czy klient powinien ponownie połączyć się automatycznie po rozłączeniu.

Komunikat łączenia

określa, czy podczas ustanawiania połączenia ma być wysyłany komunikat.

Send message (Wysłanie wiadomości): włącz, aby wysyłać wiadomości.

Use default (Użyj domyślnych): wyłącz, aby wprowadzić własną wiadomość domyślną.

Topic (Temat): wprowadź temat wiadomości domyślnej.

Payload (Próbka): wprowadź treść wiadomości domyślnej.

Retain (Zachowaj): wybierz, aby zachować stan klienta w tym **Topic (Temacie)**

QoS: zmiana warstwy QoS dla przepływu pakietów.

Wiadomość Ostatnia Wola i Testament

Funkcja Last Will Testament (LWT) zapewnia klientowi dostarczenie informacji wraz z poświadczeniami w momencie łączenia się z brokerem. Jeżeli klient nie rozłączy się w pewnym momencie w późniejszym terminie (może to być spowodowane brakiem źródła zasilania), może umożliwić brokerowi dostarczenie komunikatów do innych klientów. Ten komunikat LWT ma taką samą postać jak zwykła wiadomość i jest kierowany przez tę samą mechanikę.

Send message (Wysłanie wiadomości): włącz, aby wysyłać wiadomości.

Use default (Użyj domyślnych): wyłącz, aby wprowadzić własną wiadomość domyślną.

Topic (Temat): wprowadź temat wiadomości domyślnej.

Payload (Próbka): wprowadź treść wiadomości domyślnej.

Retain (Zachowaj): wybierz, aby zachować stan klienta w tym **Topic (Temacie)**

QoS: zmiana warstwy QoS dla przepływu pakietów.

Publikacja MQTT

Użyj domyślnego prefiksu: Wybierz ustawienie, aby używać domyślnego prefiksu zdefiniowanego za pomocą prefiksu urządzenia w zakładce **MQTT client (Klient MQTT)**.

Include condition (Uwzględnij warunek): Wybierz, aby do tematu MQTT dołączać tematy opisujące warunek.

Include namespaces (Uwzględnij przestrzenie nazw): Wybierz, aby do tematu MQTT dołączać przestrzenie nazw tematów ONVIF.

Include serial number (Uwzględnij numer seryjny): Wybierz, aby w danych właściwych usługi MQTT umieszczać numer seryjny urządzenia.

Dodaj condition (Dodaj warunek): Kliknij, aby dodać warunek.

Retain (Zachowaj): Definiuje, które komunikaty MQTT mają być wysyłane jako zachowywane.

- **None (Żaden)**: Wysyłanie wszystkich komunikatów jako niezachowywanych.
- **Property (Właściwość)**: Wysyłanie tylko komunikatów ze stanem jako zachowywanych.
- **All (Wszystkie)**: Wysyłanie komunikatów ze stanem i bez stanu jako zachowywanych.

QoS: Wybierz żądany poziom publikacji MQTT.

Subskrypcje MQTT

Add subscription (Dodaj subskrypcję): Kliknij, aby dodać nową subskrypcję usługi MQTT.

Subscription filter (Filtr subskrypcyjny): Wprowadź temat MQTT, który chcesz subskrybować.

Uwaga

Jeśli edytujesz filtr subskrypcji, pamiętaj, aby zaktualizować powiązane zdarzenia.

Use device topic prefix (Użyj prefiksu tematu urządzenia): Dodaj filtr subskrypcji jako prefiks do tematu MQTT.

Subscription type (Typ subskrypcji):

- **Stateless (Bez stanu)**: Wybierz, aby przekształcać komunikaty MQTT na komunikaty bezstanowe.
- **Stateful (Ze stanem)**: Wybierz, aby przekształcać komunikaty MQTT na warunek. Dane właściwe będą służyły do określania stanu.

QoS: Wybierz żądany poziom subskrypcji MQTT.

Akcesoria

Porty we/wy

Użyj wejścia cyfrowego do podłączenia zewnętrznych urządzeń, które mogą przełączać się pomiędzy obwodem zamkniętym i otwartym, na przykład czujników PIR, czujników okien lub drzwi oraz czujników wykrywania zbicia szyby.

Użyj wyjścia cyfrowego do podłączenia urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączone urządzenia można aktywować poprzez interfejs programowania aplikacji VAPIX® lub w interfejsie WWW.

Port

Name (Nazwa): edytuj tekst, aby zmienić nazwę portu.

Direction (Kierunek):  wskazuje, że port jest portem wejścia.  wskazuje, że jest to port wyjścia. Jeśli port jest konfigurowalny, można kliknąć ikony, aby przełączać się między wejściem a wyjściem.

Normal state (Stan normalny): Kliknij opcję  w przypadku obwodu otwartego i  w przypadku obwodu zamkniętego.

Current state (Bieżący stan): wyświetla bieżący stan portu. Wejście lub wyjście jest aktywowane w momencie zmiany bieżącego stanu na inny niż stan normalny. Obwód wejścia urządzenia jest otwarty po odłączeniu lub doprowadzeniu napięcia powyżej 1 V DC.

Uwaga

Podczas ponownego uruchomienia obwód pozostaje otwarty. Po ponownym uruchomieniu obwód powraca do pozycji normalnej. Po zmianie ustawień na tej stronie obwody wyjść powracają do normalnych pozycji, niezależnie od aktywnych wyzwalaczy.

Supervised (Nadzorowane): włącz, aby umożliwić wykrywanie i wyzwalanie działań, jeśli ktoś manipuluje przy połączeniu z cyfrowymi urządzeniami We/Wy. Oprócz wykrywania, czy wejście jest otwarte lub zamknięte, można również wykryć, czy ktoś przy nim manipulował (tzn. przeciął lub doprowadził do zwarcia). Nadzorowanie połączenia wymaga dodatkowego sprzętu (rezystorów końcowych) w zewnętrznej pętli We./Wy.

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 służy do utworzenia pliku ZIP, który zawiera pełny raport o serwerze w pliku tekstowym w formacie UTF–8. Aby dołączyć zrzut ekranu bieżącego obrazu w podglądzie na żywo, wybierz opcję **Include image (Dołącz obraz)**. 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.
- **View the audit log (Wyświetl dziennik kontroli)**: Kliknij, aby wyświetlić informacje o działaniach użytkownika i systemu, na przykład o pomyślnych lub nieudanych uwierzytelnieniach i konfiguracjach.

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)**.

Zdalny dziennik systemu

Syslog to standard rejestrowania 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 komunikatów Syslog, 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.

Type (Typ): wybierz rodzaj dzienników do wysłania.

Test server setup (Testuj ustawienia serwera): wyślij wiadomość testową do wszystkich serwerów przed zapisaniem ustawień.

CA certificate set (Certyfikat CA ustawiony): Umożliwia wyświetlenie aktualnych ustawień lub dodanie certyfikatu.

Konserwacja

Restart (Uruchom ponownie): Ponowne uruchamianie urządzenia. 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.
- **Automatic rollback** (Automatyczne przywracanie): 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.

T10125657_pl

2026-09 (M15.3)

© 2018 – 2026 Axis Communications AB