

AXIS Camera Station S2212 Mk II Appliance

Spis treści

Od czego zacząć	4
Instalacja urządzenia.....	5
Przykłady konfiguracji.....	5
Konfiguracja w niezależnej sieci dozorów	5
Konfiguracja w istniejącej sieci	6
Podłączanie przełącznika bezpośrednio do sieci firmowej.....	7
Konfiguracja urządzenia	9
Wstępna konfiguracja rejestratora Axis.....	9
Łączenie z serwerem.....	9
Łączenie z serwerem zdalnym	10
Zaloguj się do AXIS Secure Remote Access	10
Konfigurowanie oprogramowania AXIS Camera Station Pro	11
Uruchom system VMS	11
Dodawanie urządzeń.....	11
Konfiguracja metody zapisu.....	12
Oglądaj materiał wideo na żywo.....	12
Wyświetl nagrania.....	12
Dodawanie zakładki	12
Eksportuj nagrania.....	12
Odtwarzanie i weryfikacja zapisów w AXIS File Player.....	12
Network configuration (Konfiguracja sieci).....	13
Konfiguracja portu serwera.....	13
Kwestie dotyczące bezpieczeństwa.....	13
Licencja na system online.....	13
Licencja na system w trybie offline.....	14
Zarządzanie lokalnymi kontami użytkowników systemu Windows®	15
Tworzenie konta użytkownika	15
Utwórz konto administratora.....	15
Tworzenie lokalnej grupy użytkowników	15
Usuwanie konta użytkownika	15
Zmianie hasła do konta użytkownika.....	15
Tworzenie dysku resetowania hasła dla konta użytkownika	16
Zarządzanie kontami użytkowników w oprogramowaniu AXIS Camera Station Pro.....	17
Uprawnienia użytkownika	17
Dodawanie użytkowników lub grup.....	17
Uprawnienia użytkownika/grupy.....	18
Zarządzanie urządzeniem.....	21
Aktualizacja certyfikatów bezpiecznego uruchamiania	21
Sprawdzenie stanu certyfikatu	21
Zalecane działania	22
Aktualizacja certyfikatu poprzez BIOS.....	22
Aktualizacja certyfikatu za pomocą usługi Windows Update.....	22
Sprawdzanie bieżącej wersji systemu BIOS.....	23
Aktualizacja BIOS-u.....	23
Aktualizacja systemu Windows®	23
Konfigurowanie ustawień funkcji Windows® Update.....	23
Dodawanie pamięci masowej.....	24
Zdejmowanie ramki	24
Instalowanie dysku twardego.....	24
Dodawanie nowej pamięci masowej nagrań.....	25
Zarządzanie wbudowanym przełącznikiem.....	26
Informacje o wbudowanym przełączniku	26

Logowanie do strony zarządzania przełącznikiem.....	26
Uruchomiona konfiguracja	26
Informacje ogólne	26
Zarządzanie energią	27
Przydziel moc.....	27
Włączanie i wyłączanie zasilania PoE.....	29
Przegląd sieci.....	29
Blokowanie i odblokowywanie portów	30
Ustawienia	30
Konfiguracja ustawień sieciowych	30
Konfigurowanie daty i godziny.....	31
Konfigurowanie serwera DHCP.....	31
Konfiguracja SNMP.....	31
Konserwacja	31
Aktualizowanie oprogramowania sprzętowego	31
Uruchom ponownie przełącznik.....	32
Tworzenie kopii zapasowej ustawień przełącznika	32
Przywracanie ustawień przełącznika	32
Zarządzaj certyfikatami.....	32
Zmień hasło	32
Konfigurowanie ustawień sieci WWW.....	33
Przywróć domyślne ustawienia fabryczne.....	33
Dzienniki	33
Tworzenie raportów przełącznika.....	33
Specyfikacje	34
Przegląd produktów.....	34
Przód i tył.....	34
Wskaźniki LED.....	34
Rozwiązywanie problemów –	36
Resetowanie serwera.....	36
Przeprowadzanie operacji odzyskiwania systemu	36
.....	36
Rozwiązywanie problemów z oprogramowaniem AXIS Camera Station Pro.....	37
Potrzebujesz więcej pomocy?	38
Przydatne łącza.....	38
Kontakt z pomocą techniczną.....	38

Od czego zacząć

Standardowo konfiguracja serwera rejestrującego AXIS Camera Station Pro 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. P. sekcja *Wstępna konfiguracja rejestratora Axis, on page 9.*
4. Skonfiguruj system Windows®. Zalecamy następujące czynności:
 - Zaktualizuj system Windows do najnowszej wersji. Patrz *Aktualizacja systemu Windows®, on page 23.*
 - Utwórz standardowe konto użytkownika. Patrz *Tworzenie konta użytkownika, on page 15.*
5. Zaktualizuj oprogramowanie AXIS Camera Station Pro do najnowszej wersji.
 - Jeżeli system jest w trybie online: otwórz aplikację AXIS Recorder Toolbox i kliknij **Update AXIS Camera Station Pro** (Aktualizuj program AXIS Camera Station Pro).
 - Jeśli system jest w trybie offline: przejdź na stronę *axis.com* i pobierz najnowszą wersję.
6. Uruchom klienta AXIS Camera Station Pro.
7. *Łączenie z serwerem AXIS Camera Station Pro.*
8. *Konfigurowanie oprogramowania AXIS Camera Station Pro, on page 11.*

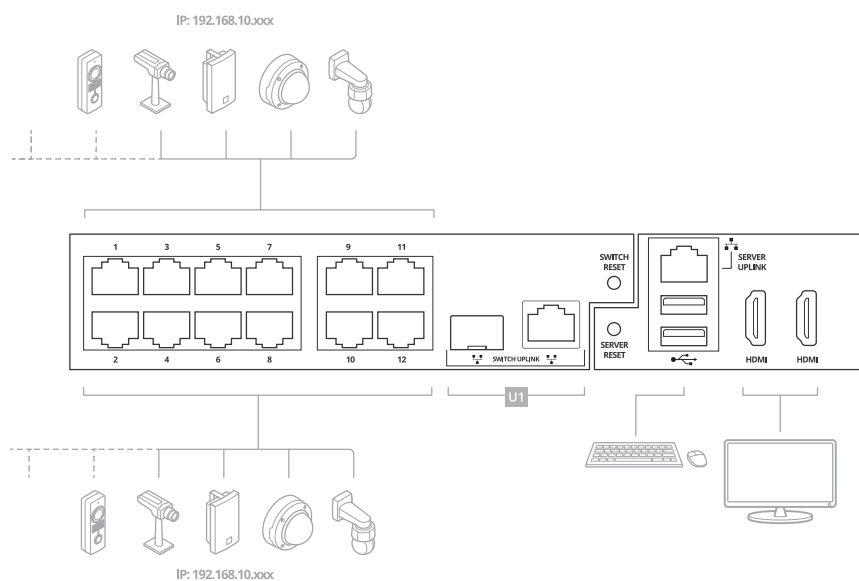
Instalacja urządzenia

Aby uzyskać instrukcje dotyczące sposobu instalowania produktu, zapoznaj się z instrukcją instalacji zawartą w pudełku lub dostępną na stronie wsparcia produktu pod adresem axis.com.

