

AXIS A8207-VE Mk II Network Video Door Station

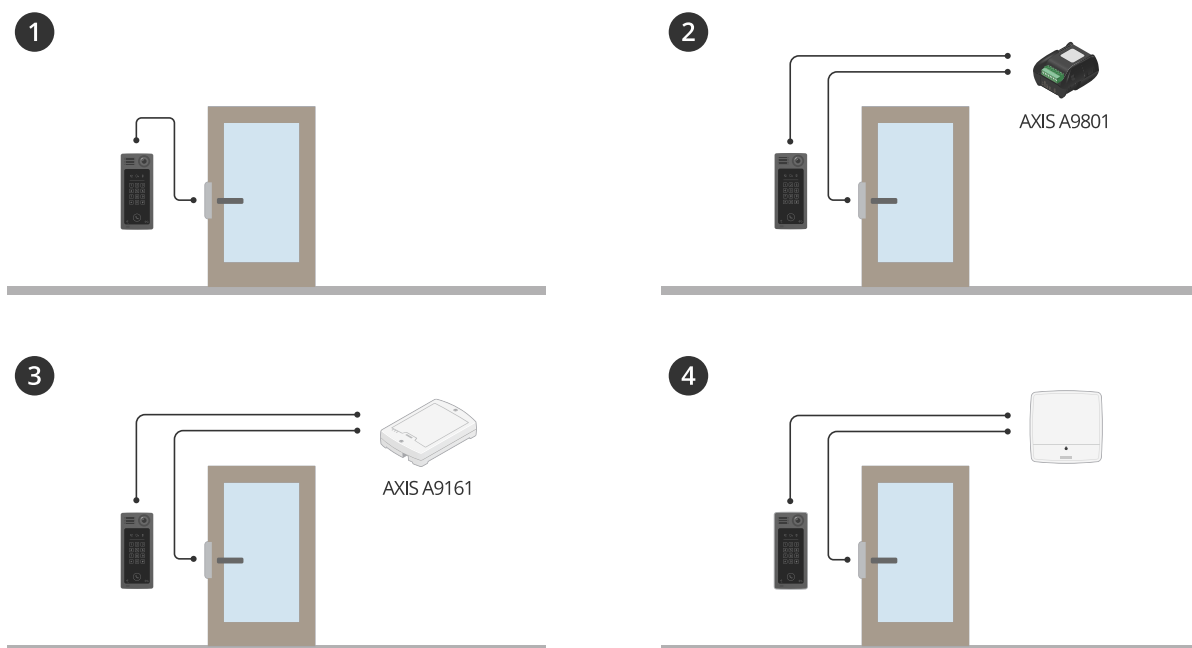
Podręcznik użytkownika

Spis treści

Informacje o rozwiązaniu.....	4
Przegląd produktów	5
Instalacja.....	7
Od czego zacząć	8
Wyszukiwanie urządzenia w sieci.....	8
Obsługiwane przeglądarki.....	8
Otwórz interfejs WWW urządzenia.....	8
Utwórz konto administratora.....	8
Bezpieczne hasła.....	9
Upewnianie się co do braku zmian w oprogramowaniu urządzenia	9
Omówienie interfejsu WWW	9
Ustawienia dodatkowe	10
Zmiana hasła root	10
Kalibracja i przeprowadzanie zdalnego testu głośnika	10
Konfiguracja bezpośredniego połączenia SIP (P2P).....	10
Konfiguracja SIP przez serwer (PBX).....	11
Tworzenie kontaktu	12
Konfiguracja przycisku połączenia.....	12
Konfigurowanie jako czytnik.....	12
Użyj listy wejść, aby zezwolić osobom mającym poświadczenia na otwarcie drzwi.....	13
Konfigurowanie jako czytnika kart przy użyciu kontrolera drzwi	13
Stosuj dane chronione na kartach, aby zwiększyć bezpieczeństwo	14
Korzystanie z DTMF do otwierania drzwi.....	15
Przesyłanie wideo do monitora	15
Interfejs WWW.....	16
Więcej informacji.....	17
Voice over IP (VoIP)	17
Protokół inicjacji sieci (Session Initiation Protocol, SIP).....	17
Peer-to-peer SIP (P2PSIP).....	17
Private Branch Exchange (PBX) – centrala abonencka.....	18
Konfiguracja reguł dotyczących zdarzeń	19
Analizy i aplikacje	19
AXIS Client for Unified Communication Systems	19
Dzienne wykorzystanie	20
Używanie klawiatury	20
Rozwiązywanie problemów –	21
Przywróć domyślne ustawienia fabryczne	21
Sprawdzanie bieżącej wersji systemu AXIS OS	21
Aktualizacja systemu AXIS OS:.....	21
Problemy techniczne, wskazówki i rozwiązania.....	22
Kwestie wydajności	23
Specyfikacje	24
Wskaźniki i elementy sterowania na panelu przednim	24
Ikony wskaźników.....	24
Pasek wskaźnika czytnika kart.....	24
Przycisk połączenia	24
Wskaźniki LED.....	24
Gniazdo karty SD.....	24
Przyciski	24
Przycisk kontrolny.....	24
Złącza.....	25
Złącze HDMI	25
Złącze sieciowe	25

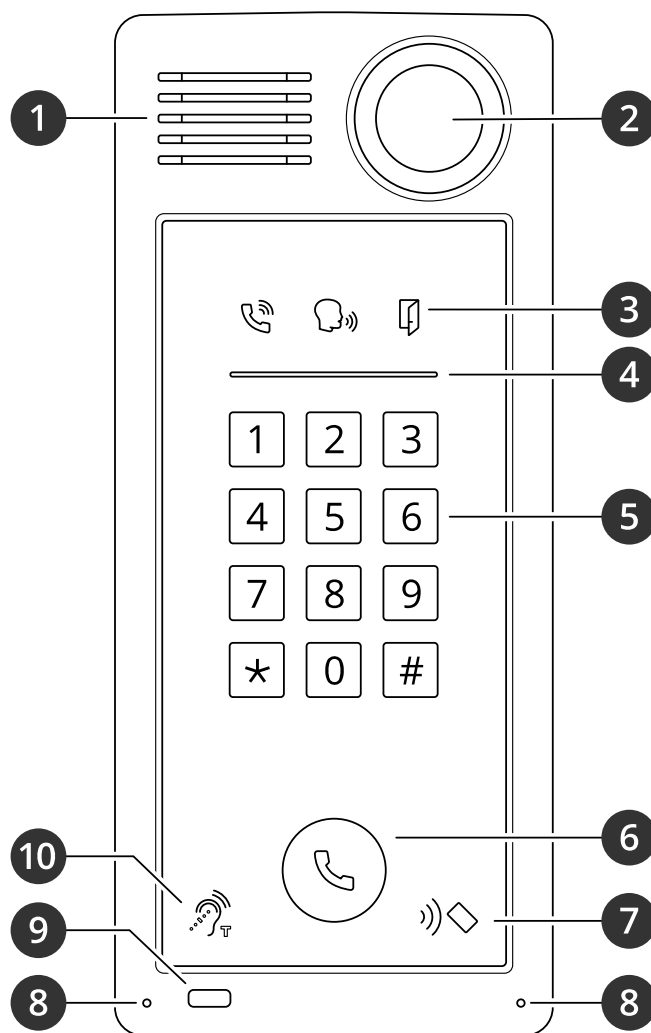
Złącze audio.....	25
Złącze przekaźnikowe.....	25
Złącze czytnika.....	26
Złącze I/O	26
Złącze zasilania	27
Informacje dotyczące bezpieczeństwa.....	28
Poziomy zagrożenia.....	28
Inne poziomy komunikatów.....	28
Cyberbezpieczeństwo	29
Postępowanie z lukami w zabezpieczeniach	29
Powiadomienia dotyczące zabezpieczeń	29
Bezpieczny cykl eksploatacji produktu	29

