

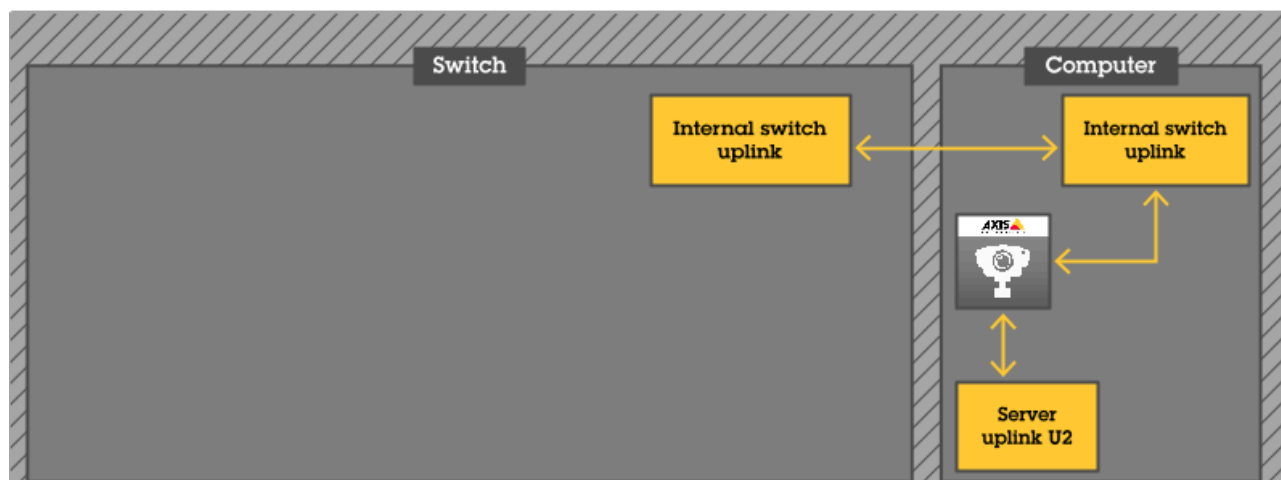
AXIS Camera Station S2108 Appliance

O urządzeniu

AXIS Camera Station S2108 Appliance jest wszechstronnym rozwiązaniem do zapisu, obejmującym wybudowany przełącznik sieciowy PoE, i przeznaczonym do dozoru w wysokiej rozdzielczości z obsługą kamer o maks. rozdzielczości 4K. Aby umożliwić szybką i łatwą instalację, urządzenie jest fabrycznie skonfigurowane i wyposażone w program AXIS Camera Station do zarządzania obrazem, w tym w licencje i całe niezbędne oprogramowanie systemowe. AXIS Camera Station udostępnia intuicyjny interfejs użytkownika, który pozwala w pełni wykorzystywać możliwości szerokiej gamy kamer i innych urządzeń sieciowych Axis. Dzięki systemowi operacyjnemu zainstalowanemu na dysku SSD i 5-letniej gwarancji sprzętowej urządzenie stanowi niezawodne rozwiązanie dozoru.

Urządzenie AXIS Camera Station S2108 Appliance obejmuje dwa komponenty:

- **Przełącznik:** Wbudowany przełącznik typu Power over Ethernet (PoE).
- **Komputer:** Fabrycznie wyposażony w całe oprogramowanie niezbędne do stworzenia rozwiązania dozoru, w tym oprogramowanie do zarządzania materiałem wizyjnym AXIS Camera Station.

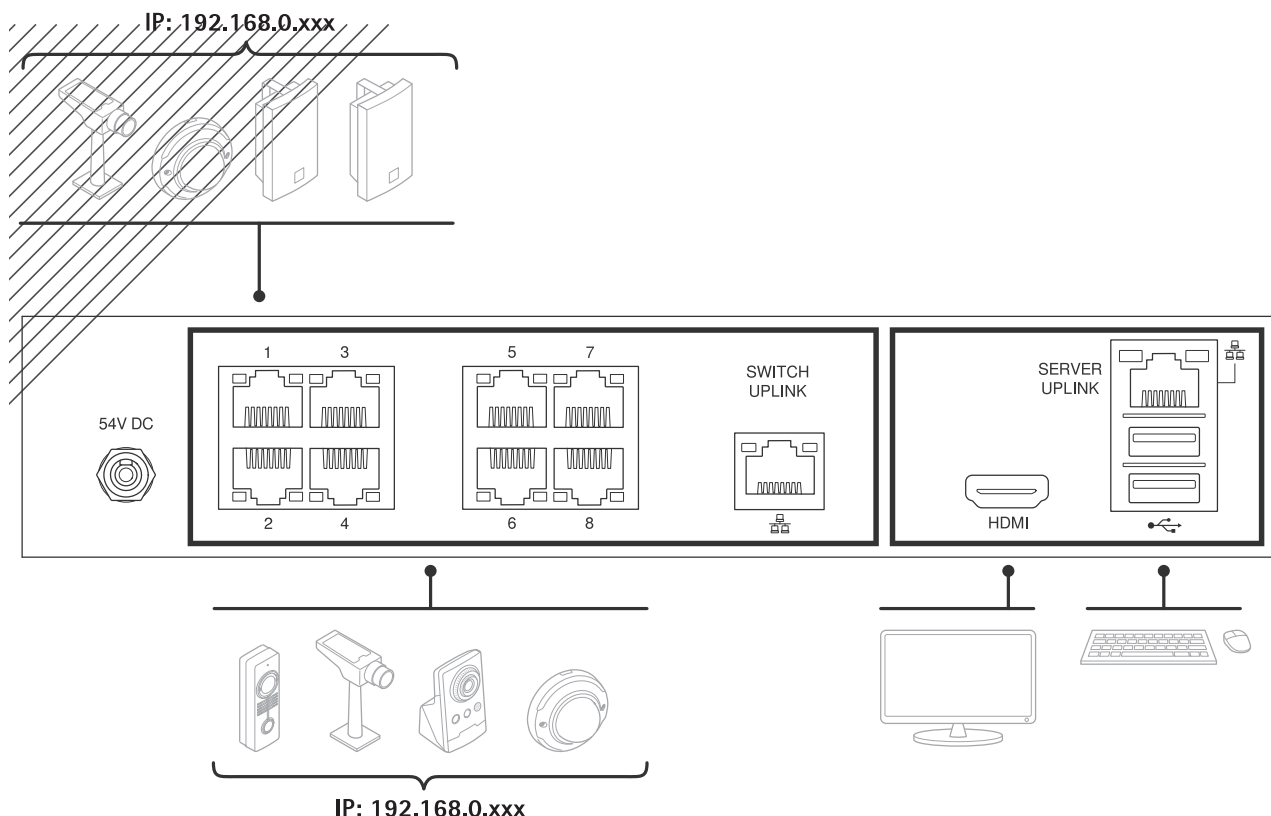


- Przełącznik i komputer to dwa oddzielne elementy.
- Przełącznik i komputer komunikują się za pośrednictwem wewnętrznych złączy typu uplink: jedno z nich znajduje się na płycie obwodu zasilania przełącznika, a drugie na płycie głównej komputera.
- Złącze uplink serwera to zewnętrzny interfejs sieciowy, który może się łączyć z istniejącą siecią IP.
- Urządzenia dołączone do złącza uplink serwera nie mogą się komunikować bezpośrednio z urządzeniami dołączonymi do przełącznika sieciowego.
- Urządzenia dołączone do złącza uplink serwera mogą się komunikować z urządzeniami dołączonymi do przełącznika sieciowego za pośrednictwem programu AXIS Camera Station.

Przykłady konfiguracji

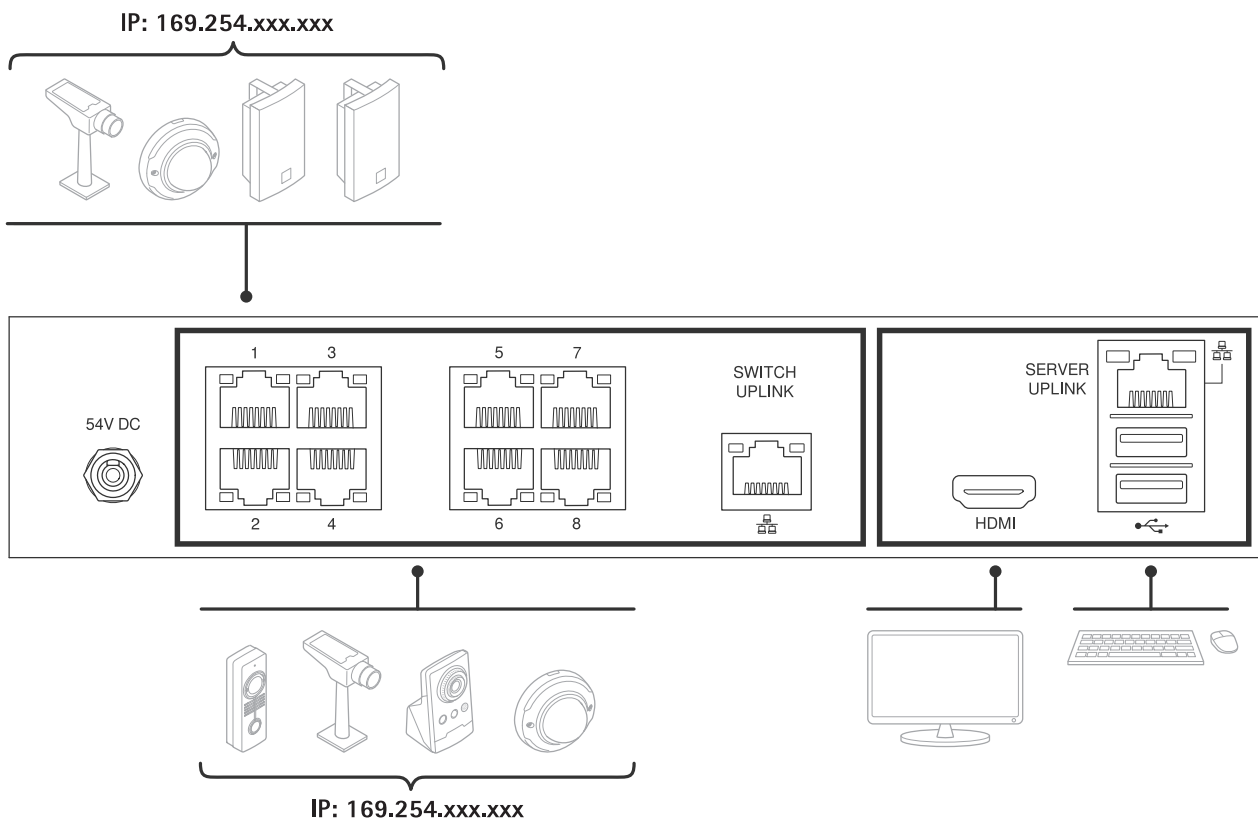
Przydzielanie adresu statycznego do każdego urządzenia

Możesz utworzyć niezależną sieć, przydzielając statyczny adres IP do każdego urządzenia oraz rejestratora AXIS S2108 Appliance. Ta sieć IP nie będzie mieć połączenia z żadną inną siecią zewnętrzną, o ile parametry tychże sieci nie będą ze sobą zgodne. Komputer może nadal łączyć się z internetem poprzez port uplink serwera. Gdy tylko urządzenia zostaną dołączone do portów z zasilaniem PoE, otrzymają adres lokalny łączy i konieczne będzie przypisanie im stałego adresu IP zgodnego z rejestratorem AXIS S2108 Appliance.