Przykłady konfiguracji

Konfiguracja w niezależnej sieci dozoru

Można utworzyć niezależną sieć dozoru, która nie ma połączenia z inną siecią zewnętrzną. Ta konfiguracja polega na prostej instalacji typu plug and play. Domyślnie włączony jest serwer DHCP wbudowanego przełącznika. Gdy tylko kamery zostaną podłączone do portów PoE, włączą się, uzyskają adres IP i będą dostępne za pośrednictwem oprogramowania AXIS Camera Station Pro.



Poziom trudności	Podstawowe
Korzyści	Odrębna sieć dozoru bez połączenia z inną siecią zewnętrzną Instalacja typu plug and play
Ograniczenia	Przepustowość Budżet PoE Brak dostępu zdalnego
Potrzebne czynności	Zmiana domyślnego hasła wbudowanego przełącznika Zarejestrowanie licencji oprogramowania AXIS Camera Station Pro

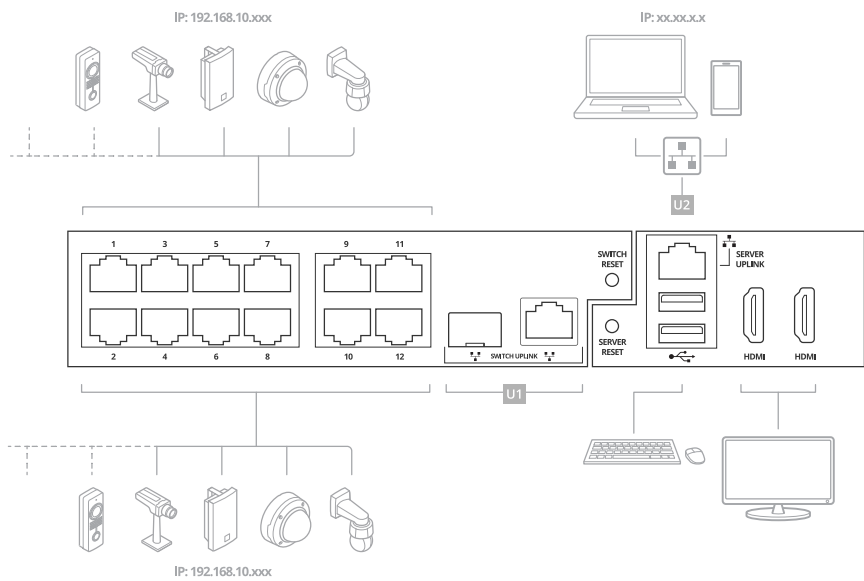
Używane złącza	Porty PoE Ethernet Porty USB 2.0 (dla klawiatury i myszy) Złącze Displayport™ lub HDMI
NIEużywane złącza	Port uplink przełącznika Port uplink serwera Port USB 3.2 (z przodu) Uniwersalne gniazdo audio (z przodu)

Konfiguracja w istniejącej sieci

Sieć dozoru można utworzyć w ramach istniejącej sieci. Oznacza to, że sieć dozoru jest oddzielona od istniejącej sieci.

Uwaga

W przypadku korzystania z dodatkowego rejestratora, na przykład AXIS S30 Recorder, urządzenie nie kieruje danych z sieci dozoru do sieci serwera na potrzeby nagrywania. Należy dopilnować, aby rejestratory AXIS S30 Recorder zostały podłączone do tej samej sieci co kamery.

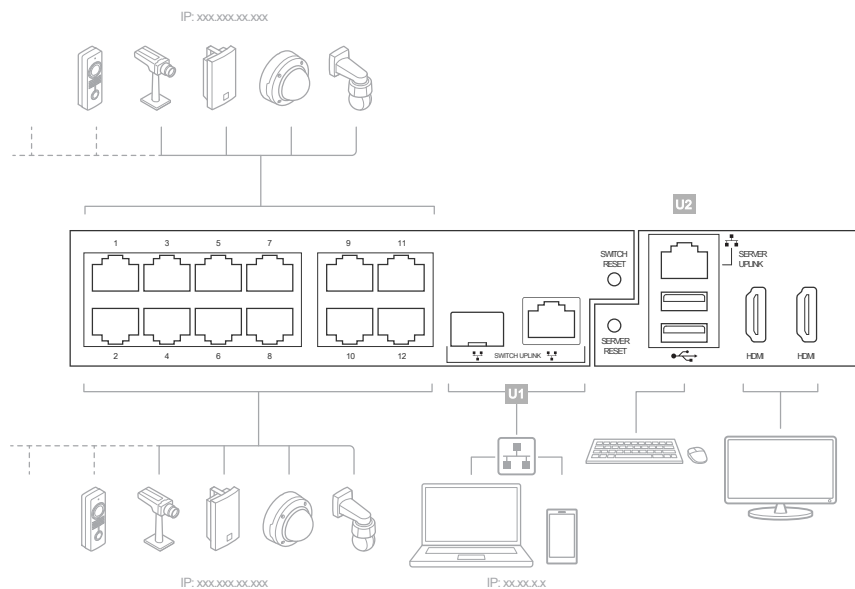


Poziom trudności	Zaawansowane
Korzyści	Możliwość użycia klienta AXIS Camera Station Pro do połączenia się z urządzeniami serii S22 przez sieć. Separacja sieciowa
Ograniczenia	Może być wymagane przestrzeganie firmowych zasad dotyczących sieci
Potrzebne czynności	Zmiana domyślnego hasła wbudowanego przełącznika Zarejestrowanie licencji oprogramowania AXIS Camera Station Pro

Używane złącza	Porty PoE Ethernet Port Ethernet – łączy uplink serwera na potrzeby połączenia z siecią (Opcjonalnie) Porty USB 2.0 (dla klawiatury i myszy) (Opcjonalnie) Złącze Displayport™ lub HDMI
NIEużywane złącza	Port uplink przełącznika Port USB 3.2 (z przodu) Uniwersalne gniazdo audio (z przodu)

Podłączanie przełącznika bezpośrednio do sieci firmowej

W tej konfiguracji system jest zintegrowany bezpośrednio z istniejącą siecią firmową, co umożliwia dostęp do kamer i ich monitorowanie z dowolnego miejsca w sieci.



Poziom trudności	Zaawansowane
Korzyści	Kamery są dostępne z sieci firmowej i mogą być monitorowane za pomocą serwera SNMP.
Ograniczenia	Może być wymagane przestrzeganie firmowych zasad dotyczących sieci
Potrzebne czynności	Wyłączenie protokołu DHCP w przełączniku Zmiana adresu IP przełącznika na statyczny z poziomu sieci firmowej Ustawienie wewnętrznej karty sieciowej komputera na DHCP lub statyczny adres IP w sieci firmowej Zmiana domyślnego hasła przełącznika Skonfigurowanie i zarejestrowanie oprogramowania AXIS Camera Station Pro

Używane złącza	Porty PoE Ethernet Port uplink przełącznika (U1) (Opcjonalnie) Porty USB 2.0 (dla klawiatury i myszy) (Opcjonalnie) Złącze Displayport™ lub HDMI
NIEużywane złącza	Port uplink komputera (U2) Port USB 3.2 (z przodu) Uniwersalne gniazdo audio (z przodu)

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.

Uwaga

Te ustawienia dotyczą serwera. Aby zmienić ustawienia przełącznika, przejdź do strony zarządzania przełącznikiem. Patrz *Ustawienia, on page 30*.

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.

Łączenie z serwerem

Klient AXIS Camera Station S2212 Mk II Appliance umożliwia połączenie się z jednym lub kilkoma serwerami 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 10*.