Informacje o rozwiązaniu

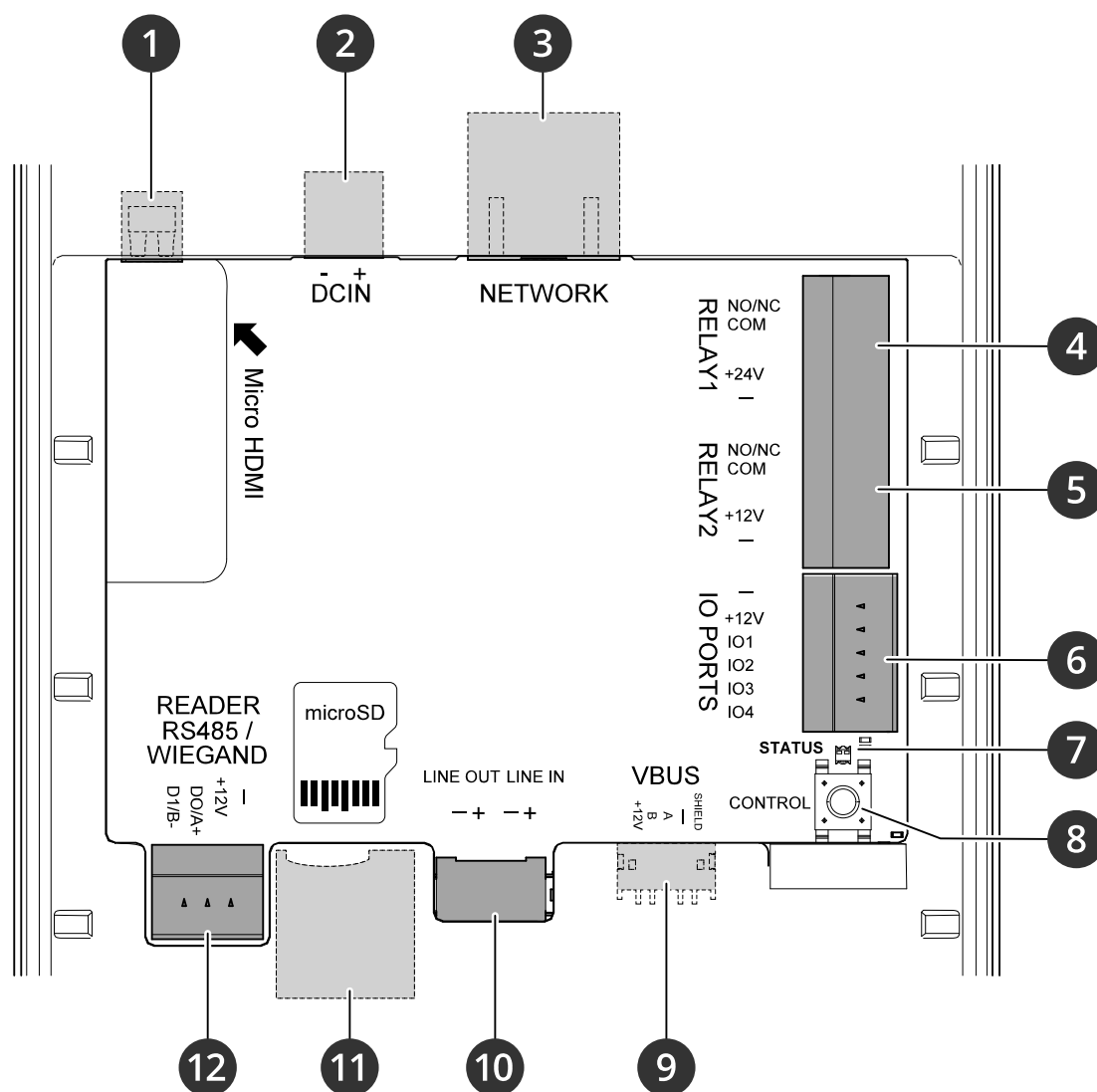


- 1 Wideodomofon
- 2 Wideodomofon i AXIS A9801
- 3 Wideodomofon i AXIS A9161
- 4 Wideodomofon z systemem kontroli dostępu, na przykład AXIS A1001 lub AXIS A1601

Przegląd produktów



- 1 Głośnik
- 2 Kamera
- 3 Ikony wskaźników, on page 24
- 4 Pasek wskaźnika czytnika kart, on page 24
- 5 Klawiatura numeryczna
- 6 Przycisk połączenia, on page 24
- 7 Ikona czytnika kart
- 8 Mikrofon
- 9 Czujnik PIR
- 10 Ikona pętli indukcyjnej



- 1 Złącze HDMI, on page 25 (microHDMI)
- 2 Złącze zasilania, on page 27
- 3 Złącze sieciowe, on page 25 (PoE+)
- 4 Złącze przekaźnikowe, on page 25
- 5 Złącze przekaźnikowe, on page 25
- 6 Złącze I/O, on page 26
- 7 Dioda stanu
- 8 Przycisk kontrolny, on page 24
- 9 2N VBUS (nieużywane)
- 10 Złącze audio, on page 25
- 11 Gniazdo karty SD, on page 24 (microSD/microSDHC/microSDXC)
- 12 Złącze czytnika, on page 26

Instalacja



Aby obejrzeć ten film wideo, przejdź do internetowej wersji dokumentu.

Film dotyczący instalacji czytnika A8207-VE.



Aby obejrzeć ten film wideo, przejdź do internetowej wersji dokumentu.

Film dotyczący instalacji przekaźnika A8207-VE.

Od czego zacząć

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*.

Obsługiwane przeglądarki

Urządzenie obsługuje następujące przeglądarki:

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

✓: zalecane

*: obsługiwane z ograniczeniami

Otwórz interfejs WWW urządzenia

1. Otwórz przeglądarkę i wpisz adres IP lub nazwę hosta urządzenia Axis. Jeśli nie znasz adresu IP, użyj narzędzia AXIS IP Utility lub AXIS Device Manager, aby zlokalizować urządzenie w sieci.
2. Wprowadź nazwę użytkownika i hasło. Jeśli korzystasz z urządzenia po raz pierwszy, musisz utworzyć konto administratora. Patrz *Utwórz konto administratora*, on page 8.

Opisy wszystkich funkcji i ustawień interfejsu WWW urządzeń z systemem operacyjnym AXIS OS można znaleźć na stronie *Pomoc dotycząca interfejsu internetowego AXIS OS*.

Utwórz konto administratora

Przy pierwszym logowaniu do urządzenia należy utworzyć konto administratora.

1. Wprowadź nazwę użytkownika.
2. Wprowadź hasło. Patrz *Bezpieczne hasła*, on page 9.
3. Wprowadź ponownie hasło.
4. Zaakceptuj umowę licencyjną.
5. Kliknij kolejno opcje **Add account (Dodaj konto)**.

Ważne

W urządzeniu nie ma konta domyślnego. Jeśli nastąpi utrata hasła do konta administratora, należy zresetować urządzenie. Patrz *Przywróć domyślne ustawienia fabryczne*, on page 21.

Bezpieczne hasła

Ważne

Używaj protokołu HTTPS (który jest domyślnie włączony), aby ustawić hasło lub skonfigurować inne poufne dane przez sieć. Protokół HTTPS umożliwia nawiązywanie bezpiecznych, szyfrowanych połączeń sieciowych, 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.

Upewnianie się co do braku zmian w oprogramowaniu urządzenia

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

1. Przywróć domyślne ustawienia fabryczne. Patrz *Przywróć domyślne ustawienia fabryczne, on page 21*. Po zresetowaniu opcja bezpiecznego uruchamiania gwarantuje bezpieczeństwo urządzenia.
2. Skonfiguruj i zainstaluj urządzenie.

Omówienie interfejsu WWW

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



Interfejs WWW urządzenia Axis

Ustawienia dodatkowe

W tej części zostały opisane wszystkie ważne konfiguracje, które musi przeprowadzić instalator, aby uruchomić produkt po zakończeniu montażu sprzętu.

Zmiana hasła root

1. Zaloguj się w interfejsie urządzenia i przejdź do menu **System > Users (System > Użytkownicy)**.
2. W przypadku użytkownika głównego kliknij kolejno opcje  > **Update user (Aktualizuj użytkownika)**.
3. Wprowadź nowe hasło i zapisz je.

Kalibracja i przeprowadzanie zdalnego testu głośnika

Za pomocą testu głośnika można z odległości sprawdzić, czy głośnik działa w oczekiwany sposób. Test głośnika to seria dźwięków testowych rejestrowanych przez wbudowany mikrofon. Po każdym przeprowadzeniu testu zarejestrowane wartości są porównywane z wartościami zarejestrowanymi podczas kalibracji.

Uwaga

Kalibrację do testu należy wykonać w położeniu montażowym na miejscu instalacji. Jeśli głośnik zostanie przesunięty lub jego lokalne otoczenie ulegnie zmianie, na przykład, jeśli ściana zostanie zbudowana lub usunięta, głośnik należy ponownie skalibrować.

Podczas kalibracji zaleca się, aby ktoś był fizycznie obecny na miejscu instalacji, aby odsłuchać sygnały testowe i upewnić się, że dźwięki testu nie są stłumione ani zablokowane przez jakiegokolwiek niezamierzone przeszkody na ścieżce akustycznej głośnika.

1. Przejdź do interfejsu urządzenia > **Audio > Speaker test (Dźwięk > Test głośnika)**.
2. Aby skalibrować urządzenie audio, kliknij przycisk **Calibrate (Kalibruj)**.