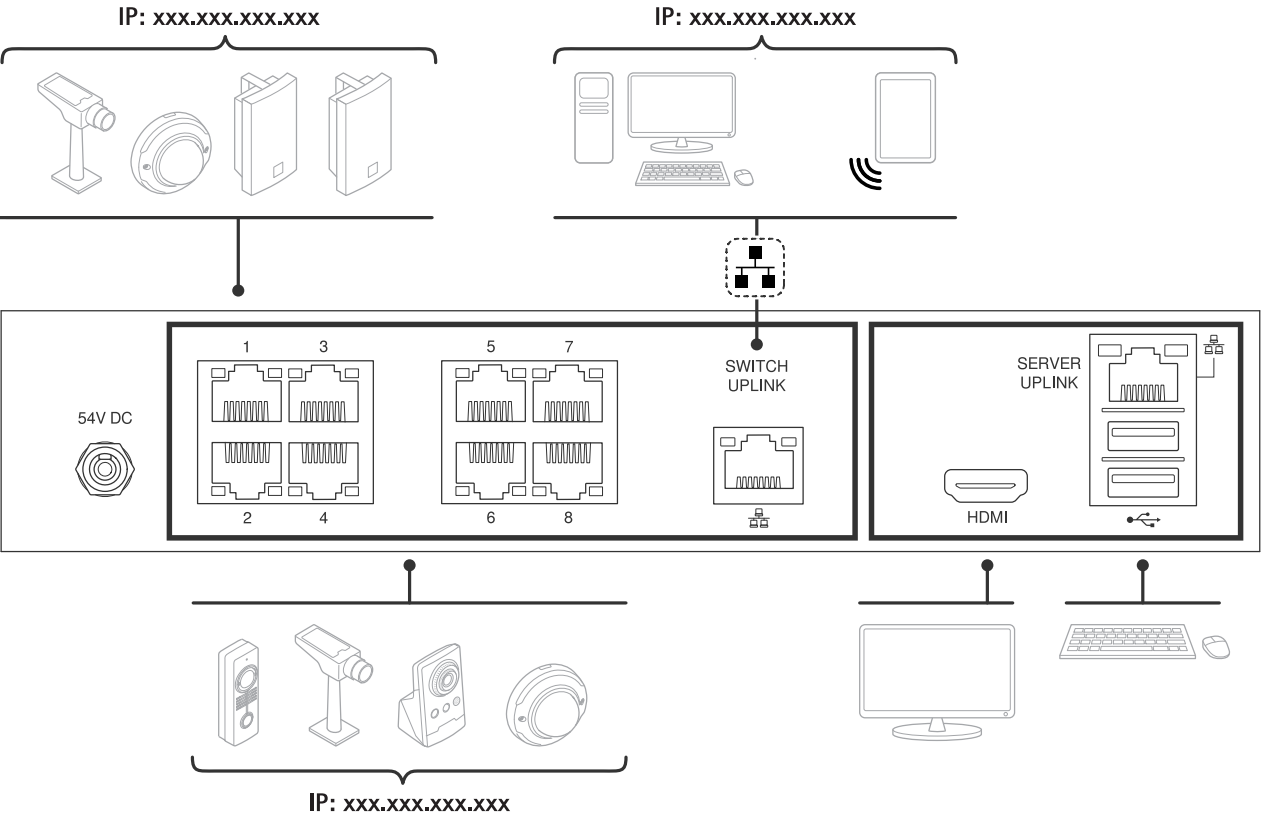
Wykorzystanie adresu lokalnego

Możesz utworzyć niezależną sieć, ustawiając adres lokalny w każdym urządzeniu oraz rejestratorze AXIS S2108 Appliance. Nie będzie ona mieć połączenia z żadną inną siecią zewnętrzną. Komputer może nadal łączyć się z internetem poprzez port uplink serwera. Gdy tylko urządzenia zostaną dołączone do portów z zasilaniem PoE, otrzymają adres lokalny łączy i będzie można je odnaleźć w programie AXIS Camera Station zainstalowanym w rejestratorze AXIS S2108 Appliance.



Wykorzystanie serwera DHCP z innej sieci

Możesz połączyć rejestrator AXIS S2108 Appliance i dołączone do niego urządzenia, korzystając z istniejącej sieci IP oraz serwera DHCP włączonego do łącza uplink przełącznika sieciowego. W ten sposób wszystkie dołączone urządzenia otrzymają adresy IP z puli adresowej serwera DHCP. Jeżeli w sieci tej dostępne jest połączenie z internetem, będzie ono dostępne również dla rejestratora AXIS S2108 Appliance. Jeżeli nie, komputer może nadal łączyć się niezależnie z internetem poprzez port uplink serwera. Po dołączeniu urządzeń do portów z zasilaniem PoE otrzymają one adres DHCP, o ile aktywny jest serwer DHCP.



Od czego zacząć

Standardowo konfiguracja serwera zapisów AXIS Camera Station wygląda następująco:

1. *Instalacja urządzenia*
2. Konfiguracja początkowa systemu Windows®: Po zainstalowaniu urządzenia kreator konfiguracji pomaga wybrać region, język, układ klawiatury, konto administratora i jego hasło.
3. Wstępna konfiguracja rejestratora Axis: Po wstępnej konfiguracji systemu Windows zostanie włączona aplikacja AXIS Recorder Toolbox, która przeprowadza użytkownika przez kilka kroków w celu skonfigurowania podstawowych i niezbędnych ustawień, na przykład nazwy komputera, daty i godziny oraz sieci. Patrz *Wstępna konfiguracja rejestratora Axis, on page 15*.
4. Skonfiguruj system Windows®. Zalecamy następujące czynności:
 - Zaktualizuj system Windows do najnowszej wersji. Patrz .
 - Utwórz standardowe konto użytkownika. Patrz *Tworzenie konta użytkownika, on page 21*.
5. Zaktualizuj AXIS Camera Station do najnowszej wersji.
 - Jeśli system jest w trybie online: otwórz aplikację AXIS Recorder Toolbox i kliknij **Update AXIS Camera Station (Aktualizuj oprogramowanie AXIS Camera Station)**.
 - Jeśli system jest w trybie offline: przejdź na stronę *axis.com* i pobierz najnowszą wersję.
6. Uruchom klienta AXIS Camera Station.
7. *Łączenie z serwerem AXIS Camera Station*
8. *Konfiguracja aplikacji AXIS Camera Station, on page 17*

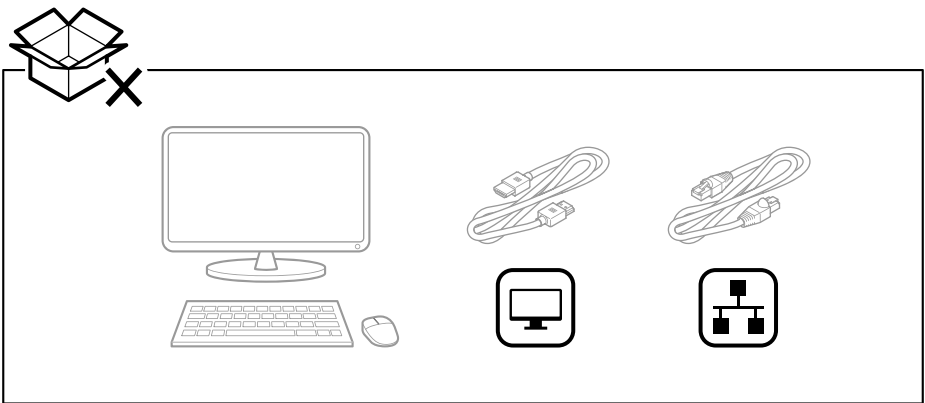
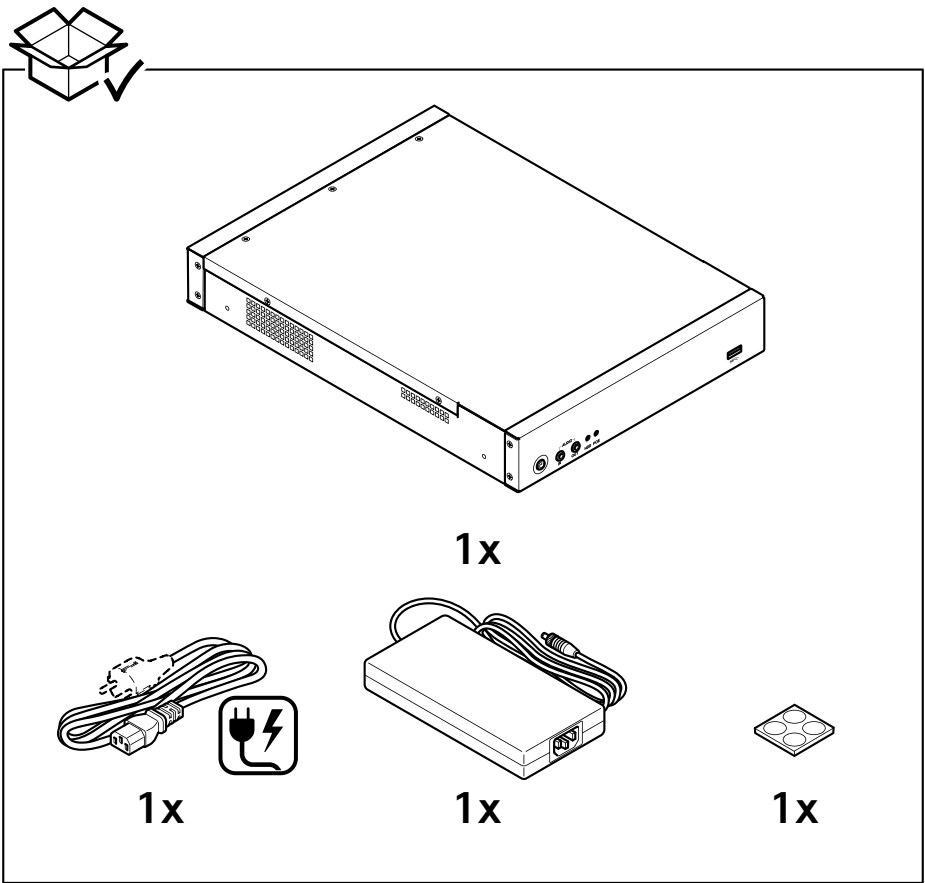
Instalacja urządzenia