Uwaga

- Przy pierwszym połączeniu z serwerem klient sprawdza identyfikator certyfikatu serwera. Aby upewnić się, że łączysz się z właściwym serwerem, porównaj identyfikator certyfikatu z identyfikatorem wyświetlanym w AXIS Camera Station S2212 Mk II Appliance 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 dla wszystkich połączonych serwerów, kliknij Delete saved passwords (Usuń zapisane hasła) .
Change client proxy settings (Zmień ustawienia klienta proxy)	Jeżeli nie możesz połączyć się z serwerem, konieczna może być aktualizacja ustawień serwera proxy w kliencie. Kliknij Change client proxy settings (Zmień ustawienia 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 S2212 Mk II 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 S2212 Mk II Appliance**, należy skonfigurować ustawienia serwera proxy w systemie Windows na serwerze **AXIS Camera Station S2212 Mk II 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)**.

Konfigurowanie oprogramowania AXIS Camera Station Pro

Zanim zaczniesz:

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

Po wykonaniu niezbędnych czynności konfiguracyjnych można rozpocząć korzystanie z oprogramowania AXIS Camera Station Pro:

1. *Uruchom system VMS*
2. *Dodawanie urządzeń*
3. *Konfiguracja metody zapisu, on page 12*
4. *Oglądaj materiał wideo na żywo, on page 12*
5. *Wyświetl nagrania, on page 12*
6. *Dodawanie zakładki, on page 12*
7. *Eksportuj nagrania, on page 12*
8. *Odtwarzanie i weryfikacja zapisów w AXIS File Player, on page 12*

Uruchom system VMS

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

Połączenie z wieloma serwerami AXIS Camera Station Pro można nawiązać na kilka sposobów.

Dodawanie urządzeń

Przy pierwszym uruchomieniu AXIS Camera Station S2212 Mk II Appliance otwiera się strona **Add devices** (Dodaj urządzenia), która przeszukuje sieć pod kątem urządzeń do dodania.

1. Wybierz z listy urządzenia, które chcesz dodać. Jeśli nie możesz znaleźć urządzenia, kliknij **Manual search (Ręczne wyszukiwanie)** lub wpisać tekst, aby zawęzić wyniki.
2. Kliknij **Dodaj**.
3. Kliknij **Close (Zamknij)**, aby pominąć konfigurację i kontynuować później. Aby kontynuować konfigurację teraz:
 - 3.1. Wybierz **Quick configuration (Szybka konfiguracja)** lub **Site Designer configuration (Konfiguracja Site Designer)**. Więcej informacji: .
 - 3.2. Wybierz **Add image overlay for date, time, and text (Dodaj nakładkę obrazu z datą, godziną i tekstem)**, aby dodać nakładki do wszystkich kamer Axis, które jeszcze ich nie mają.
 - 3.3. Kliknij **Next (Dalej)**.
 - 3.4. Wybierz preferowane ustawienie **Recording method (Metoda nagrywania)**.
 - 3.5. Kliknij **Next (Dalej)**.
 - 3.6. Wybierz opcję **Retention time (Czas przechowywania)** oraz **Recording storage (Lokalizacja przechowywania nagrań)**, a następnie kliknij **Finish (Zakończ)**, aby zastosować konfigurację.

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)

Zanim skorzystasz z AXIS Camera Station S2212 Mk II Appliance, skonfiguruj ustawienia proxy lub zapory, jeżeli klient, serwer i połączone urządzenia sieciowe znajdują się w różnych sieciach.

Ustawienia proxy klienta

Jeżeli pomiędzy klientem a serwerem znajduje się serwer proxy, skonfiguruj ustawienia serwera proxy w systemie Windows na komputerze klienckim. W celu uzyskania dalszych informacji skontaktuj się ze wsparciem Axis.

Ustawienia proxy na serwerze

Jeśli serwer proxy znajduje się między urządzeniem sieciowym a serwerem, należy skonfigurować ustawienia serwera proxy w systemie Windows na serwerze. W celu uzyskania dalszych informacji skontaktuj się ze wsparciem Axis.

NAT i Zapora sieciowa

Jeżeli klient i serwer są oddzielone przez NAT lub zaporę sieciową, skonfiguruj je tak, aby ruch był przepuszczany przez port HTTP, port TCP i port strumieniowania, które określono w usłudze AXIS Camera Station S2212 Mk II Appliance Service Control. Po pomoc zwróć się do administratora sieci.

Konfiguracja portu serwera

Serwer AXIS Camera Station S2212 Mk II Appliance używa portów 55752 (HTTP), 55754 (TCP), 55756 (komunikacja mobilna) oraz 55757 (strumieniowanie w sieci komórkowej) do komunikacji pomiędzy 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 S2212 Mk II Appliance, kamery, kodery wizyjne i urządzenia pomocnicze w zabezpieczonej sieci odseparowanej od sieci biurowej. Klienta AXIS Camera Station S2212 Mk II 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

Aby korzystać z automatycznego licencjonowania, zarejestruj system i połącz go z organizacją.

1. Przejdź do menu **Configuration (Konfiguracja) > Licenses (Licencje) > Management (Zarządzanie)**.
2. Upewnij się, że została włączona funkcja **Automatic licensing (Automatyczne licencjonowanie)**.
3. Kliknij polecenie **Register... (Zarejestruj...)**.

4. Zaloguj się za pomocą konta My Axis i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
5. Kliknij **Go to AXIS License Manager** (Przejdź do aplikacji AXIS License Manager), aby zarządzać licencjami. Aby dowiedzieć się więcej, przeczytaj *Podręcznik użytkownika funkcji My Systems na stronie help.axis.com*.

Licencja na system w trybie offline

Aby ręcznie licencjonować system:

1. Przejdź do menu **Configuration (Konfiguracja) > Licenses (Licencje) > Management (Zarządzanie)**.
2. Wyłącz **Automatic licensing (Automatyczne licencjonowanie)**.
3. Kliknij polecenie **Export system file...** (Eksportuj plik systemowy...) i zapisz ten plik na komputerze.

Uwaga

Korzystanie z aplikacji AXIS License Manager wymaga połączenia z Internetem. Jeśli komputer kliencki nie ma połączenia z Internetem, skopiuj plik systemowy na komputer z dostępem do Internetu.

4. Otwórz aplikację *AXIS License Manager*.
5. W aplikacji AXIS License Manager:
 - 5.1. Wybierz lub utwórz odpowiednią organizację. Aby dowiedzieć się więcej, przeczytaj *Podręcznik użytkownika funkcji My Systems na stronie help.axis.com*.
 - 5.2. Przejdź do menu **System setup (Konfiguracja systemu)**.
 - 5.3. Kliknij polecenie **Upload system file (Prześlij plik systemowy)**.
 - 5.4. Kliknij polecenie **Upload system file (Prześlij plik systemowy)** i wybierz plik systemowy.
 - 5.5. Kliknij polecenie **Upload system file (Prześlij plik systemowy)**.
 - 5.6. Kliknij **Download license file (Pobierz plik licencji)**.
6. Wróć do klienta AXIS Camera Station S2212 Mk II Appliance.
7. Kliknij **Import license file...** (Importuj plik licencji) i wybierz swój plik licencji.
8. Kliknij **Go to AXIS License Manager** (Przejdź do aplikacji AXIS License Manager), aby zarządzać licencjami.