Uwaga

Po kalibracji produktu Axis można w dowolnym momencie przeprowadzić test głośnika.

3. Aby przetestować głośnik, kliknij przycisk **Run the test (Uruchom test)**.

Uwaga

Inny sposób zainicjowania kalibracji to naciśnięcie przycisku kontrolnego na fizycznym urządzeniu. Znajdowanie pliku Control: *Przegląd produktów*, on page 5.

Konfiguracja bezpośredniego połączenia SIP (P2P)

VoIP (Voice over IP) to grupa technologii, która umożliwia komunikację głosową i multimedialną w sieciach IP. Więcej informacji znajduje się w rozdziale *Voice over IP (VoIP)*, on page 17.

W tym urządzeniu komunikację VoIP umożliwia protokół SIP. Więcej informacji dotyczących protokołu SIP: *Protokół inicjacji sieci (Session Initiation Protocol, SIP)*, on page 17

Istnieją dwa rodzaje konfiguracji protokołu SIP. Jednym z nich jest łączność bezpośrednia czyli peer-to-peer (P2P). Konfiguracji P2P należy używać wtedy, gdy komunikacja odbywa się pomiędzy niewielką liczbą agentów użytkownika w tej samej sieci IP i nie ma potrzeby zapewniania dodatkowych funkcji serwera PBX. Informacje na temat konfiguracji: *Peer-to-peer SIP (P2PSIP)*, on page 17.

1. Przejdź do menu **Communication > SIP > Settings (Komunikacja > SIP > Ustawienia)** i wybierz opcję **Enable SIP (Włącz SIP)**.
2. Aby zezwolić urządzeniu na odbieranie połączeń, wybierz opcję **Zezwalaj na połączenia przychodzące**.

POWIADOMIENIE

Po zezwoleniu na połączenia przychodzące urządzenie akceptuje połączenia z dowolnego urządzenia podłączonego do sieci. Zalecamy blokowanie połączeń przychodzących w przypadku produktów dostępnych z sieci publicznych lub Internetu.

3. Kliknij opcję **Call handling (Obsługa połączeń)**.
4. Ustaw maksymalny czas połączenia w przypadku braku odpowiedzi w opcji **Limit czasu nawiązywania połączenia**.
5. Jeżeli zezwalasz na połączenia przychodzące, w polu **Incoming call timeout (Limit czasu połączenia przychodzącego)** ustaw liczbę sekund limitu czasu dla takich połączeń.
6. Kliknij opcję **Ports (Porty)**.
7. Wprowadź numer portu **Port SIP** i numer portu **Port TLS**.

Uwaga

- **Port SIP** – dla sesji SIP. Ruch sygnalizacyjny przez ten port nie jest szyfrowany. Domyślny numer portu to 5060.
 - **Port TLS** – dla sesji SIPs oraz sesji SIP zabezpieczonych protokołem TLS. Ruch sygnalizacyjny za pośrednictwem tego portu jest szyfrowany przy użyciu Transport Layer Security (TLS). Domyślny numer portu to 5061.
 - **Port początkowy RTP** – port używany do pierwszego strumienia mediów RTP w wywołaniu SIP. Domyślny numer portu to 4000. Niektóre zapory mogą blokować ruch RTP na niektórych numerach portów. Numer portu musi być w przedziale od 1024 do 65535.
8. Kliknij opcję **NAT traversal**.
 9. Wybierz protokoły, które chcesz włączyć dla funkcji NAT traversal.

Uwaga

Użyj opcji NAT traversal, gdy urządzenie jest podłączone do sieci za routerem NAT lub znajduje się za zaporą. Więcej informacji znajduje się w rozdziale .

10. Kliknij przycisk **Zapisz**.

Konfiguracja SIP przez serwer (PBX)

VoIP (Voice over IP) to grupa technologii, która umożliwia komunikację głosową i multimedialną w sieciach IP. Więcej informacji znajduje się w rozdziale *Voice over IP (VoIP)*, on page 17.

W tym urządzeniu komunikację VoIP umożliwia protokół SIP. Więcej informacji dotyczących protokołu SIP: *Protokół inicjacji sieci (Session Initiation Protocol, SIP)*, on page 17

Istnieją dwa rodzaje konfiguracji protokołu SIP. Jednym z nich jest serwer PBX. Konfiguracji PBX należy używać wtedy, gdy komunikacja odbywa się pomiędzy nieograniczoną liczbą agentów użytkownika w tej samej sieci IP i poza nią. W zależności od dostawcy usługi PBX można dodać dodatkowe funkcje. Więcej informacji znajduje się w rozdziale *Private Branch Exchange (PBX) – centrala abonencka*, on page 18.

1. Od dostawcy PBX należy uzyskać następujące informacje:
 - ID użytkownika
 - Domena
 - Hasło
 - ID uwierzytelniania
 - ID rozmówcy
 - Rejestrator
 - Port początkowy RTP
2. Wybierz kolejno opcje **Communication > SIP > Accounts (Komunikacja > SIP > Konta)** i kliknij przycisk **+ Add account (+ Dodaj konto)**.
3. Wprowadź **Nazwę konta**.
4. Kliknij opcję **Registered (Zarejestrowane)**.
5. Wybierz tryb transmisji.

6. Podaj dane konta uzyskane od dostawcy serwera PBX.
7. Kliknij przycisk **Zapisz**.
8. Skonfiguruj ustawienia SIP w taki samo sposób, jak peer-to-peer – zobacz *Konfiguracja bezpośredniego połączenia SIP (P2P)*, on page 10. Użyj portu początkowego RTP od dostawcy PBX.

Tworzenie kontaktu

W tym przykładzie wyjaśniono sposób tworzenia nowego kontaktu w liście kontaktów. Zanim rozpoczniesz, włącz obsługę protokołu SIP w ustawieniu **Communication > SIP (Komunikacja > SIP)**.

Aby utworzyć nowy kontakt:

1. Przejdź do **Communication > Contact list (Komunikacja > Lista kontaktów)**.
2. Kliknij przycisk **+ Add contact (+ Dodaj kontakt)**.
3. Wprowadź imię i nazwisko kontaktu.
4. Wprowadź adres SIP kontaktu.

Uwaga

Więcej informacji dotyczących adresów SIP: *Protokół inicjacji sieci (Session Initiation Protocol, SIP)*, on page 17.

5. Wybierz konto SIP do wykonania połączenia.

Uwaga

Opcje dostępności konfiguruje się w oknie **System > Events (Zdarzenia) > Schedules (Harmonogramy)**.

6. W polu **Availability (Dostępność)** określ dostępność kontaktu. Jeżeli w czasie niedostępności kontaktu nastąpi próba nawiązania połączenia, połączenie zostanie anulowane, chyba że ustawiono kontakt rezerwowany.

Uwaga

Jest to kontakt, do którego przekierowywane jest połączenie w razie nieodebrania lub niedostępności odbiorcy.

7. W obszarze **Przekierowanie** wybierz opcję **Brak**.
8. Kliknij przycisk **Zapisz**.

Konfiguracja przycisku połączenia

Przycisk połączenia jest domyślnie skonfigurowany tak, aby nawiązywać połączenia przez VMS (oprogramowanie do zarządzania materiałem wideo). Aby zachować taką konfigurację, wystarczy dodać do systemu VMS interkom Axis.

W tym przykładzie wyjaśniono sposób konfigurowania systemu tak, by po na ciśnięciu przycisku połączenia przez gościa wykonywane było połączenie na numer kontaktu z listy kontaktów.

1. Wybierz kolejno **Communication > Calls > Call button (Komunikacja > Połączenia > Przycisk Połącz)**.
2. W obszarze **Recipients (Odbiorcy)** usuń VMS.
3. W obszarze **Recipients (Odbiorcy)** wybierz istniejący kontakt lub utwórz nowy.

Aby wyłączyć przycisk nawiązywania połączenia, wyłącz opcję **Enable call button (Włącz przycisk połączenia)**.

Konfigurowanie jako czytnik

Można skonfigurować wideodomofon jako czytnik, aby umożliwić posiadaczom poświadczeń otwieranie drzwi.

Korzystając z listy wejść, wideodomofon przechowuje poświadczenia lokalnie i może działać jako samodzielny czytnik dla maksymalnie pięćdziesięciu posiadaczy poświadczeń.

Gdy wideodomofon zostanie podłączony do kontrolera drzwi, może nadal przechowywać do pięćdziesięciu poświadczeń, a jeśli żądane poświadczenie znajduje się na liście wejść, wideodomofon zarządza uprawnieniami dostępu. Jeśli żądane poświadczenie nie znajduje się na liście wejść, a opcja **Use connected door controller** (**Użyj podłączonego kontrolera drzwi**) jest włączona, żądanie jest przekazywane do kontrolera drzwi, który następnie zarządza uprawnieniami dostępu.