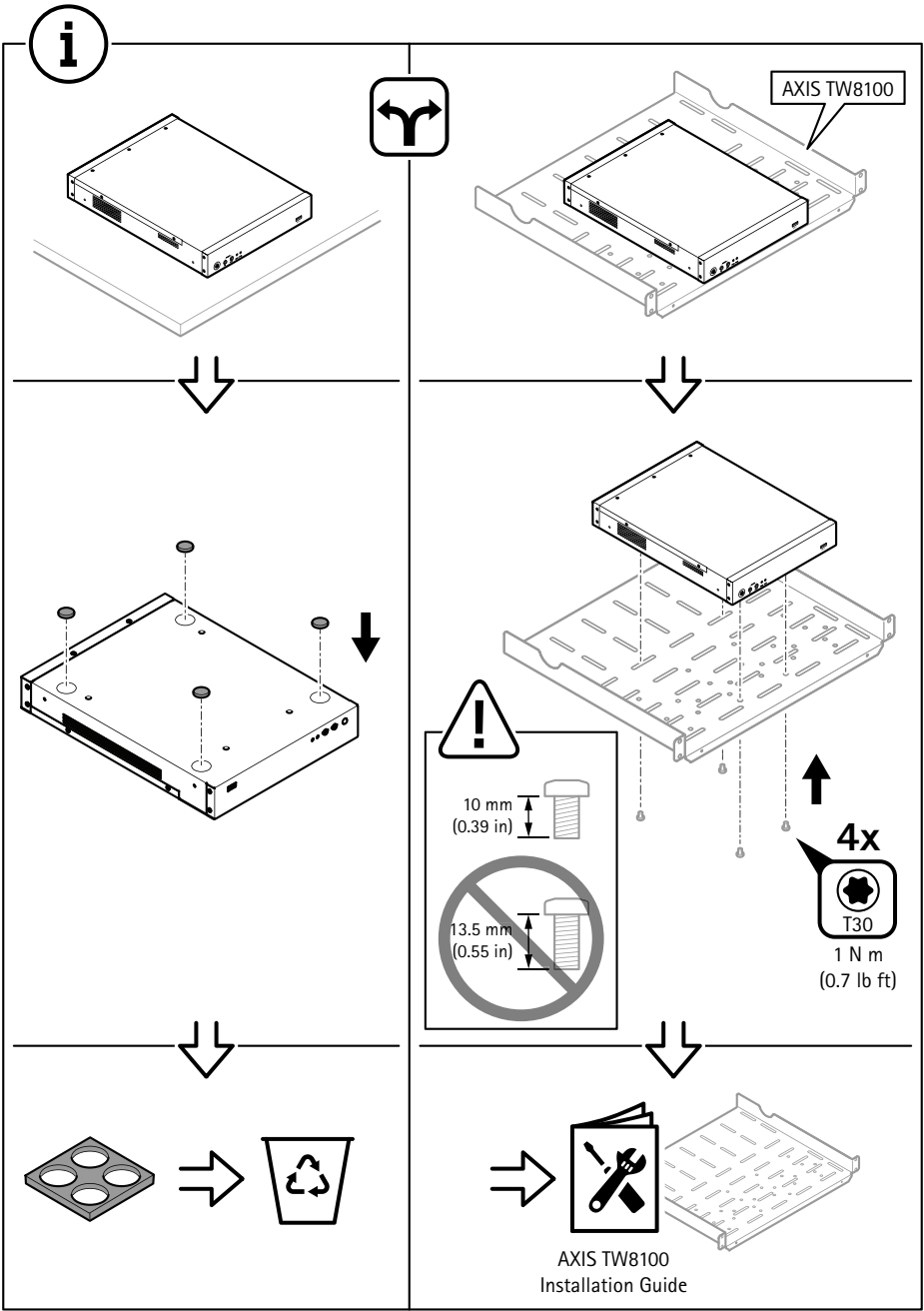
Przed rozpoczęciem instalacji

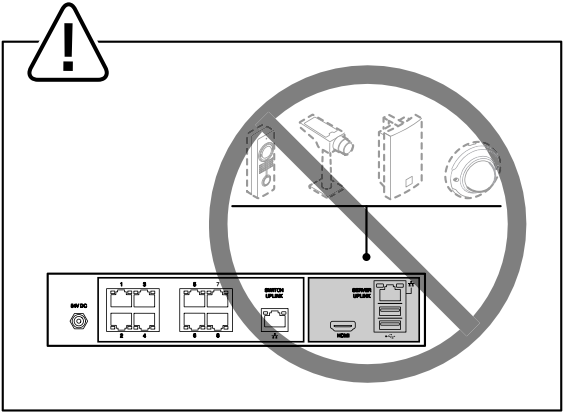
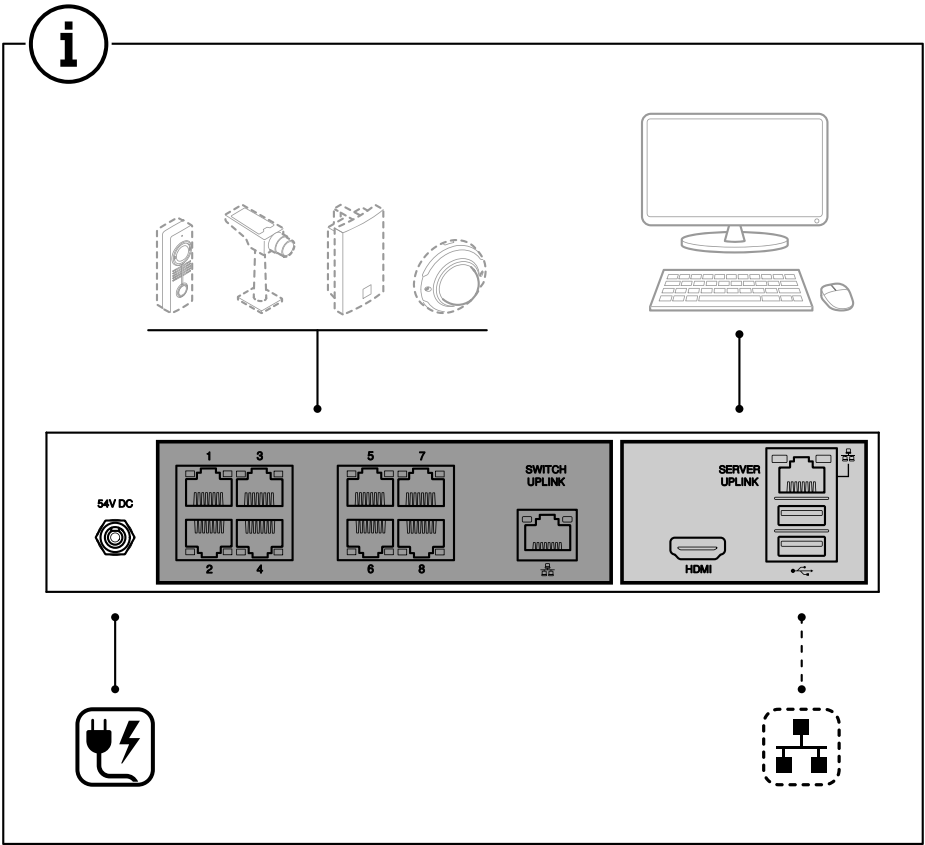
- Przygotuj wyposażenie dodatkowe konieczne przy instalacji: monitor, mysz, klawiaturę i kabel sieciowy.
- Zapoznaj się z zasadami używania różnych kont użytkowników.

W poniższej tabeli wymieniono konta użytkowników, które mogą być używane podczas instalacji, konfiguracji i obsługi systemu Axis.

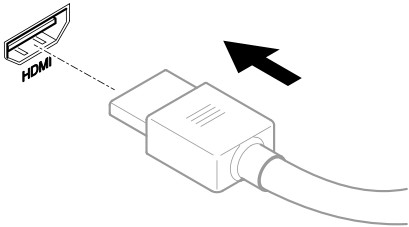
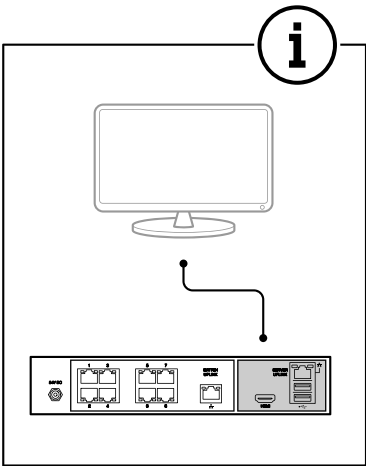
Konto użytkownika	Opis	Uwaga
MyAxis	Służy do pobierania najnowszego oprogramowania, uzyskiwania dostępu do systemu licencji, Axis Secure Remote Access i Monitorowania stanu systemu.	Rejestrowanie na <i>my.axis.com</i> .
Windows®		
Administrator systemu Windows®	Uprawnienia administratora w systemie Windows®. Zaleca się, aby użytkownik nie wykorzystywał tych uprawnień, gdy jest administratorem programu AXIS Camera Station.	Utworzone podczas pierwszej konfiguracji systemu Windows®.
Użytkownik systemu Windows® z uprawnieniami administratora AXIS Camera Station	Użytkownik systemu Windows® z uprawnieniami administratora w AXIS Camera Station do wykorzystania przez integratora systemu lub administratora systemu na potrzeby konfiguracji lub rozwiązywania problemów.	Utworzone w ustawieniach systemu Windows®.
Użytkownik systemu Windows® z uprawnieniami operatora lub dozorca w AXIS Camera Station	Użytkownik systemu Windows® z uprawnieniami operatora lub dozorca w programie AXIS Camera Station.	Utworzone w ustawieniach systemu Windows®.
Urządzenie		
Administrator urządzenia	Używany przez administratora do uzyskania dostępu do kamery z systemu zarządzania sygnałem wizyjnym lub strony internetowej urządzenia.	Utworzone ze strony internetowej urządzenia lub po dodaniu urządzenia do AXIS Camera Station.



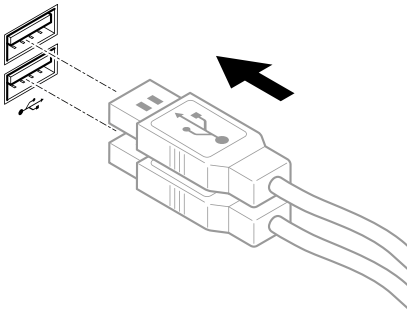
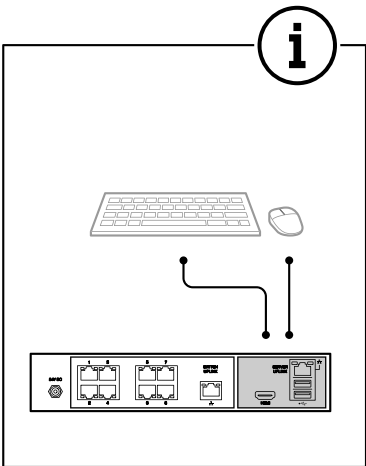




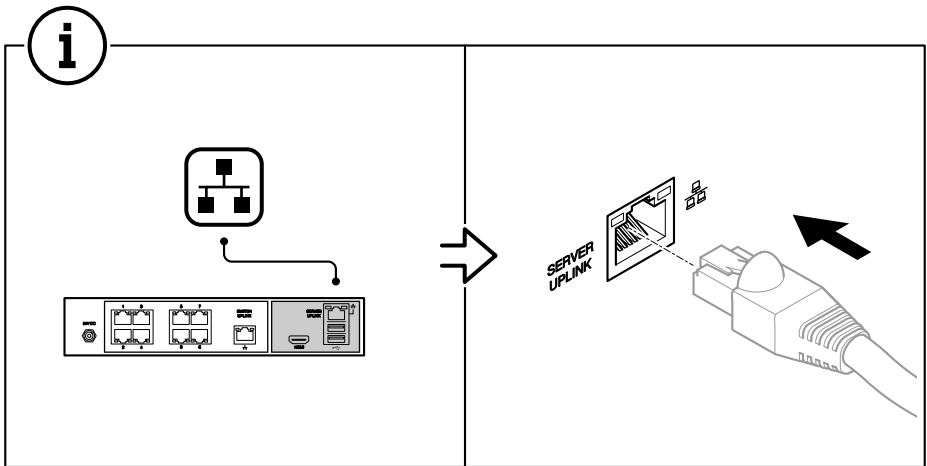
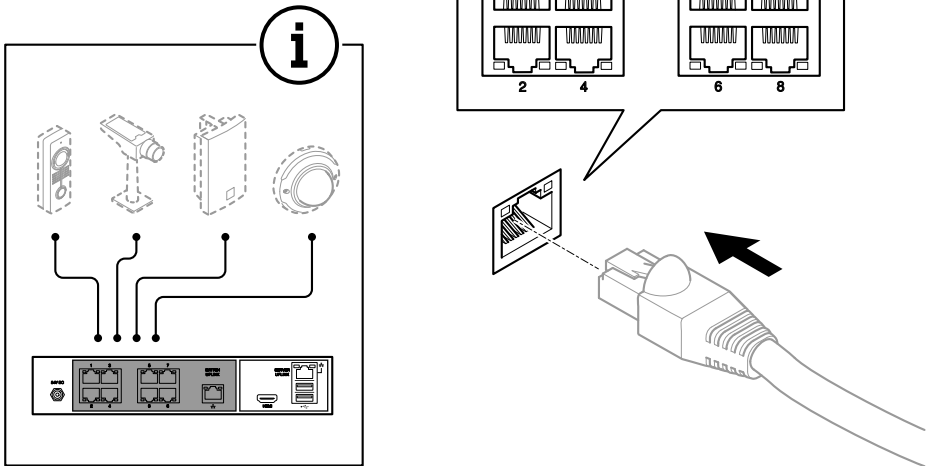
1.1