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 obszaru **Settings (Ustawienia) > Accounts (Konta) > Other users (Inni użytkownicy) > Add other user (Dodaj innego użytkownika)** i kliknij **Add account (Dodaj konto)**.
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 oprogramowaniu AXIS Camera Station Pro

Uprawnienia użytkownika

Przejdź do Configuration > Security > User permissions (Konfiguracja > Bezpieczeństwo > Uprawnienia użytkowników), aby wyświetlić użytkowników i grupy w AXIS Camera Station S2212 Mk II Appliance.

Uwaga

Administratorzy komputera, na którym jest uruchomiony serwer AXIS Camera Station S2212 Mk II Appliance, automatycznie otrzymują uprawnienia administratora w AXIS Camera Station S2212 Mk II 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 przydzielaną 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 S2212 Mk II Appliance. Aby dodać użytkownika do AXIS Camera Station S2212 Mk II 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 S2212 Mk II 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 S2212 Mk II 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)**.

Wejść 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.

Wejść na stronę	Umożliwia dostęp do widoków w AXIS Camera Station S2212 Mk II Appliance.
Edytuj	Umożliwia edycję widoków w AXIS Camera Station S2212 Mk II Appliance.

We/wy

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

Wejść 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**.

Dodawanie pamięci masowej

Zapotrzebowanie na pamięć masową może być różne. Określenie czasu przechowywania zapisanych danych lub potrzeba przechowywania nagrań o wysokiej rozdzielczości często powoduje konieczność zainstalowania dodatkowej pamięci masowej. W tej sekcji wyjaśniono, jak zainstalować dodatkowy dysk twardy w produkcie z serii AXIS S22.

Uwaga

Postępuj zgodnie z poniższymi instrukcjami, aby dodać pamięć masową do odpowiednich produktów AXIS S22. Instrukcje te są udostępniane w aktualnym stanie, a Axis Communications AB nie ponosi odpowiedzialności za utratę danych lub błędną konfigurację wynikającą z wykonania tych czynności. Należy podjąć standardowe środki ostrożności w celu wykonania kopii zapasowej krytycznych danych. Poniższa procedura powiększania pamięci masowej nie podlega wsparciu technicznemu Axis.

Uwaga

Aby uniknąć wyładowań elektrostatycznych w trakcie pracy przy wewnętrznych komponentach systemu, najlepiej korzystać z maty antystatycznej i paska antystatycznego.

Gwarancja

Szczegółowe informacje na temat gwarancji są dostępne na stronie: www.axis.com/support/warranty.



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

Zdejmowanie ramki

1. Poluzuj dwie śruby mocujące znajdujące się po obu stronach ramki.
2. Zdejmij ramkę.

Instalowanie dysku twardego

▲ UWAGA

- Należy używać wyłącznie dysków twardych, które zostały przetestowane i zatwierdzone do użytku z serią AXIS S22.
 - Podczas instalowania dysku twardego upewnij się, że kieszeń dysku została wsunięta do końca. Gdy kieszeń dysku zostanie zablokowana, usłyszysz kliknięcie.
 - Przed przystąpieniem do instalacji dysku twardego upewnij się, że przewód zasilania jest odłączony.
1. Zamknij system i upewnij się, że zasilanie jest wyłączone.

2. Odłącz przewód zasilania.
3. Naciśnij przycisk zwalniający z przodu kieszeni dysku twardego i otwórz uchwyt kieszeni dysku.
4. Wyciągnij kieszeń dysku twardego za pomocą uchwytu.
5. Włóż dysk twardy do kieszeni.
6. Przymocuj dysk twardy do kieszeni za pomocą czterech śrub.
7. Włóż kieszeń dysku twardego do gniazda dysku i wsuń ją tak, aby połączyła się z płytą montażową.
8. Zamknij uchwyt kieszeni dysku twardego, aby zablokować dysk twardy w obecnym położeniu.
9. Ponownie załóż przednią ramkę.
10. Uruchom system.

Dodawanie nowej pamięci masowej nagrań

1. Utwórz i sformatuj nową partycję dysku twardego w systemie Windows:
 - 1.1. Kliknij prawym przyciskiem myszy menu **Start** i wybierz **Disk Management (Zarządzanie dyskami)**.
 - 1.2. Kliknij **OK** w przypadku wyświetlenia wyskakującego okienka **Initialize Disk (Inicjowanie dysku)**. W przeciwnym razie kliknij prawym przyciskiem myszy nowy dysk twardy i wybierz **Initialize Disk (Zainicjuj dysk)**.
 - 1.3. Kliknij prawym przyciskiem myszy nieprzydzielony obszar na nowo zainicjowanym dysku i wybierz **New Simple Volume (Nowy wolumin prosty)**.
 - 1.4. Postępuj zgodnie z instrukcjami kreatora, aby ustawić rozmiar woluminu, przypisać literę dysku i sformatować partycję.
 - 1.5. Ukończ kreatora, aby utworzyć nowy wolumin prosty.
2. Dodaj nową pamięć masową nagrań w programie AXIS Camera Station Pro:
 - 2.1. Otwórz oprogramowanie AXIS Camera Station Pro.
 - 2.2. Przejdź do **Storage > Management (Pamięć masowa > Zarządzanie)**.
 - 2.3. Kliknij **Dodaj...**
 - 2.4. Wybierz nowo dodany dysk i kliknij **OK**.
 - 2.5. Przejdź do **Storage > Selection (Pamięć masowa > Wybór)**.
 - 2.6. Wybierz urządzenia, z których chcesz przenieść dane nagrań na nowy dysk.
 - 2.7. Z listy rozwijanej **Store to (Zapisz w)** wybierz nowy dysk i kliknij **Apply (Zastosuj)**.

Więcej informacji o zarządzaniu pamięcią masową znajduje się w *instrukcji obsługi programu AXIS Camera Station Pro*.

Zarządzanie wbudowanym przełącznikiem

Informacje o wbudowanym przełączniku

Urządzenia z serii AXIS Camera Station S22 Mk II Appliance Series są wyposażone w zintegrowany przełącznik Power over Ethernet (PoE). Ten wbudowany przełącznik można konfigurować i można nim zarządzać.

Przełącznik ma na celu separację ruchu w sieci, tak aby kamery systemu bezpieczeństwa i związane z nimi ruch zarządzany przez przełącznik (PoE i porty uplink przełącznika) nie były udostępniane innym sieciom.

Zarządzanie energią w przełączniku odbywa się zgodnie z następującymi regułami:

- Każdy port może rezerwować moc zgodnie z klasą PoE podłączonego zasilanego urządzenia. Moc do portu można także przydzielić ręcznie.
- Jeśli rzeczywisty pobór mocy na danym porcie przekroczy zarezerwowaną dla niego moc, port zostanie wyłączony.
- Gdy rzeczywisty pobór mocy przez wszystkie porty przekroczy całkowitą ilość mocy, jaką może dostarczyć zasilacz, porty zostaną wyłączone. Porty są wówczas wyłączane zgodnie ze swoim priorytetem, przy czym niższy numer portu oznacza wyższy priorytet.

Logowanie do strony zarządzania przełącznikiem

1. Przejdź do paska menu.
 - W przeglądarce internetowej wprowadź adres IP przełącznika. Wartość domyślna: 192.168.10.1
 - Z poziomu narzędzia AXIS Recorder Toolbox przejdź do obszaru **Switch (Przełącznik) > Open the switch configuration (Otwórz konfigurację przełącznika)**.
2. Zaloguj się za pomocą swojej nazwy użytkownika i hasła.
 - Nazwa użytkownika to `admin`
 - Twoje hasło znajduje się na naklejce umieszczonej na jednostce, za przednią pokrywą i znajdującej się w pudełku w formie samoprzylepnej naklejki.