Użyj listy wejść, aby zezwolić osobom mającym poświadczenia na otwarcie drzwi.

Za pomocą listy wejść można umożliwić posiadaczom poświadczeń korzystanie z ich poświadczeń do wyzwalania akcji, takich jak otwieranie drzwi. W tym przykładzie wyjaśniamy, jak dodać posiadacza poświadczeń, który może użyć swojej karty do otwarcia drzwi 10 razy.

Wymagania wstępne

- W menu **Reader > Chip types** (**Czytnik > Typy chipów**) musi być aktywny odpowiedni typ chipu.

Włącz funkcję listy wejść i dodaj posiadacza poświadczeń:

1. Otwórz menu **Reader > Entry list** (**Czytnik > Lista wejść**).
2. Włącz opcję **Use Entry list** (**Użyj listy wejść**).
3. Kliknij pozycję **+ Add credential holder** (**+ Dodaj posiadacza poświadczeń**).
4. Wprowadź imię i nazwisko posiadacza poświadczeń. Imię musi być unikatowe.
5. Wybierz pozycję **Card** (**Karta**).
6. Przesuń kartą posiadacza w urządzeniu i kliknij **Get latest** (**Pobierz najnowsze**).
7. Nie zmieniaj warunku **Access granted** (**Przyznano dostęp**).
8. W obszarze **Valid to** (**Ważne do**) wybierz **Number of times** (**Ile razy**).
9. W polu **Number of times** (**Ile razy**) wprowadź **10**.
10. Kliknij przycisk **Zapisz**.

Create a rule (Utwórz regułę):

1. Przejdź do **System > Events** (**System > Zdarzenia**).
2. W menu **Rules** (**Reguły**) kliknij **+ Add a rule** (**+ Dodaj regułę**).
3. W polu **Name** (**Nazwa**) wprowadź **Otwórz drzwi**.
4. Na liście warunków wybierz **Entry list > Access granted** (**Lista wejść > Przyznano dostęp**).
5. Z listy akcji wybierz opcję **I/O > Toggle I/O once** (**Toggle I/O once** (**We/Wy > Przełącz raz We/Wy**)).
6. Z listy portów wybierz opcję **Door** (**Drzwi**).
7. W menu **State** (**Status**) wybierz **Active** (**Aktywne**).
8. Ustaw czas trwania jako **00:00:07**.
9. Kliknij przycisk **Zapisz**.

Konfigurowanie jako czytnika kart przy użyciu kontrolera drzwi

Połączenie sieciowe

Aby użyć wideodomofonu jako czytnika kart, można podłączyć go do kontrolera drzwi. Kontroler drzwi przechowuje wszystkie poświadczenia i zapisuje informacje dotyczące osób upoważnionych do wejścia. W tym przykładzie urządzenia podłączymy w sieci. Zmodyfikujemy również dozwolone typy kart.

Ważne

Połączenie sieciowe działa wyłącznie z kontrolerami drzwi Axis. Aby połączyć się z kontrolerem drzwi firmy innej niż Axis, należy podłączyć urządzenia przewodowo. Patrz *Połączenie przewodowe, on page 14*.

Konfiguracja wideodomofonu jako czytnika kart

1. Przejdź do obszaru **Reader** (**Czytnik**) > **Connection** (**Połączenie**).

2. Wybierz typ protokołu **Czytnik VAPIX**.
3. Wybierz protokół komunikacji z kontrolerem drzwi.

Uwaga

Jeżeli jest używany protokół **HTTPS**, zalecamy włączenie opcji **Zweryfikuj certyfikat**.

4. Wprowadź adres IP kontrolera drzwi.
5. Wprowadź poświadczenia kontrolera drzwi.
6. Kliknij przycisk **Połącz**.
7. Wybierz czytnik wejścia dla odpowiednich drzwi.
8. Kliknij przycisk **Zapisz**.

Połączenie przewodowe

Aby użyć wideodomofonu jako czytnika kart, można podłączyć go do kontrolera drzwi. Kontroler drzwi przechowuje wszystkie poświadczenia i zapisuje informacje dotyczące osób upoważnionych do wejścia. W tym przykładzie podłączymy urządzenia przewodowo, korzystając z protokołu Wiegand, aktywujemy sygnał dźwiękowy i użyjemy jednego portu I/O na potrzeby wskaźnika LED. Zmodyfikujemy też dozwolone typy kart.

Ważne

Użyj portów I/O, które nie są jeszcze używane. Jeżeli użyjesz portów I/O będących w użyciu, zdarzenia utworzone dla tych portów przestaną być aktywne.

Zanim rozpoczniesz

- Podłącz wideodomofon do kontrolera drzwi.
Zapoznaj się z rysunkami okablowania elektrycznego, które można pobrać ze strony axis.com/products/axis-a8207-ve-mk-ii/support.
- Skonfiguruj kontroler drzwi, używając protokołu Wiegand dla czytnika. Instrukcje znajdują się w instrukcji obsługi kontrolera drzwi.

Konfiguracja wideodomofonu jako czytnika kart

1. Przejdź do obszaru **Reader (Czytnik) > Connection (Połączenie)**.
2. Wybierz **Wiegand** jako typ protokołu.
3. Włącz ustawienie **Sygnał dźwiękowy**.
4. W obszarze **Wejście sygnału dźwiękowego** wybierz opcję **I3**.
5. W obszarze **Input used for LED control (Wejście sterowania LED)** wybierz **1**.
6. W obszarze **Wejście LED1** wybierz **I1**.
7. Wybierz kolory dla każdego stanu.
8. W ustawieniu **Format naciśnięcia klawisza** zaznacz wartość **Czterobitowy**.
9. Kliknij przycisk **Zapisz**.
10. Wybierz kolejno opcje **Czytnik > Typy chipów** i aktywuj rodzaje mikroukładów, które mają być używane.

Uwaga

Można zachować domyślny zestaw typów mikroukładów, ale zalecamy zmodyfikowanie listy zgodnie z własnymi potrzebami.

11. Kliknij przycisk **Dodaj zestaw danych**, aby określić zestawy danych dla różnych rodzajów mikroukładów.
12. Kliknij przycisk **Zapisz**.

Stosuj dane chronione na kartach, aby zwiększyć bezpieczeństwo

W celu zwiększenia bezpieczeństwa systemu kontroli dostępu można używać bezpiecznych danych zapisanych na niektórych typach kart. Dane są zabezpieczone kluczem tajnym. Do odczytania danych karty konieczne jest zapisane w urządzeniu klucza tajnego oraz innych informacji o karcie.

1. Przejdź do menu **Reader > Chip types (Czytnik > Typy chipów)**.
2. W obszarze **Data sets (Zestawy danych)** zaznacz typ chipu, który chcesz zmodyfikować, i kliknij **Add data set (Dodaj zestaw danych)**.
3. Wprowadź dane karty. Typ wprowadzanych informacji zależy od rodzaju karty i sposobu rejestracji kart.
4. W przypadku korzystania z protokołów OSDP lub Wiegand wybierz **Use as UID (Użyj jako UID)**, aby wysłać bezpieczne dane jako UID/CSN, zamiast normalnego UID/CSN karty.
5. Aby umożliwić przesyłanie do kontrolera dostępu wyłącznie kart zgodnych z określonymi danymi karty, wybierz opcję **Required data (Wymagane dane)**. Niezgodne karty będą cicho ignorowane przez czytnik.
6. Kliknij przycisk **Zapisz**.

Korzystanie z DTMF do otwierania drzwi

Kiedy gość dzwoni wideodomofonem, osoba, która odbierze połączenie, może wykorzystać sygnał (DTMF) urządzenia SIP do odblokowania drzwi. Kontroler drzwi odblokowuje i blokuje drzwi.

W tym przykładzie wyjaśniono, jak:

- zdefiniować sygnał DTMF w wideodomofonie;
- skonfigurować wideodomofon, aby:
 - żądać odblokowania drzwi, lub
 - otwierać drzwi przy użyciu przekaźnika wewnętrznego.

Wszystkie ustawienia należy wprowadzić na stronie internetowej wideodomofonu.

Zanim rozpocznieś

- Zezwól na połączenia SIP wychodzące z urządzenia i załóż konto SIP. Patrz *Konfiguracja bezpośredniego połączenia SIP (P2P)*, on page 10 i *Konfiguracja SIP przez serwer (PBX)*, on page 11.

Definiowanie sygnału DTMF w wideodomofonie

1. Przejdź do menu **Communication > SIP > DTMF (Komunikacja > SIP > DTMF)**.
2. Kliknij **+ Add sequence (Dodaj sekwencję)**.
3. W polu **Sequence (Sekwencja)** wprowadź **1**.
4. W polu **Opis** wprowadź **Odblokowanie drzwi**.
5. W polu **Accounts (Konta)** wybierz konto SIP.
6. Kliknij przycisk **Zapisz**.