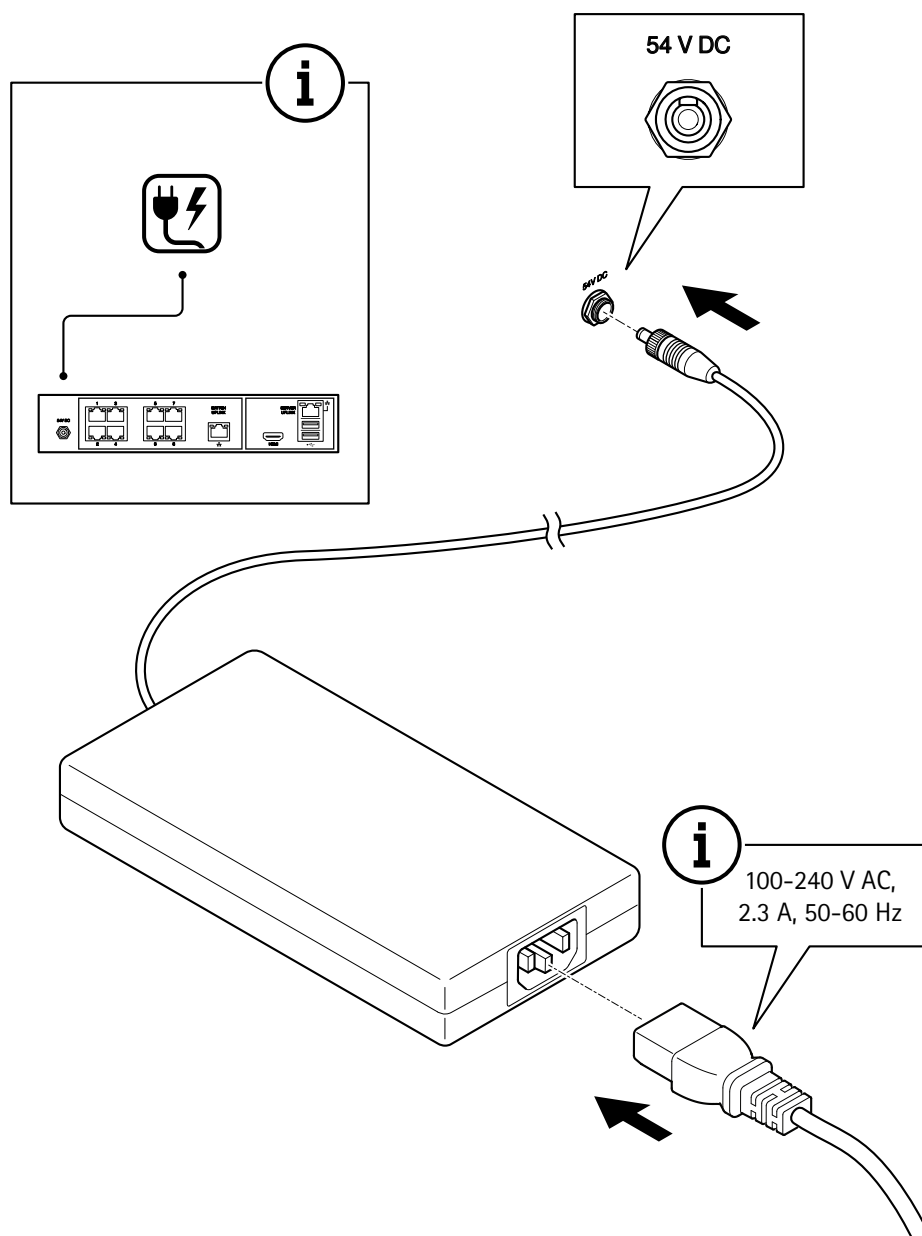
1.2



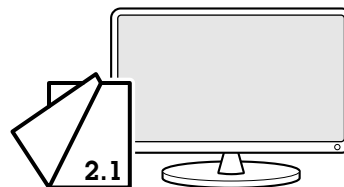
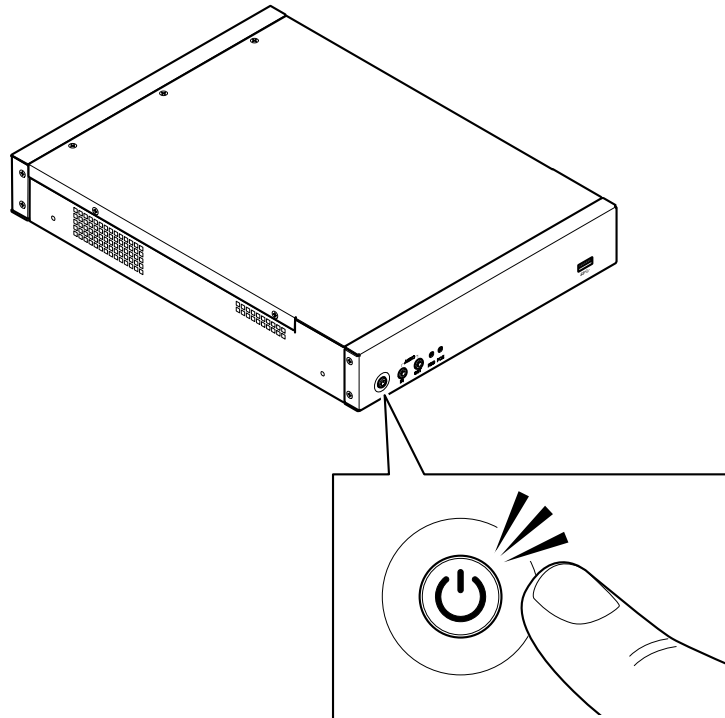
1.3



1.4



1.5



Konfiguracja urządzenia

Wstępna konfiguracja rejestratora Axis

Po skonfigurowaniu systemu Windows® nastąpi automatyczne otwarcie aplikacji AXIS Recorder Toolbox, a asystent instalacji przeprowadzi Cię przez pierwszą konfigurację. W asystencie instalacji można skonfigurować kilka podstawowych i koniecznych ustawień przed przejściem do zarządzania urządzeniem w aplikacji AXIS Recorder Toolbox.

1. Wybierz motyw **Light (Jasny)** lub **Dark (Ciemny)** i kliknij **Next (Dalej)** (jeśli ta pozycja jest dostępna dla Twojego produktu).
2. W razie potrzeby zmień nazwę komputera i kliknij **Next (Dalej)**.
3. W obszarze **Date and time (Data i godzina)** skonfiguruj poniższe ustawienia i kliknij przycisk **Next (Dalej)**.
 - Wybierz strefę czasową.
 - Aby skonfigurować serwer NTP, wybierz opcję **NTP server (Serwer NTP)** i wprowadź adres serwera NTP.
 - Aby ręcznie wykonać konfigurację, wybierz **Manual (Ręcznie)** oraz wybierz datę i godzinę.
4. W obszarze **Network settings (Ustawienia sieci)** skonfiguruj poniższe ustawienia i kliknij przycisk **Next (Dalej)**.
 - Opcje **Use automatic IP settings (DHCP) (Używaj automatycznych ustawień IP)** i **Use automatic DNS settings (Używaj automatycznych ustawień serwera DNS)** są domyślnie włączone.
 - Jeśli urządzenie jest podłączone do sieci z serwerem DHCP, zostaną automatycznie wyświetlone przypisany adres IP, maska podsieci, brama i preferowany DNS.
 - Jeśli urządzenie nie jest podłączone do sieci lub nie jest dostępny serwer DHCP, wprowadź ręcznie adres IP, maskę podsieci, bramę i preferowany DNS w zależności od wymagań sieci.
5. Kliknij przycisk **Finish (Zakończ)**. W razie zmiany nazwy komputera aplikacja AXIS Recorder Toolbox wyświetli monit o ponowne uruchomienie urządzenia.

Zaloguj się do serwera

Za pomocą aplikacji klienckiej AXIS Camera Station można nawiązać połączenie wieloma serwerami lub z jednym serwerem zainstalowanymi na lokalnym komputerze lub w innym miejscu w sieci albo z wieloma serwerami. Z serwerami AXIS Camera Station można łączyć się na różne sposoby.

Ostatni używany serwer – Nawiąż połączenie z serwerami użytymi w poprzedniej sesji.

Ten komputer – Nawiąż połączenie z serwerem zainstalowanym na tym samym komputerze, co aplikacja kliencka.

Serwer zdalny – Patrz *Łączenie z serwerem zdalnym, on page 16*.

AXIS Secure Remote Access – Patrz *Zaloguj się do AXIS Secure Remote Access, on page 16*.

Uwaga

Gdy klient próbuje nawiązać połączenie z serwerem po raz pierwszy, sprawdza identyfikator certyfikatu serwera. Aby mieć pewność, że łączysz się z odpowiednim serwerem, ręcznie porównaj identyfikator certyfikatu z widocznym w aplikacji AXIS Camera Station Service Control.

Server list (Lista serwerów)	Aby połączyć się z serwerami z listy serwerów, wybierz serwer z menu rozwijanego Server list (Lista serwerów) . Kliknij  , aby utworzyć lub edytować listy serwerów.
Import server list (Importuj listę serwerów)	Aby zaimportować plik listy serwerów wyeksportowany z AXIS Camera Station, kliknij Import server list (Importuj listę serwerów) w prawym dolnym rogu i przejdź do pliku .msl.
Delete saved passwords (Usuń zapisane hasła)	Aby usunąć zapisane nazwy użytkowników i hasła ze wszystkich połączonych serwerów, kliknij Delete saved passwords (Usuń zapisane hasła) .
Change client proxy settings (Zmień ustawienia klienta proxy)	Aby połączyć się z serwerem, konieczna może być zmiana ustawień serwera proxy klienta. W tym celu kliknij Change client proxy settings (Zmień ustawienia serwera proxy klienta) .

Łączenie z serwerem zdalnym

- Wybierz opcję **Remote server (Serwer zdalny)**.
- Wybierz serwer z listy rozwijanej **Remote server (Serwer zdalny)** albo wpisz adres IP lub DNS. Jeżeli serwera nie ma na liście, kliknij przycisk , aby odświeżyć listę wszystkich dostępnych serwerów zdalnych. Jeżeli na serwerze skonfigurowano akceptowanie połączenia od klientów na portach innych niż domyślny 55754, wprowadź adres IP, a nim numer portu, na przykład 192.168.0.5:46001.
- Wypróbuj jedno z poniższych rozwiązań:
 - Wybierz **Log in as current user (Zaloguj się jako bieżący użytkownik)**, aby zalogować się jako obecny użytkownik systemu Windows®.
 - Wyczyść pole wyboru **Zaloguj się jako bieżący użytkownik** i kliknij przycisk **Zaloguj**. Zaznacz opcję **Other user (Inny użytkownik)** i podaj inną nazwę użytkownika oraz hasło, aby się zalogować za pomocą tych poświadczeń.

Zaloguj się do AXIS Secure Remote Access

Ważne

Aby zwiększyć bezpieczeństwo i funkcjonalność, uaktualniamy funkcję **Axis Secure Remote Access (v1)** do **Axis Secure Remote Access v2**. Obecna wersja zostanie wycofana 1 grudnia 2025 r. Zalecamy przejście na funkcję **Axis Secure Remote Access v2**, przed tym terminem.

Co to oznacza dla systemu **AXIS Camera Station S2108 Appliance**?

- Po 1 grudnia 2025 r. zdalny dostęp do systemu za pośrednictwem funkcji **Axis Secure Remote Access (v1)** nie będzie możliwy.
- Aby korzystać z funkcji **Axis Secure Remote Access v2**, należy wykonać uaktualnienie do **AXIS Camera Station Pro** w wersji 6.8. Do 1 marca 2026 r. aktualizacja jest bezpłatna dla wszystkich użytkowników systemu **AXIS Camera Station 5**.