Wyloguj się z poziomu paska menu, aby opuścić stronę zarządzania przełącznikiem.

Uruchomiona konfiguracja

Uruchomiona konfiguracja to zestaw ustawień, które obecnie są aktywne i działają na urządzeniu sieciowym. Odzwierciedla ona obecny stan urządzenia i sposób jego funkcjonowania w czasie rzeczywistym. Zmiany te nie są jednak zapisywane w przypadku ponownego uruchomienia urządzenia.

Natomiast konfiguracja startowa to zestaw ustawień, które są zapisane w pamięci trwałej urządzenia. Konfiguracja ta jest ładowana i stosowana podczas uruchamiania lub ponownego uruchamiania urządzenia.

Po wprowadzeniu zmian w interfejsie WWW i kliknięciu przycisku **Save (Zapisz)** zmiany te są stosowane do uruchomionej konfiguracji.

Aby zapisać ustawienia w konfiguracji startowej, należy użyć ikony Save (Zapisz) w prawym górnym rogu interfejsu WWW.

Jeśli w uruchomionej konfiguracji znajdują się niezapisane zmiany, ikona miga na żółto.

Informacje ogólne

Na pasku menu kliknij **Overview (Przegląd)**.

Informacje ogólne

Kategoria	Element	Opis
Podsumowanie portów	Aktywne porty	Liczba używanych portów.

	Porty korzystające z PoE	Liczba używanych portów obsługujących PoE.
	Zablokowane porty	Liczba zablokowanych portów.
Pobór prądu	Bieżące wykorzystanie PoE	Moc PoE w watach pobierana przez urządzenia oraz procent wykorzystywanej mocy PoE w stosunku do całkowitej przydzielonej mocy PoE.
	Żądana moc	Całkowita moc w watach i procent przydzielony urządzeniom.
Status portu	Aktywne	Port jest w użyciu.
	Nieaktywne	Port jest gotowy do użycia.
	Zablokowane	Port jest zablokowany.

Uwaga

Można kliknąć port, aby wyświetlić więcej informacji na jego temat.

Zarządzanie energią

Na pasku menu kliknij **Power management (Zarządzanie zasilaniem)**.

Lista portów

Element	Opis
Port	Numer portu, do którego jest podłączone urządzenie.
PoE	Status PoE. Można kliknąć ikonę, aby włączyć lub wyłączyć PoE na danym porcie.
Klasa PoE	Klasa PoE podłączonego urządzenia.
Priorytet	Priorytet przydzielania mocy podłączonemu urządzeniu. Domyślnie priorytetem jest numer portu.
Pobór mocy (W)	Moc w watach pobierana przez urządzenie podłączone do portu.
Żądana moc (W)	Moc w watach żądana przez urządzenie podłączone do portu.
Przydzielona moc (W)	Ręcznie dostosuj moc przydzieloną do portu. Pozycja dostępna tylko w przypadku wybrania metody przydzielania mocy Manual (Ręcznie) .

Przydziel moc

Moc PoE można przydzielić podłączonym urządzeniom w następujący sposób:

- **Klasa PoE:** Przełącznik przydziela zasilanie PoE w oparciu o klasę PoE połączonego urządzenia.
- **Manual (Ręcznie):** Można ręcznie dostosować moc PoE przydzieloną do podłączonego urządzenia.
- **LLDP-MED:** Przełącznik komunikuje się z podłączonym urządzeniem i dynamicznie przydziela moc PoE w zależności od potrzeb.

Uwaga

Metoda przydzielania mocy LLDP-MED działa tylko w przypadku kamer z systemem AXIS OS 9.20 lub nowszym.

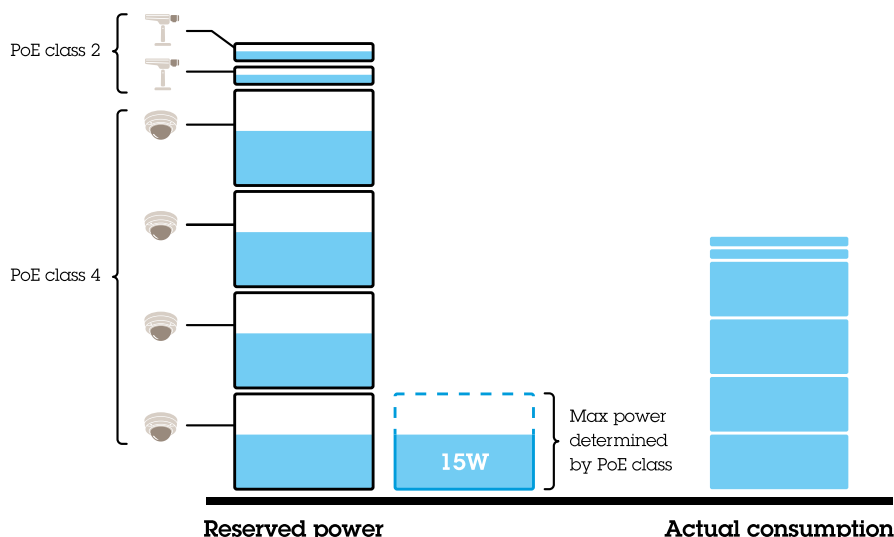
Aby zmienić metodę przydziału mocy:

1. Na stronie zarządzania energią przełącznika przejdź do pozycji **Power management (Zarządzanie energią)**.
2. Wybierz opcję **PoE class (Klasa PoE)**, **Manual (Ręcznie)** lub **LLDP-MED** w obszarze **Allocate power (Przydziel moc)**.
3. W przypadku wybrania opcji **Manual (Ręcznie)** można zmienić moc przydzieloną podłączonemu urządzeniu w kolumnie **Power allocated (Przydzielona moc)**.
4. Jeśli chcesz zmienić priorytet podłączonego urządzenia, wybierz żadaną wartość jego priorytetu. Priorytet innych urządzeń zmieni się w sposób automatyczny.

Przykład:

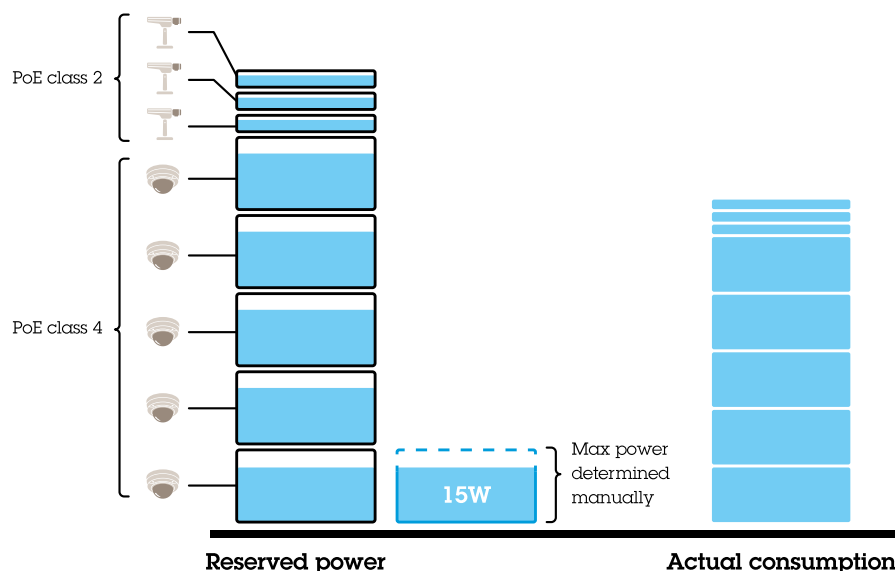
W tym przykładzie całkowity budżet mocy przełącznika wynosi 135 W. Urządzenie PoE klasy 4 żąda 30 W mocy, ale zużywa tylko 15 W. Urządzenie PoE klasy 2 żąda 7 W mocy, ale zużywa tylko 5 W.