Skonfiguruj wideodomofon do otwierania drzwi za pomocą przekaźnika wewnętrznego

7. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i dodaj regułę.
8. W polu **Name (Nazwa)** wprowadź **Odblokowanie drzwi przez DTMF**.
9. Z listy warunków w obszarze **Call (Połączenie)** wybierz kolejno opcje **DTMF** i **Unlock door (Odblokuj drzwi)**.
10. Z listy akcji w obszarze **I/O (We/Wy)** wybierz opcję **Toggle I/O once (Przełącz raz WE/WY)**.
11. Z listy portów wybierz **Relay 1 (Przekaźnik 1)**.
12. W polu **Duration (Czas trwania)** zmień wartość na **00:00:07**, co oznacza, że drzwi będą pozostawać otwarte przez 7 sekund.
13. Kliknij przycisk **Zapisz**.

Przesyłanie wideo do monitora

Urządzenie może przysyłać strumień wideo na żywo do monitora HDMI bez połączenia sieciowego. Użyj monitora, aby sprawdzić, kto stoi przed drzwiami.

1. Podłącz monitor zewnętrzny za pomocą złącza HDMI.
2. Dostosuj ustawienia HDMI w oknie **System > Wyjście wideo**.

Interfejs WWW

Aby zapoznać się ze wszystkimi funkcjami i ustawieniami dostępnymi w interfejsie WWW urządzeń z systemem operacyjnym AXIS OS, przejdź do strony *Pomoc dotycząca interfejsu internetowego AXIS OS*.

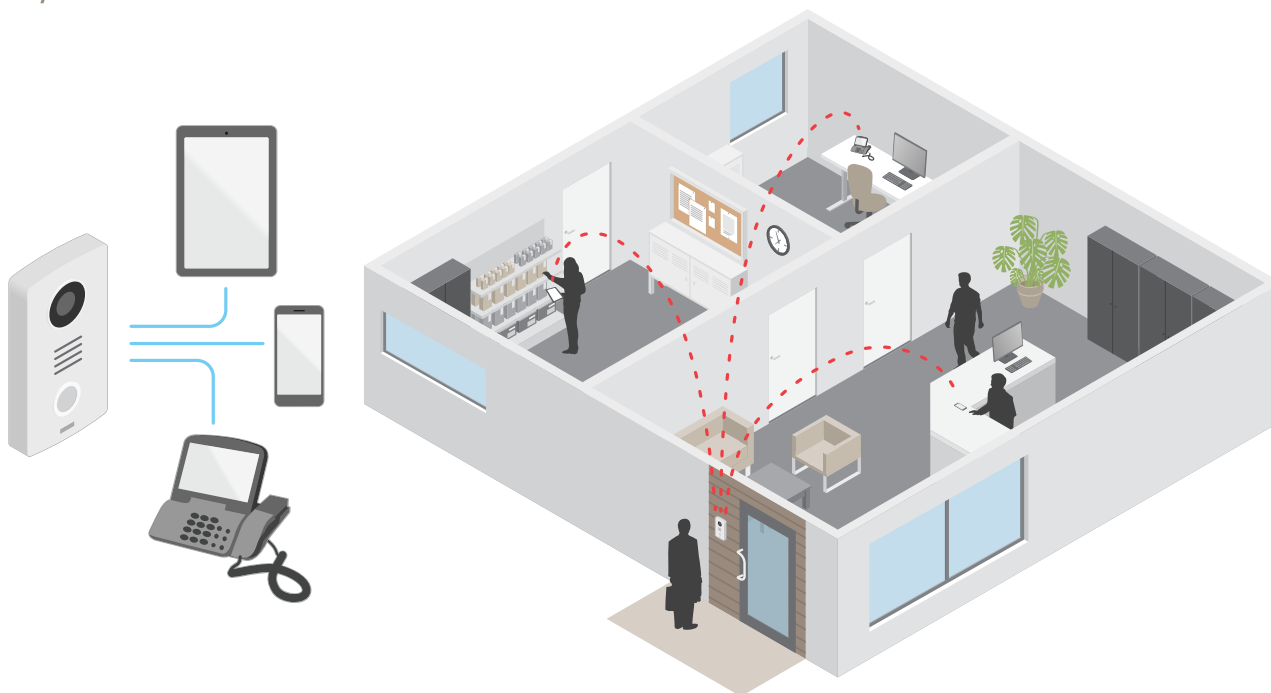
Więcej informacji

Voice over IP (VoIP)

Voice over IP (VoIP) to grupa technologii, która umożliwia komunikację głosową i sesje multimedialne w sieciach IP, na przykład przez internet. Podczas tradycyjnych połączeń telefonicznych sygnały analogowe przesyłane są obwodami przez publiczną komutowaną sieć telefoniczną – Public Switched Telephone Network (PSTN). Podczas połączeń VoIP sygnały analogowe są konwertowane na sygnały cyfrowe, tak aby można je było przesyłać jako pakiety danych przez lokalne sieci IP lub Internet.

W produkcie Axis protokół VoIP jest włączany za pośrednictwem sygnalizacji Session Initiation Protocol (SIP) i Dual-Tone Multi-Frequency (DTMF).

Przykład:



Po naciśnięciu przycisku nawiązywania połączenia na wideodomofonie Axis wykonywane jest połączenie do jednego ze wstępnie zdefiniowanych odbiorców. Po odebraniu połączenia rozpoczyna się rozmowa. Obraz i dźwięk są transmitowane za pomocą technologii VoIP.

Protokół inicjacji sieci (Session Initiation Protocol, SIP)

Protokół inicjacji sieci (SIP) jest stosowany do konfiguracji, utrzymywania i kończenia połączeń VoIP. Połączenia można wykonywać pomiędzy dwoma rozmówcami lub większą ich liczbą (tzw. agentami użytkowników SIP). Aby wykonać połączenie SIP, można skorzystać na przykład z telefonów SIP, softphone'ów lub urządzeń Axis obsługujących SIP.

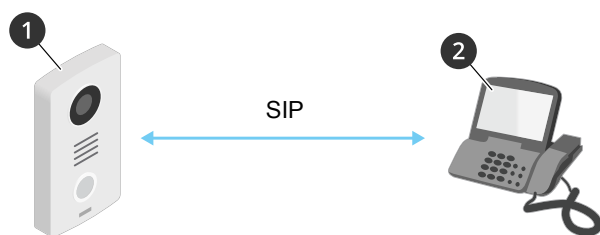
Sygnał audio i wideo jest wymieniany pomiędzy agentami użytkowników SIP z użyciem protokołu transmisji, takiego jak RTP (Real-Time Transport Protocol).

W sieci lokalnej można nawiązywać połączenia w konfiguracji peer-to-peer, a pomiędzy sieciami – za pomocą PBX.

Peer-to-peer SIP (P2PSIP)

Podstawowa komunikacja SIP odbywa się bezpośrednio pomiędzy dwoma lub większą liczbą agentów użytkowników SIP. Połączenie takie nazywane jest peer-to-peer SIP (P2PSIP). Jest ono wykonywane w sieci lokalnej i wymaga jedynie adresów SIP agentów użytkowników. Adres SIP to zazwyczaj `sip:<local-ip>`.

Przykład:



- 1 Agent użytkownika A – wideodomofon. Adres SIP: sip:192.168.1.101
- 2 Agent użytkownika B – telefon z włączonym SIP. Adres SIP: sip:192.168.1.100

Można skonfigurować wideodomofon Axis tak, by łączył się z telefonem SIP w tej samej sieci za pomocą peer-to-peer SIP.