Uwaga

- Klient łączący się z serwerem za pomocą usługi **Axis Secure Remote Access**. Serwer nie może uaktualnić klienta automatycznie.
 - Jeśli serwer proxy znajduje się między urządzeniem sieciowym a serwerem **AXIS Camera Station S2108 Appliance**, należy skonfigurować ustawienia serwera proxy w systemie **Windows** na serwerze **AXIS Camera Station S2108 Appliance**, aby umożliwić dostęp do serwera za pomocą usługi **AXIS Secure Remote Access**.
- Kliknij łącze **Sign in to AXIS Secure Remote Access (Zaloguj się do AXIS Secure Remote Access)**.

2. Wprowadź dane swojego konta MyAxis.
3. Kliknij przycisk **Sign in (Zaloguj)**.
4. Kliknij **Grant (Przyznaj)**.

Konfiguracja aplikacji AXIS Camera Station

Ten samouczek przeprowadzi Cię przez podstawowe kroki, które pozwolą Ci uruchomić system.

Zanim zaczniesz:

- Skonfiguruj sieć w zależności od instalacji. Patrz *Network configuration (Konfiguracja sieci)*, on page 19.
- W razie potrzeby skonfiguruj porty serwera. Patrz *Konfiguracja portu serwera*, on page 19.
- Weź pod uwagę kwestie bezpieczeństwa. Patrz *Kwestie dotyczące bezpieczeństwa*.

Po wykonaniu niezbędnych konfiguracji można rozpocząć korzystanie z aplikacji AXIS Camera Station:

1. *Uruchom system VMS*, on page 17
2. *Dodawanie urządzeń*, on page 17
3. *Konfiguracja metody zapisu*, on page 17
4. *Oglądaj materiał wideo na żywo*, on page 18
5. *Wyświetl nagrania*, on page 18
6. *Dodawanie zakładki*, on page 18
7. *Eksportuj nagrania*, on page 18
8. *Odtwarzanie i weryfikacja zapisów w AXIS File Player*, on page 18

Uruchom system VMS

Kliknij dwukrotnie ikonę klienta AXIS Camera Station, aby uruchomić klienta. Przy pierwszym uruchomieniu klient próbuje zalogować się do serwera AXIS Camera Station zainstalowanego na tym samym komputerze co klient.

Z wieloma serwerami AXIS Camera Station można łączyć się na różne sposoby.

Dodawanie urządzeń

Strona Add devices (Dodaj urządzenia) otwiera się, gdy po raz pierwszy włączysz AXIS Camera Station. AXIS Camera Station przeszukuje sieć w poszukiwaniu podłączonych urządzeń i wyświetla listę znalezionych urządzeń.

1. Wybierz z listy kamery, które chcesz dodać. Jeśli nie możesz znaleźć kamery, kliknij **Manual search (Wyszukiwanie ręczne)**.
2. Kliknij **Dodaj**.
3. Wybierz **Quick configuration (Szybka konfiguracja)** lub **Site Designer configuration (Konfiguracja AXIS Site Designer)**. Kliknij **Next (Dalej)**.
4. Użyj ustawień domyślnych i upewnij się, że metoda zapisu jest ustawiona na **None (Brak)**. Kliknij przycisk **Install (Instaluj)**.

Konfiguracja metody zapisu

1. Wybierz kolejno opcje **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.
2. Wybierz kamerę.
3. Włącz **Motion detection (Po detekcji ruchu)**, or **Continuous (Ciągłe)** lub obie te opcje.

4. Kliknij przycisk **Apply (Zastosuj)**.

Oglądaj materiał wideo na żywo

1. Otwórz kartę **Live view (Podgląd na żywo)**.
2. Wybierz kamerę, aby oglądać jej obraz na żywo.

Wyświetl nagrania

1. Otwórz kartę **Recordings (Nagrania)**.
2. Wybierz kamerę, z której chcesz wyświetlić nagrania.

Dodawanie zakładki

1. Przejdź do nagrania.
2. Ustaw znacznik w odpowiednim położeniu poprzez powiększanie, pomniejszanie i przesuwanie na osi czasu.
3. Kliknij .
4. Wprowadź nazwę i opis zakładki. Użyj słów kluczowych, aby łatwo znaleźć zakładkę.
5. Wybierz **Prevent recording deletion (Chroń zapis przed usunięciem)**, aby zablokować zapis.

Uwaga

Aby odblokować nagranie, usuń zaznaczenie **Prevent recording deletion (Chroń zapis przed usunięciem)** lub usuń zakładkę.

6. Kliknij przycisk **OK**, aby zapisać zakładkę.

Eksportuj nagrania

1. Otwórz kartę **Recordings (Nagrania)**.
2. Wybierz kamerę, z której chcesz eksportować nagrania.
3. Kliknij , aby wyświetlić znaczniki wyboru.
4. Przeciągnij odpowiednie znaczniki, aby uwzględnić zapis, który chcesz wyeksportować.
5. Kliknij , aby otworzyć kartę **Export (Eksportuj)**.
6. Kliknij **Export...** (Eksportuj).

Odtwarzanie i weryfikacja zapisów w AXIS File Player

1. Przejdź do folderu z wyeksportowanymi nagraniami.
2. Kliknij dwukrotnie **AXIS File Player**.
3. Kliknij  w celu wyświetlenia notatek dotyczących nagrania.
4. Aby zweryfikować podpis cyfrowy:
 - 4.1. Przejdź do menu **Tools > Verify digital signature (Narzędzia > Weryfikuj podpis cyfrowy)**.
 - 4.2. Wybierz **Validate with password (Uwierzytelnij hasłem)** i wprowadź hasło.
 - 4.3. Kliknij **Verify (Weryfikuj)**, aby zapoznać się z wynikami weryfikacji.

Uwaga

- Podpis cyfrowy różni się od podpisanego obrazu. Podpisany obraz (nagranie) pozwala ustalić kamerę, z

której pochodzi, dzięki czemu można sprawdzić, czy nie doszło w niej do sabotażu. Więcej informacji można znaleźć w sekcji *Signed video (Podpisane wideo)* i instrukcji użytkownika kamery.

- Jeżeli przechowywane pliki nie mają połączenia z bazą danych programu AXIS Camera Station (pliki nieindeksowane), należy poddać je konwersji, by możliwe było odtwarzanie ich w programie AXIS File Player. Aby uzyskać wsparcie w tym zakresie, prosimy o kontakt z pomocą techniczną Axis.

Network configuration (Konfiguracja sieci)

Skonfiguruj ustawienia serwera proxy lub zapory, zanim zaczniesz używać aplikacji AXIS Camera Station, jeśli klient AXIS Camera Station, serwer AXIS Camera Station i podłączone urządzenia sieciowe znajdują się w różnych sieciach.

Ustawienia proxy klienta

Jeśli klient i serwer są oddzielone serwerem proxy, skonfiguruj ustawienia proxy klienta.

1. Otwórz klienta aplikacji Axis Camera Station.
2. Kliknij **Change client proxy settings (Zmień ustawienia proxy klienta)**.
3. Zmień ustawienia proxy klienta.
4. Kliknij **OK**.

Ustawienia proxy na serwerze

Jeśli urządzenia sieciowe i serwerowe są oddzielone serwerem proxy, skonfiguruj ustawienia proxy serwera.

1. Otwórz program AXIS Camera Station Service Control.
2. Wybierz **Modify settings (Zmień ustawienia)**.
3. W sekcji ustawień proxy użyj domyślnego ustawienia **System account internet option** lub wybierz opcję **Use manual proxy settings (Użyj ręcznych ustawień proxy)**.
4. Kliknij przycisk **Zapisz**.

NAT i Zapora sieciowa

Jeśli klient i serwer są oddzielone przez NAT, zaporę sieciową lub podobny element, należy skonfigurować NAT lub zaporę tak, aby ruch portu HTTP, portu TCP i portu przesyłania strumieniowego, które określono w usłudze AXIS Camera Station Service Control, może przechodzić przez zaporę lub NAT. Skontaktuj się z administratorem sieci w celu uzyskania instrukcji dotyczących konfigurowania NAT lub zapory.

Konfiguracja portu serwera

Serwer AXIS Camera Station używa portów 55752 (HTTP), 55754 (TCP), 55756 (komunikacja mobilna) oraz 55757 (strumieniowanie w sieci komórkowej) do komunikacji między serwerem a klientem. W razie potrzeby porty można zmieniać w usłudze AXIS Camera Station Service Control.

Kwestie dotyczące bezpieczeństwa

Aby zapobiec nieuprawnionemu dostępowi do kamer i nagrań:

- Używaj silnych haseł dla wszystkich urządzeń sieciowych (kamer, koderów wideo i urządzeń pomocniczych).
- Zainstaluj serwer AXIS Camera Station S2108 Appliance, kamery, kodery wizyjne i urządzenia pomocnicze w zabezpieczonej sieci odseparowanej od sieci biurowej. Klienta AXIS Camera Station S2108 Appliance możesz zainstalować na komputerze w innej sieci, na przykład sieci z dostępem do Internetu.
- Upewnij się, że wszyscy użytkownicy mają silne hasła.

Licencja na system online

Zarówno klient AXIS Camera Station, jak i serwer muszą mieć połączenie z Internetem.

1. Przejdź do menu **Configuration > Licenses > Management** (Konfiguracja > Licencje > Zarządzanie).
2. Upewnij się, że opcja **Manage licenses online** (Zarządzaj licencjami online) zostanie włączona.
3. Zaloguj się przy użyciu konta My Axis.
4. Klucz licencyjny jest generowany automatycznie i wyświetlany w obszarze **License keys** (Klucze licencyjne).
5. Jeżeli klucze licencyjne zostały zakupione osobno, wprowadź klucz licencyjny w polu **Add license key** (Dodaj klucz licencyjny).
6. Kliknij **Dodaj**.
7. W kliencie AXIS Camera Station upewnij się, że klucze licencyjne są wyświetlane w sekcji **Configuration** (Konfiguracja) > **Licenses** (Licencje) > **Keys** (Klucze).

Licencja na system w trybie offline

1. Przejdź do menu **Configuration > Licenses > Management** (Konfiguracja > Licencje > Zarządzanie).
2. Wyłącz opcję **Manage licenses online** (Zarządzaj licencjami online).
3. Kliknij **Export system file** (Eksportuj plik systemowy).
4. Zapisz plik systemowy na dysku flash USB.
5. Zaloguj się przy użyciu konta My Axis.
6. Kliknij **Upload system file** (Wczytaj plik systemowy), aby wczytać plik z dysku flash USB.
7. Klucz licencyjny jest generowany automatycznie i wyświetlany w obszarze **License keys** (Klucze licencyjne).
8. Jeżeli klucze licencyjne zostały zakupione osobno, wprowadź klucz licencyjny w polu **Add license key** (Dodaj klucz licencyjny).
9. Kliknij **Dodaj**.
10. W obszarze **License keys** (Klucze licencji) kliknij **Download license file** (Pobierz plik licencji) i zapisz plik na dysku flash USB.
11. W kliencie AXIS Camera Station przejdź do obszaru **Configuration** (Konfiguracja) > **Licenses** (Licencje) > **Management** (Zarządzanie).
12. Kliknij **Import license file** (Importuj plik licencji) i wybierz plik licencji znajdujący się na dysku flash USB.
13. Upewnij się, że klucze licencyjne są wyświetlane w sekcji **Configuration** (Konfiguracja) > **Licenses** (Licencje) > **Keys** (Klucze).

Zarządzanie lokalnymi kontami użytkowników systemu Windows®

Tworzenie konta użytkownika

Aby zwiększyć bezpieczeństwo danych osobowych i informacji, zalecamy dodanie hasła dla każdego konta lokalnego.

Ważne

Musisz zapamiętać hasło do konta lokalnego. W przypadku konta lokalnego nie istnieje możliwość odzyskania zapomnianego hasła.