Przydzielanie mocy według klasy PoE



Moc żądana przez każde urządzenie jest określona przez klasę PoE. Przełącznik może zasilać 4 urządzenia PoE klasy 4 i 2 urządzenia PoE klasy 2. Całkowita żądana moc wynosi $(4 \times 30) + (2 \times 7) = 134$ W. Rzeczywiście zużywana moc wynosi $(4 \times 15) + (2 \times 5) = 70$ W. W ten sposób wszystkie podłączone urządzenia mają zagwarantowaną wystarczającą moc, a priorytet jest mniej ważny.

Ręczne przydzielanie mocy



W przypadku urządzeń PoE klasy 4 żądana moc jest ustawiana ręcznie na 20 W. Przełącznik może zasilać 5 urządzeń PoE klasy 4 i 3 urządzenia PoE klasy 2. Całkowita żądana moc wynosi $(5 \times 20) + (3 \times 7) = 121$ W. Rzeczywiście zużywana moc wynosi $(5 \times 15) + (3 \times 5) = 90$ W. W ten sposób wszystkie podłączone urządzenia mają zagwarantowaną wystarczającą moc, a priorytet jest mniej ważny.

Włączanie i wyłączanie zasilania PoE

Włączanie zasilania PoE na porcie

1. Na pasku menu kliknij **Overview (Przegląd)**.
2. W kolumnie PoE kliknij , aby włączyć zasilanie PoE na określonym porcie.

Wyłączanie zasilania PoE na porcie

1. Na pasku menu kliknij **Overview (Przegląd)**.
2. W kolumnie PoE kliknij , aby wyłączyć zasilanie PoE na określonym porcie.

Włączanie i wyłączanie zasilania PoE na wszystkich portach

1. Na pasku menu kliknij **Power management (Zarządzanie zasilaniem)**.
2. Aby wyłączyć zasilanie PoE na wszystkich portach, przejdź do menu rozwijanego PoE ports state (Stan portów PoE) i wybierz Turn off all (Wyłącz wszystkie).
3. Aby włączyć zasilanie PoE na wszystkich portach, przejdź do menu rozwijanego PoE ports state (Stan portów PoE) i wybierz Turn on all (Włącz wszystkie).

Przegląd sieci

Przegląd sieci zawiera szczegółowe informacje o stanie ruchu sieciowego na każdym porcie.

Porty PoE

Element	Opis
Port	Numer portu, do którego jest podłączone urządzenie.
Urządzenie	Nazwa urządzenia podłączonego do portu.
IP address (Adres IP)	Adres IP urządzenia podłączonego do portu.
Adres MAC	Adres MAC urządzenia podłączonego do portu.

Odbiór	Bieżąca szybkość transmisji danych przychodzących na porcie, wyrażona w megabitach na sekundę.
Transmisja	Bieżąca szybkość transmisji danych wychodzących na porcie, wyrażona w megabitach na sekundę.
Pakiety wysłane	Liczba pakietów danych przesłanych przez przełącznik do sieci.
Pakiety odebrane	Liczba pakietów danych odebranych przez przełącznik z sieci.
Pakiety utracone	Liczba i procent pakietów danych, które nie dotarły do miejsca docelowego z powodu problemów z siecią.
Lock (Blokada)	Pokazuje, czy port jest zablokowany. Można kliknąć ikonę, aby zablokować lub odblokować port.

Blokowanie i odblokowywanie portów

Istnieje możliwość zablokowania adresu MAC na porcie, tak aby przepuszczany był tylko ruch pochodzący z tego adresu MAC. Zwiększa to bezpieczeństwo i uniemożliwia nieautoryzowanym użytkownikom np. podłączenie laptopa lub innego urządzenia do sieci bezpieczeństwa.

Blokowanie adresu MAC na porcie

1. Na pasku menu kliknij **Network overview (Przegląd sieci)**.
2. W kolumnie **Lock (Blokada)** kliknij , aby zablokować określony port.

Odblokowywanie adresu MAC z portu

1. Na pasku menu kliknij **Network overview (Przegląd sieci)**.
2. W kolumnie **Lock (Blokada)** kliknij , aby odblokować określony port.

Blokowanie lub odblokowywanie wszystkich portów

1. Na pasku menu kliknij **Network overview (Przegląd sieci)**.
2. Aby zablokować wszystkie porty, przejdź do menu rozwijanego **Lock ports (Zablokuj porty)** i wybierz **Lock all (Zablokuj wszystkie)**.
3. Aby odblokować wszystkie porty, przejdź do menu rozwijanego **Lock ports (Zablokuj porty)** i wybierz **Unlock all (Odblokuj wszystkie)**.

Ustawienia

Konfiguracja ustawień sieciowych

Adres IP przełącznika można zmienić. Jednak w większości instalacji z kamerami zalecamy korzystanie z ustawień domyślnych. Wynika to z faktu, że sieć dozoru zwykle jest odizolowana od innych sieci, na przykład firmowej sieci lokalnej. W takim przypadku sieć dozoru służy wyłącznie do zarządzania urządzeniami systemu dozoru i gromadzenia danych na temat dozoru z oprogramowania do zarządzania materiałem wizyjnym zainstalowanego na serwerze.

1. Na pasku menu przejdź do pozycji **Settings (Ustawienia) > Network settings (Ustawienia sieci)**.
2. Wprowadź typ połączenia, adres IP, maskę podsieci, bramę, podstawowy serwer DNS, dodatkowy serwer DNS i nazwę hosta.

Uwaga

Domyślne ustawienia fabryczne to statyczne połączenie IP z adresem 192.168.10.1 i maska podsieci z adresem 255.255.255.0.

3. Kliknij przycisk **Zapisz**.

Konfigurowanie daty i godziny

1. Na pasku menu przejdź do pozycji **Settings (Ustawienia) > Date and time (Data i godzina)**.
2. Wybierz kraj i strefę czasową.
3. Aby ustawić godzinę ręcznie, wybierz **Manual (Ręcznie)** i ręcznie ustaw godzinę.
4. Aby skonfigurować serwer NTP, wybierz opcję **NTP server (Serwer NTP)** i wprowadź adres serwera NTP.

Uwaga

Protokół NTP działa tylko wtedy, gdy przełącznik jest podłączony do sieci i ma skonfigurowany dostęp do Internetu.

5. Kliknij przycisk **Zapisz**.

Konfigurowanie serwera DHCP

Przełącznik można skonfigurować tak, aby korzystał z wewnętrznego serwera DHCP w celu przydzielania adresów IP podłączonym urządzeniom. Jeśli jest używane połączenie uplink przełącznika, które umożliwia urządzeniom dostęp do aplikacji zewnętrznych lub aplikacjom zewnętrznym dostęp do urządzeń, należy określić adresy bramy i serwera DNS.