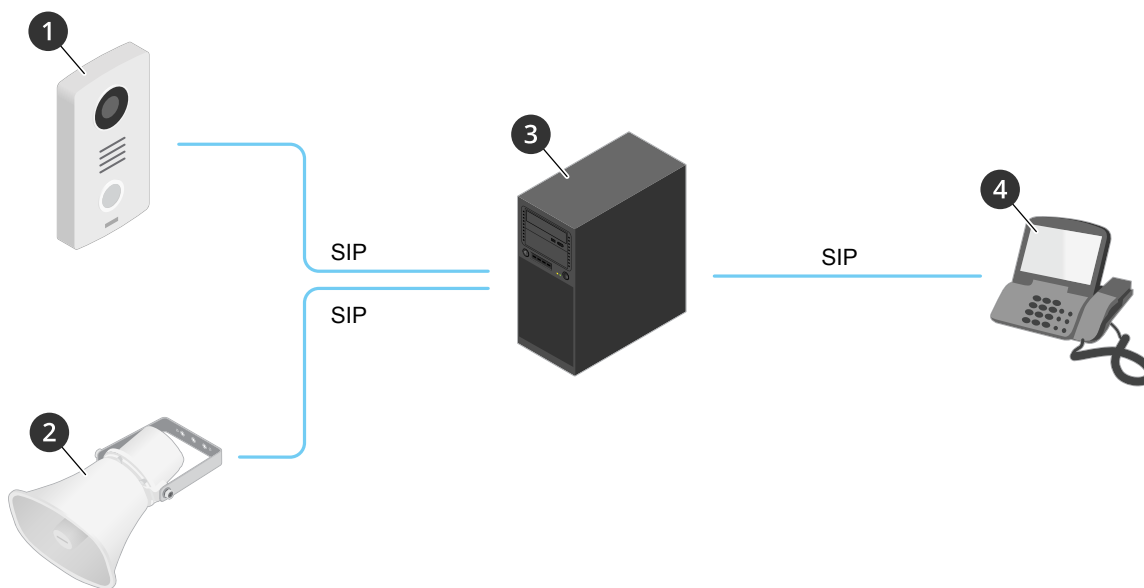
Private Branch Exchange (PBX) – centrala abonencka

Podczas wykonywania połączeń SIP poza lokalną sieć IP PBX może służyć za centralkę. Głównym elementem PBX jest serwer SIP, zwany również serwerem proxy SIP lub rejestratorem. PBX działa jak tradycyjna centralka telefoniczna, wyświetla bieżący status klienta i umożliwia na przykład przekazywanie połączeń, rejestrację wiadomości głosowych i przekierowania.

Serwer SIP PBX można skonfigurować lokalnie lub zdalnie. Można go umieścić w intranecie lub u zewnętrznego dostawcy usług serwerowych. Podczas wykonywania połączeń SIP pomiędzy sieciami połączenia są przekazywane przez zestaw PBX, które wysyłają zapytania o lokalizację docelowego adresu SIP.

Każdy agent użytkownika SIP jest rejestrowany w PBX; mogą łączyć się z innymi poprzez wybranie właściwego numeru wewnętrznego. Adres SIP to zazwyczaj sip:<user>@<domain> lub sip:<user>@<registrar-ip>. Adres SIP jest niezależny od adresu IP, a PBX udostępnia urządzenie przez cały czas, kiedy jest ono zarejestrowane.

Przykład:



- 1 sip:mydoor@company.com
- 2 sip:myspeaker@company.com
- 3 PBX sip.company.com
- 4 sip:office@company.com

Po naciśnięciu przycisku wykonywania połączenia na wideodomofonie Axis połączenie jest przekazywane przez jedną lub więcej centralek PBX do adresu SIP w lokalnej sieci IP lub przez internet.

Konfiguracja reguł dotyczących zdarzeń

Można utworzyć reguły sprawiające, że urządzenie będzie wykonywać konkretne akcje po wystąpieniu określonych zdarzeń. Reguła składa się z warunków i akcji. Warunki mogą służyć do wyzwalania akcji. Urządzenie może na przykład rozpocząć zapis lub wysłać wiadomość e-mail po wykryciu ruchu albo wyświetlić nałożony tekst podczas rejestracji.

Aby dowiedzieć się więcej, zob. *Get started with rules for events (Reguły dotyczące zdarzeń)*.

Analizy i aplikacje

Analizy i aplikacje pozwalają lepiej wykorzystać potencjał urządzeń Axis. AXIS Camera Application Platform (ACAP) to otwarta platforma umożliwiająca podmiotom zewnętrznym opracowywanie funkcji analizy i innych aplikacji dla urządzeń Axis. Aplikacje mogą być fabrycznie zainstalowane na urządzeniu, dostępne do pobrania za darmo lub oferowane za opłatą licencyjną.

Podręczniki użytkownika do analiz i aplikacji Axis można znaleźć na stronie *help.axis.com*.

AXIS Client for Unified Communication Systems

Dzięki tej platformie możesz wykonywać połączenia pomiędzy urządzeniami Axis z protokołem SIP a powiązanymi kontami Microsoft® Teams. Więcej informacji znajduje się w *instrukcji obsługi platformy AXIS Client for Unified Communication Systems*.

Dzienne wykorzystanie

Używanie klawiatury

Pożądaný efekt	Akcja
Połączyć się z osobą, która wpuści mnie do budynku.	Naciśnij  .
Połączyć się z osobą znajdującą się w budynku.	Wprowadź numer szybkiego wybierania danej osoby i naciśnij  .
Otworzyć drzwi, używając mojej karty i numeru PIN.	Wybierz kartę i wprowadź PIN.
Otworzyć drzwi, używając mojego numeru PIN.	Wprowadź PIN i naciśnij #.
Otworzyć drzwi, używając mojej karty.	Wybierz kartę.

Rozwiązywanie problemów –

Przywróć domyślne ustawienia fabryczne

Ważne

Przywracanie domyślnych ustawień fabrycznych należy stosować rozważnie. Opcja resetowania do domyślnych ustawień fabrycznych powoduje przywrócenie wszystkich domyślnych ustawień fabrycznych produktu, włącznie z adresem IP.

Przywracanie domyślnych ustawień fabrycznych produktu:

1. Odłącz zasilanie produktu.
2. Naciśnij i przytrzymaj przycisk kontrolny i włącz zasilanie. Patrz *Przegląd produktów, on page 5*.
3. Przytrzymuj przycisk Control przez 15–30 sekund, aż wskaźnik LED stanu zacznie migać na bursztynowo.
4. Zwolnij przycisk Control. Proces zostanie zakończony, gdy wskaźnik LED stanu zmieni kolor na zielony. Jeśli w sieci nie ma żadnego serwera DHCP, urządzenie będzie mieć domyślnie jeden z następujących adresów IP:
 - Urządzenia z systemem AXIS OS w wersji 12.0 lub nowszej: Uzyskany z podsieci adres łącza lokalnego (169.254.0.0/16)
 - Urządzenia z systemem AXIS OS w wersji 11.11 lub starszej: 192.168.0.90/24
5. Użyj narzędzi do instalacji i zarządzania, aby przypisać adres IP, ustawić hasło i uzyskać dostęp do urządzenia.
Narzędzia do instalacji i zarządzania są dostępne na stronach pomocy technicznej axis.com/support.

Fabryczne wartości parametrów można również przywrócić za pośrednictwem interfejsu WWW urządzenia. Wybierz kolejno opcje Maintenance (Konserwacja) > Factory default (Ustawienia fabryczne) > Default (Domyślne).

Sprawdzanie bieżącej wersji systemu AXIS OS

System AXIS OS określa funkcjonalność naszych urządzeń. W przypadku pojawienia się problemów zalecamy rozpoczęcie ich rozwiązywania od sprawdzenia bieżącej wersji systemu AXIS OS. Najnowsza wersja może zawierać poprawki, które rozwiążą problem.

Aby sprawdzić bieżącą wersję systemu AXIS OS:

1. Przejdź do interfejsu WWW urządzenia i wybierz opcję Status.
2. W menu Device info (Informacje o urządzeniu) sprawdź wersję systemu AXIS OS.

Aktualizacja systemu AXIS OS:

Ważne

- Po aktualizacji oprogramowania urządzenia poczynione ustawienia zostaną zachowane. Axis Communications AB nie gwarantuje, że ustawienia te zostaną zachowane, nawet gdy funkcje są dostępne w nowej wersji systemu operacyjnego AXIS OS.
- Począwszy od systemu operacyjnego AXIS OS w wersji 12.6, pomiędzy aktualną a docelową wersją urządzenia należy zainstalować każdą wersję LTS. Przykładowo, jeżeli aktualnie zainstalowana wersja oprogramowania urządzenia to AXIS OS 11.2, przed aktualizacją urządzenia do wersji AXIS OS 12.6 należy zainstalować wersję LTS AXIS OS 11.11. Więcej informacji znajduje się w dokumencie *Cykł eksploatacji oprogramowania AXIS OS: ścieżka aktualizacji*.
- Upewnij się, że podczas całego procesu aktualizacji urządzenie jest podłączone do źródła zasilania.

Uwaga

- Aktualizacja urządzenia Axis do najnowszej dostępnej wersji systemu AXIS OS umożliwia uaktualnienie produktu o najnowsze funkcje. Przed aktualizacją oprogramowania zawsze należy przeczytać instrukcje dotyczące aktualizacji oraz informacje o wersji dostępne z każdą nową wersją. Przejdź do strony axis.com/support/device-software, aby znaleźć najnowszą wersję systemu AXIS OS oraz informacje o wersji.