1. Przejdź do menu **Settings > Accounts > Other people > Add someone else to this PC** (Ustawienia > Konta > Inne osoby > Dodaj inną osobę do tego komputera).
2. Kliknij **I don't have this person's sign-in information** (Nie mam danych logowania tej osoby).
3. Kliknij **Add a user without a Microsoft account** (Dodaj użytkownika bez konta Microsoft).
4. Wprowadź nazwę użytkownika, hasło i wskazówkę dotyczącą hasła.
5. Kliknij **Next** (Dalej) i postępuj zgodnie z instrukcjami.

Utwórz konto administratora

1. Przejdź do menu **Settings > Accounts > Other people** (Ustawienia > konta > inne osoby).
2. Przejdź do konta, które chcesz zmienić, a następnie kliknij przycisk **Change account type** (Zmień typ konta).
3. Przejdź do menu **Account type** (Typ konta) i wybierz opcję **Administrator**.
4. Kliknij **OK**.
5. Uruchom ponownie urządzenie i zaloguj się przy użyciu nowego konta administratora.

Tworzenie lokalnej grupy użytkowników

1. Przejdź do opcji **Computer Management** (Zarządzanie komputerem).
2. Przejdź do menu **Local Users and Groups > Group** (Lokalni użytkownicy i grupy > Grupa).
3. Kliknij prawym przyciskiem myszy **Group** (Grupa) i wybierz **New group** (Nowa grupa).
4. Wprowadź nazwę grupy i opis.
5. Dodawanie członków grupy:
 - 5.1. Kliknij **Dodaj**.
 - 5.2. Kliknij przycisk **Advanced** (Zaawansowane).
 - 5.3. Znajdź konta użytkowników, które chcesz dodać do grupy, i kliknij przycisk **OK**.
 - 5.4. Kliknij ponownie przycisk **OK**.
6. Kliknij polecenie **Create** (Utwórz).

Usuwanie konta użytkownika

Ważne

Usunięcie konta użytkownika spowoduje usunięcie go także z ekranu logowania. Ponadto zostaną usunięte wszystkie pliki, ustawienia i dane programów zapisane na koncie użytkownika.

1. Przejdź do menu **Settings > Accounts > Other people** (Ustawienia > konta > inne osoby).
2. Przejdź do konta, które chcesz usunąć, a następnie kliknij przycisk **Remove** (Usuń).

Zmienianie hasła do konta użytkownika

1. Zaloguj się przy użyciu konta administratora.

2. Przejdź do menu **User Accounts > User Accounts > Manage another account in sequence** (Konta użytkownika > Konta użytkownika > Zarządzaj następnym kontem w kolejności). Zostanie wyświetlona lista wszystkich kont użytkownika na tym urządzeniu.
3. Wybierz konto użytkownika, którego hasło chcesz zmienić.
4. Kliknij **Change the password (Zmień hasło)**.
5. Wprowadź nowe hasło i kliknij na przycisk **Change password (Zmień hasło)**.

Tworzenie dysku resetowania hasła dla konta użytkownika

Zalecamy utworzenie dysku resetowania hasła w postaci dysku flash USB. Umożliwi on zresetowanie hasła. Bez dysku resetowania hasła zresetowanie hasła nie będzie możliwe.

Uwaga

Jeśli używasz systemu Windows® 10 lub nowszego, możesz dodać do konta lokalnego pytania zabezpieczające na wypadek zapomnienia hasła, dzięki czemu nie musisz tworzyć dysku resetowania hasła. W tym celu przejdź do menu **Start** i kliknij **Settings > Sign-in options > Update your security questions** (Ustawienia > Opcje logowania > Zaktualizuj pytania zabezpieczające).

1. Zaloguj się do urządzenia przy użyciu konta użytkownika lokalnego. Nie można utworzyć dysku resetowania hasła dla podłączonego konta.
2. Podłącz pusty dysk flash USB do urządzenia.
3. W polu wyszukiwania systemu Windows® przejdź do menu **Create a password reset disk (Utwórz dysk resetowania hasła)**.
4. W asystencie konfiguracji **Forgotten Password (Zapomniane hasło)** kliknij **Next (Dalej)**.
5. Wybierz dysk flash USB i kliknij przycisk **Next (Dalej)**.
6. Wpisz aktualne hasło i kliknij **Next (Dalej)**.
7. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
8. Odłącz dysk flash USB i przechowuj go w bezpiecznym miejscu. Nie musisz tworzyć nowego dysku, gdy chcesz zmienić hasło, nawet jeśli będziesz wielokrotnie zmieniać hasło.

Zarządzanie kontami użytkowników w aplikacji AXIS Camera Station

Uprawnienia użytkownika

Przejdź do Configuration > Security > User permissions (Konfiguracja > Bezpieczeństwo > Uprawnienia użytkowników), aby wyświetlić użytkowników i grupy w AXIS Camera Station S2108 Appliance.

Uwaga

Administratorzy komputera, na którym jest uruchomiony serwer AXIS Camera Station S2108 Appliance, automatycznie otrzymują uprawnienia administratora w AXIS Camera Station S2108 Appliance. Nie można zmienić ani usunąć uprawnień grupy administratorów.

Przed dodaniem użytkownika lub grupy sprawdź, czy są zarejestrowani na komputerze lokalnym lub mają konto użytkownika w usłudze Windows® Active Directory. Aby dodać użytkowników lub grupy, patrz *Dodawanie użytkowników lub grup*.

Gdy użytkownik należy do grupy, otrzymuje najwyższą rolę uprawnień przydzieloną jemu bądź grupie. Na przykład użytkownik mający dostęp do kamery X należący równocześnie do grupy z dostępem do kamer Y i Z ma dostęp do wszystkich trzech kamer.

	Wskazuje, że dana pozycja dotyczy indywidualnego użytkownika.
	Wskazuje, że pozycja dotyczy grupy.
Nazwa	Nazwa użytkownika wyświetlana na komputerze lokalnym lub w usłudze Active Directory.
Domena	Domena, do której należy użytkownik lub grupa.
Rola	Rola dostępu przydzielona użytkownikowi lub grupie. Możliwe wartości: administrator, operator i dozorca.
Szczegóły	Szczegółowe informacje o użytkownikach pojawiające się na komputerze lokalnym lub w usłudze Active Directory.
Serwer	Serwer, do którego należy użytkownik lub grupa.

Dodawanie użytkowników lub grup

Użytkownicy i grupy systemu Microsoft Windows® oraz usługi Active Directory mają dostęp do AXIS Camera Station S2108 Appliance. Aby dodać użytkownika do AXIS Camera Station S2108 Appliance, należy dodać użytkowników lub grupę do systemu Windows®.

Aby dodać użytkownika w systemie Windows® 10 i 11:

- Naciśnij klawisz Windows + X i wybierz opcję **Computer Management (Zarządzanie komputerem)**.
- W oknie **Computer Management (Zarządzanie komputerem)** przejdź do sekcji **Local Users and Groups (Lokalni użytkownicy i grupy) > (Users) Użytkownicy**.
- Kliknij prawym przyciskiem myszy **Users (Użytkownicy)** i wybierz opcję **New User (Nowy użytkownik)**.
- W wyskakującym oknie dialogowym wpisz dane nowego użytkownika i usuń zaznaczenie pola **User must change password at next login (Użytkownik musi zmienić hasło przy następnym logowaniu)**.
- Kliknij polecenie **Create (Utwórz)**.

Jeżeli korzystasz z domeny Active Directory, skonsultuj się z administratorem sieci.

Dodawanie użytkowników lub grup

1. Przejdź do obszaru **Configuration (Konfiguracja) > Security (Zabezpieczenia) > User permissions (Uprawnienia użytkownika)**.

2. Kliknij **Dodaj**. Na liście pojawią się dostępni użytkownicy i grupy.
3. W obszarze **Scope (Zakres)** wybierz lokalizację, w której chcesz szukać użytkowników i grupy.
4. W menu **Show (Pokaż)** wybierz wyświetlanie użytkowników lub grup. Wyniki wyszukiwania mogą się nie wyświetlić, jeżeli liczba użytkowników lub grup jest zbyt duża. Użyj filtru, aby zawęzić wyniki.
5. Wybierz użytkowników lub grupy i kliknij **Add (Dodaj)**.

Scope (Zakres)	
Serwer	Wybierz tę opcję, aby wyszukać użytkowników lub grupy na komputerze lokalnym.
Domena	Ta funkcja umożliwia wyszukiwanie użytkowników lub grupy usługi Active Directory.
Selected server (Wybrany serwer)	W przypadku połączenia z wieloma serwerami AXIS Camera Station S2108 Appliance wybierz serwer, na którym odbędzie się wyszukiwanie użytkowników lub grup.

Konfigurowanie użytkownika lub grupy

1. Wybierz użytkownika lub grupę z listy.
2. W obszarze **Role (Rola)** wybierz opcję **Administrator**, **Operator** lub **Viewer (Dozorca)**.
3. W przypadku wybrania opcji **Operator** lub **Viewer (Dozorca)** można skonfigurować uprawnienia użytkownika lub grupy. Patrz *Uprawnienia użytkownika/grupy*.
4. Kliknij przycisk **Zapisz**.

Usuwanie użytkownika lub grupy

1. Wybierz użytkownika lub grupę.
2. Kliknij przycisk **Remove (Usuń)**.
3. W wyskakującym oknie dialogowym kliknij przycisk **OK**, aby usunąć użytkownika lub grupę.

Uprawnienia użytkownika/grupy

Do użytkownika lub grupy można przypisać trzy role. Aby uzyskać informacje na temat definiowania ról dla użytkownika lub grupy, zobacz *Dodawanie użytkowników lub grup*.

Administrator – Pełny dostęp do całego systemu, w tym dostęp do obrazów na żywo i zarejestrowanego materiału wideo z wszystkich kamer. Użytkownik z tymi uprawnieniami ma dostęp do wszystkich portów i widoków WE/WY. Rola ta wymagana jest, aby uzyskać dostęp do konfiguracji systemowej.

Operator – Wybierz kamery, widoki i porty we / wy, aby uzyskać dostęp do podglądu na żywo i nagrań. Operator ma pełny dostęp do wszystkich funkcji AXIS Camera Station S2108 Appliance – oprócz opcji konfiguracji systemu.

Dozorca – Dostęp do obrazów na żywo z wybranych kamer i dostęp do zaznaczonych portów oraz widoków WE/WY. Dozorca nie ma dostępu do zarejestrowanego materiału wideo ani konfiguracji systemu.

Kamery

Następujące uprawnienia dostępu są dostępne dla użytkowników lub grup z rolą **Operator (Operator)** lub **Viewer (Dozorca)**.

Wejdź na stronę	Umożliwia dostęp do kamery i wszystkich funkcji kamery.
Nagranie wideo	Umożliwia dostęp do wideo w trybie na żywo z kamery.
Nasłuch audio	Umożliwia dostęp w celu słuchania przez kamerę.
Odtwarzanie komunikatu audio	Dostęp do mówienia do kamery.
Manual Recording (Nagrywanie manualne)	Umożliwia ręczne uruchamianie i zatrzymywanie zapisu.
Mechanical PTZ (Mechaniczny PTZ)	Zezwala na dostęp do mechanicznych funkcji sterowania PTZ. Opcja dostępna tylko dla kamer wyposażonych w mechaniczne sterowanie PTZ.
Priorytet PTZ	Umożliwia ustawienie priorytetu PTZ. Mniejsza wartość oznacza wyższy priorytet. Żaden przypisany priorytet nie jest ustawiony jako 0. Najwyższy priorytet ma administrator. Gdy kamera PTZ jest obsługiwana przez osobę o wyższym priorytecie, inne osoby nie mogą obsługiwać tej samej kamery przez 10 sekund. Opcja dostępna tylko dla kamer z mechanicznym sterowaniem PTZ, które mają zaznaczoną opcję Mechanical PTZ (Mechaniczne PTZ).