1. Na pasku menu przejdź do pozycji **Settings (Ustawienia) > DHCP server (Serwer DHCP)**.
2. Wybierz **Enable DHCP server (Włącz serwer DHCP)**.
3. Wprowadź początkowy adres IP, końcowy adres IP, maskę podsieci, bramę, podstawowy serwer DNS, dodatkowy serwer DNS, długość dzierżawy i nazwę domeny.
4. Kliknij przycisk **Zapisz**.

Konfiguracja SNMP

1. Na pasku menu przejdź do pozycji **Settings (Ustawienia) > SNMP**.
2. Wprowadź nazwę serwera, kontakt i lokalizację używane na potrzeby połączenia SNMP.
3. Jeśli chcesz używać protokołu SNMPV1 lub SNMPV2c, wybierz **SNMPV1 / SNMPV2c** i wprowadź społeczność odczytu.
4. Jeśli chcesz używać protokołu SNMPV3, wybierz **SNMPV3 (MD5)** oraz wprowadź nazwę użytkownika i hasło.

Uwaga

Obecnie obsługujemy tylko uwierzytelnianie MD5 używane na potrzeby protokołu SNMP.

5. Kliknij przycisk **Zapisz**.

Konserwacja

Aktualizowanie oprogramowania sprzętowego

1. Na pasku menu przejdź do pozycji **Maintenance (Konserwacja) > Update firmware (Zaktualizuj oprogramowanie sprzętowe)**.
2. Przeciągnij i upuść plik oprogramowania sprzętowego lub kliknij **Browse (Przeglądaj)** i przejdź do pliku oprogramowania sprzętowego.
3. Kliknij przycisk **Upload (Prześlij)**.
4. Po zaktualizowaniu oprogramowania sprzętowego uruchom ponownie przełącznik.

Uruchom ponownie przełącznik

Ważne

Podczas ponownego uruchamiania przełącznika wszystkie podłączone urządzenia tymczasowo utracą połączenie z przełącznikiem, w tym z zasilaniem PoE.

1. Na pasku menu przejdź do pozycji **Maintenance (Konserwacja) > Reboot switch (Uruchom ponownie przełącznik)**.
2. Kliknij **Reboot (Uruchom ponownie)** i **Yes (Tak)**.
3. Gdy po kilku minutach przełącznik uruchomi się ponownie, wprowadź nazwę użytkownika i hasło, aby się zalogować.

Tworzenie kopii zapasowej ustawień przełącznika

Uwaga

Plik kopii zapasowej zawiera nazwę użytkownika i hasło.

1. Na pasku menu przejdź do pozycji **Maintenance (Konserwacja) > Backup and restore (Kopia zapasowa i przywracanie)**.
2. Kliknij **Create a backup file (Utwórz plik kopii zapasowej)**. Spowoduje to utworzenie pliku kopii zapasowej w formacie .bin i zapisanie go w folderze **Downloads (Pobrane)**.

Przywracanie ustawień przełącznika

Uwaga

Aby przywrócić ustawienia przełącznika, należy wcześniej utworzyć plik kopii zapasowej.

1. Na pasku menu przejdź do pozycji **Maintenance (Konserwacja) > Backup and restore (Kopia zapasowa i przywracanie)**.
2. Przecignij i upuść plik kopii zapasowej lub kliknij **Browse (Przeglądaj)** i przejdź do pliku kopii zapasowej.
3. Kliknij przycisk **Upload (Prześlij)**.

Przywrócenie przełącznika z pliku kopii zapasowej może potrwać kilka minut. Po przywróceniu ustawień przełącznik zostanie automatycznie uruchomiony ponownie i konieczne będzie ponowne zalogowanie się.

Zarządzaj certyfikatami

1. Na pasku menu przejdź do pozycji **Maintenance (Konserwacja) > Manage certificates (Zarządzaj certyfikatami)**.
2. Kliknij  i przejdź do pliku klucza prywatnego.
3. Kliknij  i przejdź do pliku certyfikatu.
4. Kliknij  i przejdź do pliku pakietu CA.
5. Kliknij przycisk **Zapisz**.
6. Uruchom ponownie przełącznik.

Zmień hasło

Domyślne hasło przełącznika można zmienić na własne.

Ważne

Konieczne wybierz hasło, które będziesz w stanie zapamiętać. Jeśli zapomnisz hasła, zobacz *Przywróć domyślne ustawienia fabryczne, on page 33*, aby przywrócić hasło domyślne.

1. Na pasku menu przejdź do pozycji **Maintenance (Konserwacja) > Change password (Zmień hasło)**.
2. Wprowadź bieżące hasło i nowe hasło zgodnie z wymaganiami.
3. Kliknij przycisk **Zapisz**.

Konfigurowanie ustawień sieci WWW

1. Na pasku menu przejdź do pozycji **Maintenance (Konserwacja) > Web settings (Ustawienia Internetu)**.
2. Wprowadź numer portu.

Uwaga

- Jeśli zdecydujesz się zmienić numer portu, koniecznie zapisz nowy numer. Jeśli zapomnisz nowego numeru portu, zobacz *Przywróć domyślne ustawienia fabryczne, on page 33*, aby przywrócić domyślny numer portu.
- Zalecamy niewyłączanie protokołu HTTPS.

Przywróć domyślne ustawienia fabryczne

Przytrzymaj przycisk resetowania przez pięć sekund, aby przywrócić domyślne ustawienia fabryczne przełącznika.

Przełącznik można również zresetować za pomocą interfejsu WWW:

1. Na pasku menu przejdź do pozycji **Maintenance (Konserwacja) > Reset to factory default settings (Przywróć ustawienia fabryczne)**.
2. Kliknij **Reset (Resetuj)** i **Yes (Tak)**.

Po wykonaniu resetu przełącznik uruchomi się ponownie w sposób automatyczny.

Dzienniki

Na pasku menu kliknij **Logs (Dzienniki)**, aby wyświetlić listę dzienników. Kliknij tytuł kolumny, aby posortować listę w kolejności alfabetycznej.

Element	Opis
Time (Godzina)	Data i godzina wystąpienia zdarzenia z dziennika.
Poziom	Poziom istotności wyświetlany w postaci ikony ostrzeżenia.
Użytkownik	Użytkownik, który zainicjował zdarzenie dziennika.
IP address (Adres IP)	Adres IP użytkownika, który zainicjował zdarzenie dziennika.
Serwis	Usługa, której dotyczy zdarzenie dziennika. Możliwe wartości to desktop (komputer), network (sieć), system, ntpd, storage (pamięć masowa), dhcp itp.
Zdarzenie	Opis zdarzenia z dziennika.