1. Pobierz na komputer plik systemu AXIS OS dostępny bezpłatnie na stronie axis.com/support/device-software.
2. Zaloguj się do urządzenia jako administrator.
3. Wybierz kolejno opcje Maintenance > AXIS OS upgrade (Konserwacja > Aktualizacja systemu AXIS OS) > Upgrade (Aktualizuj).

Po zakończeniu aktualizacji produkt automatycznie uruchomi się ponownie.

Problemy techniczne, wskazówki i rozwiązania

Jeśli nie możesz znaleźć tego, czego szukasz, przejdź na stronę poświęconą rozwiązywaniu problemów: axis.com/support.

Problemy z aktualizacją oprogramowania sprzętowego	
Niepowodzenie podczas aktualizacji oprogramowania sprzętowego	Jeśli aktualizacja oprogramowania sprzętowego zakończy się niepowodzeniem, urządzenie załaduje ponownie poprzednią wersję oprogramowania sprzętowego. Najczęstszą przyczyną tego jest wczytanie niewłaściwego oprogramowania sprzętowego. Upewnij się, że nazwa pliku oprogramowania sprzętowego odpowiada danemu urządzeniu i spróbuj ponownie.

Problemy z ustawieniem adresu IP

Urządzenie należy do innej podsieci	Jeśli adres IP przeznaczony dla danego urządzenia oraz adres IP komputera używanego do uzyskania dostępu do urządzenia należą do różnych podsieci, ustawienie adresu IP jest niemożliwe. Skontaktuj się z administratorem sieci, aby uzyskać adres IP.
Adres IP jest używany przez inne urządzenie	Odłącz urządzenie Axis od sieci. Uruchom polecenie Ping (w oknie polecenia/DOS wpisz <code>ping</code> oraz adres IP urządzenia): • Jeśli otrzymasz: <code>Reply from <IP address>: bytes=32; time=10...</code>, oznacza to, że ten adres IP może już być używany przez inne urządzenie w sieci. Poproś administratora sieci o nowy adres IP i zainstaluj ponownie urządzenie. • Jeśli otrzymasz: <code>Request timed out</code>, oznacza to, że ten adres IP jest dostępny do wykorzystania przez urządzenie Axis. Sprawdź całe okablowanie i zainstaluj urządzenie ponownie.
Możliwy konflikt adresów IP z innym urządzeniem w tej samej podsieci	Zanim serwer DHCP ustawi adres dynamiczny, używany jest statyczny adres IP urządzenia Axis. Oznacza to, że jeśli ten sam domyślny statyczny adres IP jest używany także przez inne urządzenie, mogą wystąpić problemy podczas uzyskiwania dostępu do urządzenia.

Nie można uzyskać dostępu do urządzenia przez przeglądarkę

Nie można się zalogować	Jeśli protokół HTTPS jest włączony, trzeba upewnić się, że podczas logowania używany jest właściwy protokół (HTTP lub HTTPS). Może zajść konieczność ręcznego wpisania <code>http</code> lub <code>https</code> w polu adresu przeglądarki. W razie utraty hasła dla użytkownika root należy przywrócić ustawienia fabryczne urządzenia. Patrz <i>Przywróć domyślne ustawienia fabryczne, on page 21</i> .
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 urządzenie w sieci. Znajdź urządzenie przy użyciu nazwy modelu lub numeru seryjnego bądź nazwy DNS (jeśli skonfigurowano tę nazwę).

Dostęp do urządzenia można uzyskać lokalnie, ale nie z zewnątrz

Aby uzyskać dostęp do urządzenia z zewnątrz, zalecamy skorzystanie z jednej z następujących aplikacji dla systemu Windows®:

- AXIS Companion: darmowa aplikacja idealna do małych systemów o niewielkich wymaganiach w zakresie dozoru.
- AXIS Camera Station: 30-dniowa darmowa wersja próbna, idealna do małych i średnich systemów.

Instrukcje i plik do pobrania znajdują się na stronie axis.com/vms.

Kwestie wydajności

Podczas konfigurowania systemu należy wziąć pod uwagę wpływ różnych ustawień i sytuacji na wydajność. Niektóre czynniki wpływają na przepustowość (przepływność), inne na poklatkowość, a jeszcze inne na oba te parametry.

Najważniejsze czynniki, które należy uwzględnić:

- Wysoka rozdzielczość obrazu lub niższe poziomy kompresji zapewniają obrazy zawierające więcej danych, co z kolei wpływa na przepustowość.
- Dostęp ze strony dużej liczby klientów MJPEG lub H.264/H.265/AV1 unicast wpływa na przepustowość.
- Jednoczesne oglądanie różnych strumieni (rozdzielczość, kompresja) za pomocą różnych klientów wpływa zarówno na liczbę klatek na sekundę, jak i na przepustowość. W miarę możliwości używaj identycznych strumieni, aby utrzymać wysoką liczbę klatek na sekundę. Aby upewnić się, że strumienie są identyczne, możesz użyć profili strumieni.
- Jednoczesny dostęp do strumieni wideo z różnymi kodekami wpływa zarówno na poklatkowość, jak i na przepustowość. Aby uzyskać optymalną wydajność, należy używać strumieni z tym samym kodekiem.
- Intensywne korzystanie z ustawień zdarzeń wpływa na obciążenie procesora, co z kolei wpływa na liczbę klatek na sekundę.
- Korzystanie z protokołu HTTPS może zmniejszać liczbę klatek na sekundę, szczególnie w przypadku przesyłania strumieniowego obrazów wideo w formacie MJPEG.
- Znaczące obciążenie sieci ze względu na słabą infrastrukturę wpływa na przepustowość.
- Wyświetlanie obrazu z użyciem komputerów klienckich o niewystarczających parametrach obniża subiektywnie obserwowaną wydajność i wpływa na liczbę klatek na sekundę.
- Jednoczesne uruchamianie wielu aplikacji AXIS Camera Application Platform (ACAP) może mieć wpływ na liczbę klatek na sekundę i ogólną wydajność.

Specyfikacje

Wskaźniki i elementy sterowania na panelu przednim

Po podłączeniu produktu do zasilania wskaźniki na panelu przednim zaświecą się na kilka sekund.

Ikony wskaźników

Ikona	Wskazanie
	Stałe niebieskie światło po zainicjowaniu połączenia wychodzącego. Miga na niebiesko po zainicjowaniu połączenia przychodzącego.
	Stałe bursztynowe światło podczas trwającego połączenia.
	Stałe zielone światło po otwarciu drzwi.

Pasek wskaźnika czytnika kart

Pasek wskazuje informacje zwrotne z czytnika.

Przycisk połączenia

Aby podświetlić twarze gości, można użyć wbudowanego oświetlenia dookoła przycisku.

Wskaźniki LED

Dioda stanu	Wskazanie
Zielony	Stałe zielone światło przy normalnym działaniu.

Gniazdo karty SD

POWIADOMIENIE

- Ryzyko uszkodzenia karty SD. Nie używaj ostrych narzędzi, metalowych przedmiotów ani nadmiernej siły podczas wkładania i wyjmowania karty SD. Wkładaj i wyjmuj kartę palcami.
- Ryzyko utraty danych i uszkodzenia nagrań. Odłącz kartę SD od interfejsu WWW urządzenia, zanim ją wyjmiesz. Nie wyjmuj karty SD w trakcie działania produktu.

Urządzenie obsługuje karty microSD/microSDHC/microSDXC.

Zalecenia dotyczące kart SD można znaleźć w witrynie axis.com.



Logo microSD, microSDHC i microSDXC są znakami towarowymi firmy SD-3C LLC. microSD, microSDHC, microSDXC są znakami towarowymi lub znakami towarowymi firmy SD-3C, LLC w Stanach Zjednoczonych, innych krajach lub w Stanach Zjednoczonych i innych krajach.

Przyciski

Przycisk kontrolny

Przycisk ten służy do:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz *Przywróć domyślne ustawienia fabryczne, on page 21*.

Złącza

Złącze HDMI

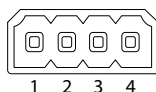
Użyj złącza microHDMI™, aby podłączyć wyświetlacz lub monitor dostępne publicznie.

Złącze sieciowe

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

Złącze audio

4-pinowy blok złączy wejść i wyjść audio.

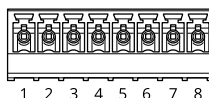


Funkcje	Styk	Uwagi
Wejście liniowe	1	Wejście liniowe (mono)
GND	2	Uziemienie audio
Wyjście liniowe	3	Wyjście liniowe
GND	4	Uziemienie audio

Złącze przekaźnikowe

8-stykowy blok złączy przekaźników półprzewodnikowych, które można wykorzystać w następujący sposób:

- Jako standardowe przekaźniki otwierające i zamykające obwody pomocnicze.
- Do bezpośredniego sterowania zamkiem.
- Do sterowania zamkiem przez przekaźnik bezpieczeństwa. Korzystanie z przekaźnika bezpieczeństwa po bezpiecznej stronie drzwi zapobiega podłączeniu zewnętrznych przewodów.