Widoki

Następujące uprawnienia dostępu są dostępne dla użytkowników lub grup z rolą **Operator (Operator)** lub **Viewer (Dozorca)**. Można wybrać wiele widoków i ustawić uprawnienia dostępu.

Wejdź na stronę	Umożliwia dostęp do widoków w AXIS Camera Station S2108 Appliance.
Edytuj	Umożliwia edycję widoków w AXIS Camera Station S2108 Appliance.

We/wy

Następujące uprawnienia dostępu są dostępne dla użytkowników lub grup z rolą **Operator (Operator)** lub **Viewer (Dozorca)**.

Wejdź na stronę	Zezwala na pełny dostęp do portu WE/WY.
Zapoznaj się z	Umożliwia wyświetlanie stanu portu we / wy bez wprowadzania zmian.
Write (Zapis)	Umożliwia zmianę stanu portu we / wy.

System

Nie można skonfigurować wyszczególnionych uprawnień dostępu na liście. Znacznik oznacza, że uprawnienie jest domyślnie przypisane do użytkownika albo grupy.

Następujące uprawnienia dostępu są dostępne dla użytkowników lub grup z rolą **Operator**. W przypadku roli **Viewer (Dozorca)** dostępna jest też funkcja **Take snapshots (Wykonywanie ujęć)**.

Wykonaj ujęcia	Umożliwia tworzenie ujęć w trybie podglądu na żywo i trybie zapisu.
Eksportuj nagrania	Umożliwia eksportowanie zapisów.
Generuj raport o zdarzeniu	Zezwala na generowanie raportów o zdarzeniach.
Prevent access to recordings older than (Blokowanie dostępu do nagrań starszych niż)	Zapobiega dostępowi do nagrań wcześniejszych niż podana liczba minut. Użytkownicy nie znajdą tych nagrań przy wyszukiwaniu.
Dostęp do alarmów, zadań i dzienników	Umożliwia odbierania powiadomień o alarmach i zezwala na dostęp do paska Alarms and tasks (Alarmy i zadania) oraz karty Logs (Dzienniki) .
Access data search (Dostęp do wyszukiwania danych)	Umożliwiają wyszukiwanie danych w celu śledzenia tego, co wydarzyło się w czasie zdarzenia.
Add categories to events (Dodaj kategorie do zdarzeń)	Umożliwia dodawanie kategorii do zdarzeń na karcie Recordings (Nagrania) .
Remove categories from event (Usuń kategorie ze zdarzenia)	Umożliwia usuwanie kategorii ze zdarzeń na karcie Recordings (Nagrania) .

Kontrola dostępu

Następujące uprawnienia dostępu są dostępne dla użytkowników lub grup z rolą **Operator**. **Access Management (Zarządzanie dostępem)** jest też dostępne dla roli **Viewer (Dozorca)**.

Konfiguracja kontroli dostępu	Umożliwia konfigurację drzwi i stref, profili identyfikacyjnych, formatów kart i kodów PIN, szyfrowanej komunikacji i środowiska wieloserwerowego.
Zarządzanie dostępem	Umożliwia zarządzanie dostępem i dostęp do ustawień usługi Active Directory.

Następujące uprawnienia dostępu są dostępne dla użytkowników lub grup z rolą **Viewer (Dozorca)**.

Monitorowanie stanu systemu

Następujące uprawnienia dostępu są dostępne dla użytkowników lub grup z rolą **Operator**. **Access to system health monitoring (Dostęp do monitorowania stanu systemu)** jest też możliwy w przypadku roli **Viewer (Dozorca)**.

Configuration of system health monitoring (Konfiguracja monitorowania stanu systemu)	Umożliwia konfigurowanie monitorowania stanu systemu.
Access to system health monitoring (Dostęp do monitorowania stanu systemu)	Umożliwia dostęp do monitorowania stanu systemu.

Zarządzanie urządzeniem

Aktualizacja certyfikatów bezpiecznego uruchamiania

W czerwcu 2026 r. Microsoft wycofuje certyfikaty bezpiecznego uruchamiania 2011, zastępując je certyfikatami 2023. Aby zapewnić bezpieczeństwo rejestratora, zainstaluj certyfikaty 2023 wcześniej.

Instalacja certyfikatów 2023 wymaga systemu Windows 10 LTSC (Long-Term Servicing Channel) lub Windows 11 LTSC. Jeżeli Twoje urządzenie jest objęte gwarancją, ale działa pod kontrolą systemu Windows 10 SAC (Semi-Annual Channel) zamiast wersji LTSC, prosimy o kontakt z działem pomocy technicznej Axis. Pomoc techniczna doradzi, czy aktualizacja do wersji LTSC jest możliwa przed aktualizacją BIOS-u lub zmianą jakichkolwiek certyfikatów.

Uwaga

Po czerwcu 2026 r. urządzenia bez certyfikatów 2023 będą działać normalnie, ale nie będą otrzymywać nowych zabezpieczeń dotyczących wczesnego etapu uruchamiania systemu, w tym aktualizacji menedżera rozruchu Windows Boot Manager ani list unieważnionych certyfikatów związanych z nowymi lukami w zabezpieczeniach.

Sprawdzanie stanu certyfikatu

Aby sprawdzić, czy certyfikaty 2023 zostały zainstalowane oraz czy bootloader systemu Windows został zaktualizowany, użyj jednej z dwu metod:

Metoda 1:

1. Otwórz Registry Editor (Edytor rejestru).
2. Przejdź do HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing.
3. Sprawdź wartość UEFICA2023Status. Jeżeli wartość ma postać Updated (Zaktualizowano), oznacza to, że certyfikat 2023 jest zainstalowany.

 (Default)	REG_SZ	(value not set)
 BucketHash	REG_SZ	5a3041a8e6c7476f988f369de06e65e224df7d53cf7f9...
 ConfidenceLevel	REG_SZ	No Data Observed - Action Required
 ConfidenceUpdateType	REG_DWORD	0x00000000 (0)
 LastParsedBucketDataVersion	REG_DWORD	0x0000000c (12)
 UEFICA2023Status	REG_SZ	Updated
 WindowsUEFICA2023Capable	REG_DWORD	0x00000002 (2)

Metoda 2:

1. Otwórz Windows Security (Zabezpieczenia systemu Windows).
2. Przejdź do Device security (Bezpieczeństwo urządzenia).
3. W sekcji Secure boot (Bezpieczne uruchamianie) sprawdź komunikat o stanie. Jeżeli certyfikat jest aktualny, na karcie wyświetla się komunikat: „Secure Boot is on and all required certificate updates have been applied. No further certificate changes are needed” (Bezpieczne uruchamianie jest włączone, a wszystkie wymagane aktualizacje certyfikatu zostały zastosowane. Nie są konieczne dalsze zmiany w certyfikacie).

Secure boot

Secure Boot is on and all required certificate updates have been applied.
No further certificate changes are needed.

Uwaga

Funkcja Zabezpieczenia systemu Windows wyświetla stan certyfikatu tylko, jeżeli w urządzeniu zainstalowano aktualizację zbiorczą z 14 kwietnia 2026 r. lub nowszą. Jeżeli nie wyświetla się komunikat dotyczący stanu certyfikatu, zainstaluj najnowszą aktualizację systemu Windows lub skorzystaj z Metody 1.

Zalecane działania

Aktualizacja BIOS-u powoduje trwałe zapisanie certyfikatów 2023 w oprogramowaniu układowym. Jest to metoda najbardziej niezawodna i zalecana nawet jeżeli certyfikaty zostały już zainstalowane za pośrednictwem usługi Windows Update.

Ważne

Jeżeli zainstalujesz certyfikaty tylko za pośrednictwem usługi Windows Update, a następnie zresetujesz klucze bezpiecznego uruchamiania w BIOS-ie do ustawień fabrycznych, certyfikaty zostaną utracone, a urządzenie nie uruchomi się przy włączonym bezpiecznym uruchamianiu. Przed zresetowaniem kluczy bezpiecznego uruchamiania zaktualizuj BIOS, aby certyfikaty zostały trwałe zapisane.

Aktualizacja certyfikatu poprzez BIOS

Zainstaluj wersję BIOS-u przeznaczoną dla Twojego modelu lub nowszą. Wersje możesz pobrać ze strony produktu w witrynie Axis.com:

Model	Minimalna wersja BIOS-u
AXIS S2208	Do ustalenia
AXIS S2212	Do ustalenia
AXIS S2216	Do ustalenia
AXIS S2224	Do ustalenia
AXIS S2108	Z218-004
AXIS S2208 Mk II	Z670-005
AXIS S2212 Mk II	Z671-005
AXIS S2216 Mk II	Z672-005
AXIS S2224 Mk II	Z673-005

Aktualizacja certyfikatu za pomocą usługi Windows Update

Jeżeli aktualizacja BIOS-u nie jest jeszcze dostępna w posiadanym modelu, możesz pobrać certyfikaty 2023 za pośrednictwem usługi Windows Update.

Ważne

Certyfikaty zainstalowane w ten sposób przechowywane są w bieżącej bazie danych Secure Boot (Bezpieczne uruchamianie), a nie w oprogramowaniu układowym. W sytuacji przywrócenia ustawień fabrycznych kluczy bezpiecznego uruchamiania w BIOS-ie utracisz certyfikaty, a urządzenie może nie uruchomić się przy włączonej funkcji Secure Boot (Bezpieczne uruchamianie). Zainstaluj aktualizację BIOS-u, jak tylko będzie dostępna dla Twojego modelu, nawet jeżeli skorzystałeś już z tego sposobu.

Aby skorzystać z tej ścieżki:

1. Sprawdź, czy w Twoim urządzeniu zainstalowany jest system Windows 10 LTSC lub Windows 11 LTSC.
2. Zainstaluj wszystkie aktualizacje systemu Windows wydane 14 kwietnia 2026 r. lub później.
3. Przejdź do **Windows Security > Device security > Secure Boot** (Zabezpieczenia systemu Windows > Bezpieczeństwo urządzeń > Bezpieczne uruchamianie), aby sprawdzić status Twojego certyfikatu.

4. Jeżeli certyfikat nie zaktualizuje się po zainstalowaniu najnowszych aktualizacji, sprawdź wartość rejestru **UEFICA2023Status**. Jeżeli Twoje urządzenie nadal nie kwalifikuje się do automatycznej aktualizacji, zaktualizuj BIOS lub skontaktuj się z działem pomocy technicznej Axis.

Ważne

Nie unieważniaj ręcznie certyfikatu 2011, dopóki nie potwierdzisz, że wszystkie nośniki odzyskiwania, środowiska uruchomieniowe oraz sterowniki w Twoim środowisku są podpisane certyfikatem 2023. Zbyt szybkie unieważnienie certyfikatu 2011 spowoduje, że urządzenie nie będzie mogło się uruchomić przy włączonej funkcji Secure Boot (Bezpieczne uruchamianie).

Sprawdzanie bieżącej wersji systemu BIOS

Sprawdzanie bieżącej wersji systemu BIOS:

1. Włącz urządzenie i wielokrotnie naciskaj klawisz **Del** aż do pojawienia się logotypu Axis.
2. Wersja wyświetlana jest jako pierwszy wpis w sekcji **Main** (Strona główna).

Aktualizacja BIOS-u

Postępuj zgodnie z instrukcjami zawartymi w przewodniku dot. obsługi BIOS-u, dostępnym na stronie pobierania pliku BIOS.

Aktualizacja systemu Windows®

System Windows® okresowo sprawdza dostępność aktualizacji. Jeżeli aktualizacja będzie dostępna, urządzenie automatycznie ją pobierze, ale instalację trzeba będzie wykonać ręcznie.

Uwaga

Podczas zaplanowanego ponownego uruchomienia systemu zapis zostanie przerwany.