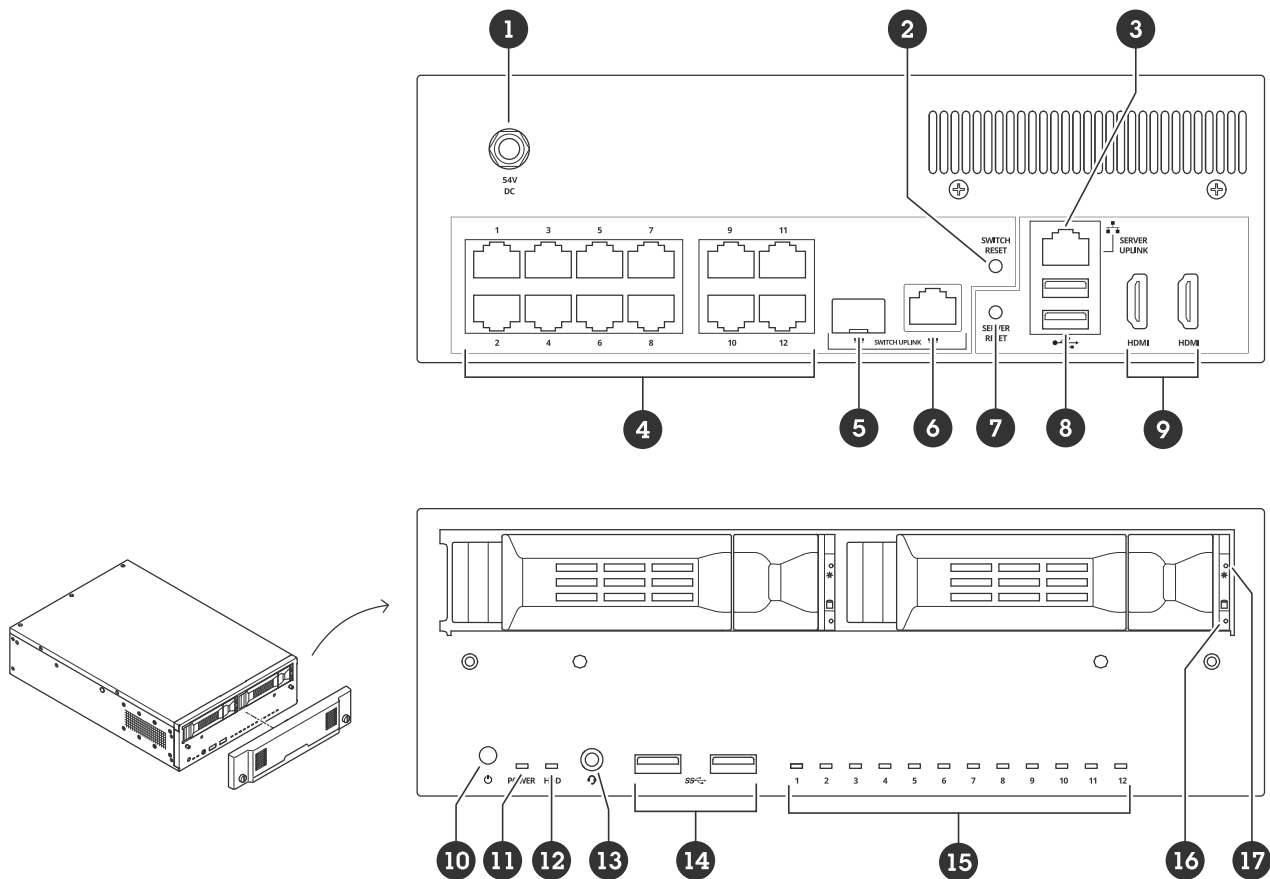
Tworzenie raportów przełącznika

Na stronie dziennika kliknij **Export (Eksportuj)**, aby utworzyć plik tekstowy zawierający informacje o przełączniku, w tym wpisy dziennika ze strony dziennika.

Specyfikacje

Przegląd produktów

Przód i tył



- 1 Złącze zasilania
- 2 Przycisk resetowania przełącznika
- 3 Port 1 GbE Ethernet – złącze uplink serwera
- 4 Porty 1 GbE PoE Ethernet
- 5 Port 1 GbE Ethernet – złącze uplink przełącznika (SFP)
- 6 Port 1 GbE Ethernet – złącze uplink przełącznika (RJ45)
- 7 Przycisk resetowania serwera
- 8 Porty USB 2.0
- 9 Porty HDMI
- 10 Przycisk zasilania
- 11 Wskaźnik LED zasilania
- 12 Wskaźnik LED aktywności dysku twardego
- 13 Uniwersalne złącze audio
- 14 Porty USB 3.2
- 15 Wskaźnik LED stanu portów PoE Ethernet
- 16 Wskaźnik LED aktywności dysku twardego
- 17 Wskaźnik LED stanu dysku twardego

Wskaźniki LED

Przednie diody LED

Przycisk zasilania	Wskaźnik LED zasilania	Wskazanie
Niewciśnięty	Wył.	Komputer i przełącznik są wyłączone
	Bursztynowy	Komputer jest włączony, a przełącznik wyłączony
	Miga na bursztynowo	Komputer jest włączony, a przełącznik uruchamia się
	Zielony	Komputer jest włączony, a przełącznik zakończył uruchamianie
Wciśnięty	Do 0 sekund	Włącza zarówno przełącznik, jak i komputer, jeśli są wyłączone
	Dopóki nie zacznie migać na bursztynowo (3 sekundy)	Przełącznik inicjuje łagodne wyłączenie
	Dopóki nie zacznie migać na czerwono (6 sekund)	Komputer i przełącznik inicjują łagodne wyłączenie
	Dopóki nie zacznie świecić na czerwono światłem stałym (9 sekund)	Komputer inicjuje nagłe wyłączenie, przełącznik inicjuje łagodne wyłączenie

Wskaźnik LED	Kolor	Wskazanie
Dysk twardy	Miga na zielono	Aktywność dysku twardego
	Czerwony	Możliwa awaria dysku twardego
Stan portu PoE Ethernet	Zielony	Stan łącza
	Bursztynowy	Zasilane urządzenie, brak stanu łącza
	Czerwony	Przekroczenie budżetu PoE
Stan dysku twardego	Zielony	Dysk twardy obecny
	Czerwony	Możliwa awaria dysku twardego

Tylne wskaźniki LED

Szybkość sieci i aktywność sieciowa	Kolor	Wskazanie
Prawy wskaźnik LED	Bursztynowy	10/100 Mbit/s
	Zielony	1000 Mbit/s
Lewy wskaźnik LED	Zielony	Połączenie PoE OK
	Czerwony	Przekroczenie budżetu PoE

Rozwiązywanie problemów –

Resetowanie serwera

Serwer można zresetować za pomocą przycisku resetowania serwera. Zresetowanie serwera potrwa ponad godzinę.

1. Wyłącz urządzenie.
2. Naciśnij i przytrzymaj przycisk resetowania serwera przez 5 sekund. Zostanie uruchomione środowisko Windows® RE.
3. Wybierz Troubleshoot (Rozwiązywanie problemów).
4. Wybierz Reset your PC (Resetuj komputer).
5. Wybierz Keep my files (Zachowaj moje pliki) lub Remove everything (Usuń wszystko). Jeśli wybierzesz Keep my files (Zachowaj moje pliki), musisz podać poświadczenia administratora.
6. Postępuj zgodnie z instrukcjami na ekranie.
7. Serwer uruchomi się ponownie i rozpocznie procedurę przywracania domyślnych ustawień fabrycznych systemu Windows®.



Przywracanie domyślnych ustawień fabrycznych serwera

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 oprogramowaniem AXIS Camera Station Pro

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

Potrzebujesz więcej pomocy?

Przydatne łącza

- *Instrukcja obsługi użytkownika oprogramowania AXIS Camera Station Pro*
- *Zaloguj się do AXIS Secure Remote Access*
- *Logowanie do funkcji AXIS Secure Remote Access v2*
- *Co ma się znaleźć na białej liście oprogramowania antywirusowego po zainstalowaniu programu AXIS Camera Station*

Kontakt z pomocą techniczną

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

T10207040_pl

2026-07 (M4.3)

© 2024 – 2026 Axis Communications AB