Funkcje	Styk	Uwagi	Specyfikacje
NO/NZ	1	Normalnie otwarte/normalnie zamknięte Do podłączania urządzeń przekaźnikowych. Obwód przekaźnika jest odizolowany galwanicznie od pozostałych obwodów.	Maks. prąd 1 A Maks. napięcie 30 V DC
COM	2	Wspólny	
24 V DC	3	Do zasilania urządzeń dodatkowych. Uwaga: ten styk może być używany tylko jako wyjście zasilania.	Napięcie wyjściowe 24 V DC Maks. prąd 50 mA ¹ Maks. prąd 350 mA ²

1. W przypadku zasilania typu Power over Ethernet IEEE 802.3af/802.3at typ 1 klasa 3.

2. W przypadku zasilania typu Power over Ethernet Plus (PoE+) IEEE 802.3at typ 2 klasa 4 lub za pośrednictwem wejścia zasilania DC.

Masa DC	4		0 V DC
NO/NZ	5	Normalnie otwarte/normalnie zamknięte Do podłączania urządzeń przekaźnikowych. Obwód przekaźnika jest odizolowany galwanicznie od pozostałych obwodów.	Maks. prąd 1 A Maks. napięcie 30 V DC
COM	6	Wspólny	
12 V DC	7	Do zasilania urządzeń dodatkowych. Uwaga: ten styk może być używany tylko jako wyjście zasilania.	Napięcie wyjściowe 12 V DC Maks. prąd 100 mA ³ Maks. prąd 700 mA ⁴
Masa DC	8		0 V DC

Złącze czytnika

4-pinowy blok złączy umożliwiający podłączenie czytnika zewnętrznego.

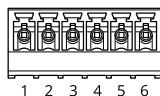
Funkcje	Styk	Uwagi	Specyfikacje
Masa DC	1		0 V DC
12 V DC	2	Do zasilania urządzeń dodatkowych. Uwaga: ten styk może być używany tylko jako wyjście zasilania.	Napięcie wyjściowe 12 V DC
D0/A+	3	Wiegand: wyjście DATA0 RS485: A+	
D1/B-	4	Wiegand: wyjście DATA1 RS485: B-	

Złącze I/O

Złącze I/O 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 12 V) złącze WE/WY 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 zbiecia szyby.

Wyjście cyfrowe – Do podłączenia urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączonymi urządzeniami można zarządzać poprzez API VAPIX®, zdarzenie lub interfejs WWW urządzenia.

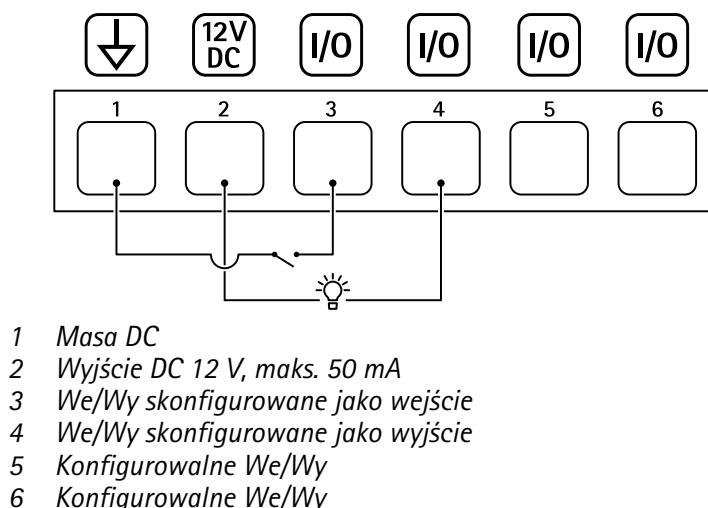


3. W przypadku zasilania typu Power over Ethernet IEEE 802.3af/802.3at typ 1 klasa 3.

4. W przypadku zasilania typu Power over Ethernet Plus (PoE+) IEEE 802.3at typ 2 klasa 4 lub za pośrednictwem wejścia zasilania DC.

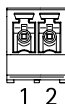
Funkcje	Styk	Uwagi	Specyfikacje
Masa DC	1		0 V DC
Wyjście DC	2	 Może być wykorzystywane do zasilania dodatkowego sprzętu. Uwaga: ten styk może być używany tylko jako wyjście zasilania.	12 V DC Maks. obciążenie = 50 mA
Konfigurowalne (wejście lub wyjście)	3–6	Wejście cyfrowe – podłącz do styku 1, aby 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.	Od 0 do maks. 30 V DC, otwarty dren, 100 mA

Przykład:



Złącze zasilania

2-pinowy blok złączy na wejście zasilania DC. Używaj urządzenia LPS zgodnego z SELV z nominalną mocą wyjściową ograniczoną do ≤ 100 W lub nominalnym prądem ograniczonym do ≤ 5 A.



Funkcje	Styk	Uwagi	Specyfikacje
Masa 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.	8–28 V DC, maks. 22 W Maks. obciążenie wyjść 9 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.

Cyberbezpieczeństwo

Bezpieczeństwo cybernetyczne jest składnikiem udanego cyklu eksploatacji produktu dzięki minimalizacji narażeń. Szczegółowe informacje i dokumentacja na temat naszego podejścia do cyberbezpieczeństwa znajdują się na stronie: axis.com/about-axis/cybersecurity. Przestrzegaj poniższych wytycznych dotyczących cyberbezpieczeństwa, aby otrzymywać powiadomienia od Axis dotyczące bezpieczeństwa produktów oraz skonfigurować produkt w sposób zapewniający bezpieczny cykl eksploatacji oraz wycofanie z użytku.

Na stronie *Axis Trust Center* znajdują się informacje o sposobach, w jakie Axis zapewnia zgodność z wymogami bezpieczeństwa, transparentność, ochronę danych oraz ochronę prywatności.

Postępowanie z lukami w zabezpieczeniach

Axis ma status *Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA)*. Aby zminimalizować ryzyko narażenia na zagrożenia, postępujemy zgodnie z branżowymi normami w zakresie wykrywania i usuwania luk w zabezpieczeniach naszych urządzeń, oprogramowania i usług. Informacje na temat naszej polityki zarządzania lukami w zabezpieczeniach oraz instrukcje dotyczące zgłaszania luk znajdują się na stronie axis.com/vulnerability-management.

Powiadomienia dotyczące zabezpieczeń

Subskrybuj powiadomienia o zagrożeniach bezpieczeństwa w produktach Axis na stronie axis.com/security-notification-service. Będziemy informować Cię o lukach w zabezpieczeniach, udzielać odnośnych wskazówek oraz powiadamiać o innych kwestiach związanych z bezpieczeństwem użytkowanego produktu Axis.

Bezpieczny cykl eksploatacji produktu

Axis minimalizuje ryzyko w całym cyklu eksploatacji swoich produktów dzięki bezpiecznemu zarządzaniu cyklem eksploatacji. Skorzystaj z naszych przewodników dotyczących zwiększenia bezpieczeństwa dostępnych na stronie help.axis.com, aby bezpieczniej konfigurować i obsługiwać produkty Axis oraz uzyskać informacje na poniższe tematy:

Bezpieczne pierwsze użycie – Produkty Axis są skonfigurowane fabrycznie z wysokim poziomem domyślnej ochrony, co oznacza bezpieczną pierwszą konfigurację oraz szyfrowaną komunikację od samego początku użytkowania.

Przeznaczenie i typowe błędy w konfiguracji – Nasze przewodniki zawierają informacje o przeznaczeniu produktów Axis, w tym o typowych błędach użytkowania związanych z bezpieczeństwem oraz błędach przy konfiguracji, których należy unikać.

Zarządzanie lukami w zabezpieczeniach i transparentność łańcucha dostaw – Wraz z każdą wersją oprogramowania na stronie axis.com publikowany jest wykaz komponentów oprogramowania (SBOM – Software Bill of Material) w celu poinformowania o lukach w zabezpieczeniach (podatnościach na zagrożenie) oraz zwiększenia transparentności łańcucha dostaw.

Wycofanie z eksploatacji i bezpieczne usuwanie danych – Aby bezpiecznie wycofać produkt po zakończeniu cyklu eksploatacji, przywróć jego ustawienia fabryczne. Spowoduje to usunięcie konfiguracji, zapisanych danych oraz informacji poufnych.

T10176599_pl

2026-07 (M25.2)

© 2021 – 2026 Axis Communications AB