Aby ręcznie sprawdzić dostępność aktualizacji:

1. Przejdź do obszaru **Settings (Ustawienia) > Windows Update**.
2. Kliknij **Check for updates** (Sprawdź dostępność aktualizacji).

Konfigurowanie ustawień funkcji Windows® Update

Sposób i czas aktualizowania systemu Windows® można zmienić, aby dostosować je do własnych potrzeb.

Uwaga

Podczas zaplanowanego ponownego uruchomienia systemu wszystkie bieżące zapisy są wstrzymywane.

1. Otwórz aplikację **Run**.
 - Przejdź do menu **Windows System > Run** lub
2. Wpisz `gpedit.msc` i kliknij przycisk **OK**. Zostanie otwarty Edytor lokalnych zasad grupy.
3. Przejdź do menu **Computer Configuration > Administrative Templates > Windows Components > Windows Update (Konfiguracja komputera > Szablony administracyjne > Składniki systemu Windows > Windows Update)**.
4. W razie potrzeby skonfiguruj ustawienia (zobacz przykład).

Przykład:

Aby automatycznie pobierać i instalować aktualizacje bez udziału użytkownika oraz aby w razie potrzeby urządzenie było ponownie uruchamiane poza godzinami pracy, należy użyć następującej konfiguracji:

1. Otwórz menu **Always automatically restart at the scheduled time (Zawsze automatycznie uruchamiaj ponownie o zaplanowanej godzinie)** i wybierz:
 - 1.1. **Włączone**
 - 1.2. **Zegar restartu da użytkownikom tyle czasu na zapisanie swojej pracy (minuty): 15.**
 - 1.3. Kliknij **OK**.

2. Otwórz menu **Configure Automatic Updates (Konfigurowanie automatycznych aktualizacji)** i wybierz:
 - 2.1. **Włączone**
 - 2.2. **Konfigurowanie automatycznych aktualizacji:** automatyczne pobieranie i planowanie instalacji
 - 2.3. **Planowanie dnia instalacji:** W każdą niedzielę
 - 2.4. **Planowanie godziny instalacji:** 00:00
 - 2.5. Kliknij OK.
3. Otwórz menu **Allow Automatic Updates immediate installation (Zezwalaj na natychmiastową instalację automatycznych aktualizacji)** i wybierz:
 - 3.1. **Włączone**
 - 3.2. Kliknij OK.

Zarządzanie energią

Łączny budżet mocy przełącznika wynosi 105 W. Jest to maksymalna moc wyjściowa podawana do wszystkich dołączonych urządzeń.

W większości przypadków dołączone urządzenia pobierają mniej mocy niż zakładano. W celu optymalizacji poboru mocy kontroler PoE umożliwia dołączonym urządzeniom żądanie mocy maks. 125 W, jednocześnie ograniczając rzeczywisty pobór mocy do 105 W.

Za przykład niech posłuży przełącznik, który jest w stanie zasilić 8 urządzeń PoE klasy 3.

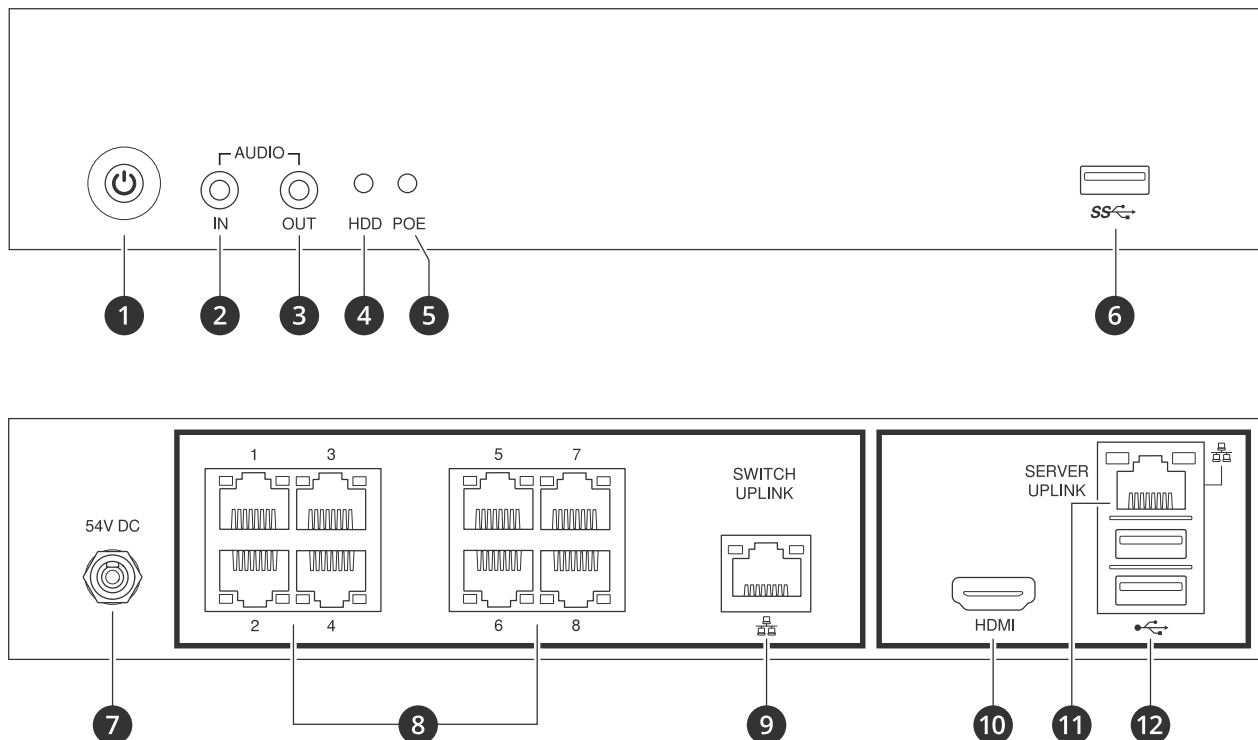
- 1 urządzenie PoE klasy 3 pobiera moc 15,4 W.
- 8 urządzeń PoE klasy 3 pobiera moc $(8 \times 15,4) = 123,2$ W. Wartość ta mieści się w ograniczeniu 125 W dopuszczonym przez kontroler PoE.
- 1 urządzenie PoE klasy 3 pobiera zazwyczaj moc 10 – 12 W.
- 8 urządzeń PoE klasy 3 pobiera zazwyczaj moc 80 – 96 W. Wartość ta mieści się w ograniczeniu 105 W całkowitego budżetu mocy.

▲ OSTRZEŻENIE

- Gdy dołączone urządzenia żądają mocy przekraczającej 125 W:
 - Ostatnie dołączone urządzenie nie uruchomi się.
 - Wskaźnik LED przeciążenia zasilania PoE będzie świecić się stale na czerwono do momentu odłączenia ostatniego dołączonego urządzenia lub uwolnienia wystarczającej ilości mocy PoE poprzez odłączenie innych urządzeń.
- Gdy dołączone urządzenia faktycznie pobierają moc przekraczającą 105 W:
 - Ostatnie włączone urządzenie wyłączy się i podejmie próbę ponownego uruchomienia.
 - Wskaźnik LED przeciążenia zasilania PoE nie zaświeci się.

Przegląd produktów

Przód i tylne boki



- 1 Wskaźnik LED przycisku zasilania/zasilania
- 2 Wejście audio
- 3 Wyjście audio
- 4 Wskaźnik LED aktywności dysku twardego
- 5 Wskaźnik LED stanu portów PoE
- 6 Port USB 3.0
- 7 Złącze zasilania
- 8 Porty PoE
- 9 Port uplink RJ45 przełącznika sieciowego
- 10 Port HDMI
- 11 Port uplink RJ45 serwera
- 12 Porty USB 2.0

Specyfikacje

Przednie diody LED

Wskaźnik LED	Kolor	Wskazanie
Zasilanie	Zielony	Serwer włączony
Dysk twardy	Miga na bursztynowo	Aktywność dysku twardego
	Miga na czerwono	Możliwa awaria dysku twardego
Przeciążenie zasilania PoE	Czerwony	Przekroczenie budżetu mocy PoE
	Wył.	OK

Tylne wskaźniki LED

Szybkość sieci i aktywność sieciowa	Kolor	Wskazanie
Prawy wskaźnik LED	Bursztynowy	10/100 Mbit/s
	Zielony ¹	1000 Mbit/s
Lewy wskaźnik LED	Miga na zielono	Aktywność sieciowa

1. Dotyczy to wyłącznie połączeń uplink przełącznika sieciowego i połączeń uplink serwera.

Rozwiązywanie problemów –

Przeprowadzanie operacji odzyskiwania systemu

Jeśli wystąpi całkowita awaria systemu, do odtworzenia systemu Windows® należy użyć obrazu odzyskiwania. W celu pobrania zestawu AXIS Network Video Recorder Recovery Kit należy skontaktować się ze wsparciem technicznym Axis i podać numer seryjny urządzenia.

Uwaga

Zestaw AXIS Network Video Recorder Recovery Kit jest dostępny w dwóch wersjach:

- **sb11** – dla urządzeń, które nadal korzystają z certyfikatu 2011.
- **sb23** – dla urządzeń, które przeszły na certyfikat 2023.

Przed pobraniem zestawu sprawdź status certyfikatu i wybierz właściwą wersję. Jeżeli wybierzesz niewłaściwą wersję, instalacja nie zakończy się uruchomieniem i konieczne będzie rozpoczęcie procedury od nowa przy użyciu prawidłowego obrazu. Nie spowoduje to uszkodzenia urządzenia.

Jeżeli w urządzeniu zainstalowano już certyfikat 2023, wersji sb11 nadal można bezpiecznie używać, o ile certyfikat 2011 nie został unieważniony ręcznie. Po jego unieważnieniu działać będzie wyłącznie wersja sb23.

Aby ponownie utworzyć system:

1. Pobierz zestaw AXIS Network Video Recorder Recovery Kit i narzędzie AXIS Network Video Recorder Recovery: ISO to USB Tool.
2. Włóż dysk USB do komputera.
 - Użyj dysku USB o pojemności minimum 16 GB.
 - Nastąpi sformatowanie dysku USB i usunięcie wszystkich zapisanych na nim danych.
3. Uruchom narzędzie AXIS Network Video Recorder Recovery: ISO to USB Tool i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
Zapisywanie danych na dysku USB trwa 10–15 minut. Nie wyjmuj napędu USB, aż proces zostanie zakończony.
4. Po zakończeniu pracy przez narzędzie AXIS Network Video Recorder Recovery: ISO to USB Tool podłącz dysk USB do urządzenia.
5. Uruchom urządzenie.
6. Po wyświetleniu ekranu powitalnego Axis naciśnij klawisz F12.
7. Kliknij **UEFI: USB Drive (UEFI: dysk USB)**.
8. Przejdź do dysku USB i naciśnij klawisz enter. System zostanie uruchomiony w zestawie AXIS Network Video Recorder Recovery Kit.
9. Kliknij **Reinstall Operating System** (Zainstaluj ponownie system operacyjny).
Odzyskiwanie trwa 10–15 minut. Szczegółowe instrukcje znajdziesz w pliku do pobrania do zestawu do odzyskiwania danych.

Rozwiązywanie problemów z aplikacją AXIS Camera Station

Aby uzyskać informacje dotyczące sposobu rozwiązywania problemów z aplikacją AXIS Camera Station, przejdź do *Instrukcji obsługi AXIS Camera Station*.

Potrzebujesz więcej pomocy?

Przydatne łącza

- *Instrukcja obsługi użytkownika AXIS Camera Station*
- *Zaloguj się do AXIS Secure Remote Access*
- *Co ma znajdować się na białej liście oprogramowania antywirusowego po zainstalowaniu AXIS Camera Station*

Kontakt z pomocą techniczną

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

T10181903_pl

2026-07 (M7.2)

© 2022 – 2026 Axis Communications AB