

Stacja robocza AXIS Camera Station S9302 Mk II Workstation

Podręcznik użytkownika

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 4.*
4. Skonfiguruj system Windows®. Zalecamy następujące czynności:
 - Zaktualizuj system Windows do najnowszej wersji. Patrz *Aktualizacja systemu Windows®, on page 16.*
 - Utwórz standardowe konto użytkownika. Patrz *Tworzenie konta użytkownika, on page 8.*
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 4.*

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®. Zalecamy, aby użytkownik nie wykorzystywał tych uprawnień, gdy jest administratorem programu AXIS Camera Station Pro.	Utworzone podczas pierwszej konfiguracji systemu Windows®.
Użytkownik systemu Windows® z uprawnieniami administratora AXIS Camera Station Pro	Użytkownik systemu Windows® z uprawnieniami administratora w AXIS Camera Station Pro, wykorzystywany przez integratora systemu lub administratora systemu do konfiguracji lub rozwiązywania problemów.	Utworzone w ustawieniach systemu Windows®.
Użytkownik systemu Windows® z uprawnieniami operatora lub obserwatora w AXIS Camera Station Pro	Użytkownik systemu Windows® z uprawnieniami operatora lub obserwatora w AXIS Camera Station Pro.	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 Pro.

Instalacja

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*.

Konfiguracja urządzenia

Wstępna konfiguracja rejestratora Axis

Po skonfigurowaniu systemu Windows® nastąpi automatyczne otwarcie aplikacji AXIS Recorder Toolbox. Kreator przeprowadzi Cię przez wstępną konfigurację. W tym kreatorze można skonfigurować kilka podstawowych i koniecznych ustawień do zarządzania urządzeniem w aplikacji AXIS Recorder Toolbox.

1. Wybierz motyw **Light** (Jasny) lub **Dark** (Ciemny) i kliknij przycisk **Next** (Dalej).
2. W razie potrzeby zmień nazwę komputera i kliknij **Next** (Dalej).
3. W obszarze **Power settings** (Ustawienia zasilania)
 - opcje **Never put the computer to sleep** (Nigdy nie przełączaj komputera w stan uśpienia) i **Never turn off the display** (Nigdy nie wyłączaj wyświetlacza) są wybrane domyślnie.
 - Zalecamy pozostawienie obu opcji zaznaczonych, aby podgląd na żywo i zapisy były dostępne przez cały czas. Możesz w dowolnym momencie przejść do menu **Start > Settings > System > Power & sleep** (Start > Ustawienia > System > Zasilanie i uśpienie) i zmienić te ustawienia.
4. 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.
5. 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.
6. Kliknij przycisk **Finish** (Zakończ). W razie zmiany nazwy komputera aplikacja AXIS Recorder Toolbox wyświetli monit o ponowne uruchomienie urządzenia.

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 5*
4. *Oglądaj materiał wideo na żywo, on page 5*
5. *Wyświetl nagrania, on page 5*
6. *Dodawanie zakładki, on page 5*

7. *Eksportuj nagrania, on page 6*
8. *Odtwarzanie i weryfikacja zapisów w AXIS File Player, on page 6*

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 Stacja robocza AXIS Camera Station S9302 Mk II Workstation 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 z łatwością 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. Przecignij 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 Stacją roboczą **AXIS Camera Station S9302 Mk II Workstation**, skonfiguruj ustawienia proxy lub zapory, jeżeli klient, serwer i połączone urządzenia sieciowe znajdują się w różnych sieciach.

Ustawienia proxy klienta

Jeżeli między 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 był przepuszczany ruch przez port HTTP, port TCP i port strumieniowania, które określono w usłudze Stacja robocza AXIS Camera Station S9302 Mk II Workstation Service Control. Po pomoc zwróć się do administratora sieci.

Konfiguracja portu serwera

Serwer Stacja robocza AXIS Camera Station S9302 Mk II Workstation 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 Stacja robocza AXIS Camera Station S9302 Mk II Workstation, kamery, koderzy wizyjne i urządzenia pomocnicze w zabezpieczonej sieci odseparowanej od sieci biurowej. Klienta Stacja robocza AXIS Camera Station S9302 Mk II Workstation możesz zainstalować na komputerze w innej sieci, na przykład sieci z dostępem do Internetu.
- Upewnij się, że wszyscy użytkownicy mają silne hasła.

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 Stacja robocza AXIS Camera Station S9302 Mk II Workstation.

Uwaga

Administratorzy komputera, na którym jest uruchomiony serwer Stacja robocza AXIS Camera Station S9302 Mk II Workstation, automatycznie otrzymują uprawnienia administratora w Stacja robocza AXIS Camera Station S9302 Mk II Workstation. Nie można zmienić ani usunąć uprawnień grupy administratorów.

Zanim dodasz użytkownika lub grupę, 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 mu indywidualnie lub przydzielaną tej grupie. Na przykład użytkownik mający dostęp do kamery X, który jednocześnie należy do grupy mającej dostęp 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 do użytkownika lub grupy. 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 Stacja robocza AXIS Camera Station S9302 Mk II Workstation. Aby dodać użytkownika do Stacja robocza AXIS Camera Station S9302 Mk II Workstation, 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 Stacja robocza AXIS Camera Station S9302 Mk II Workstation 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 Stacja robocza AXIS Camera Station S9302 Mk II Workstation – 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)	Zezwalanie na ręczne uruchamianie i zatrzymywanie nagrań.
Mechanical PTZ (Mechaniczny PTZ)	Zezwalanie 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 Stacja robocza AXIS Camera Station S9302 Mk II Workstation.
Edytuj	Umożliwia edycję widoków w Stacja robocza AXIS Camera Station S9302 Mk II Workstation.

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 zaleca się zastosowanie jej 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

W przypadku serii AXIS S12 i S93 pobierz aktualizację BIOS-u ze strony Dell, a nie z witryny Axis.com. P. sekcja *Aktualizacja BIOS-u, on page 16*.

Więcej informacji:

- *Dell: Wygaśnięcie certyfikatu bezpiecznego uruchamiania Microsoft 2011.*
- *Dell: Wytyczne dotyczące aktualizacji BIOS-u serwerów PowerEdge w zakresie bezpiecznego uruchamiania.*

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 F2 aż do pojawienia się logotypu Axis.

2. Wersja wyświetlana jest jako pierwszy wpis w sekcji **Overview** (Przegląd).

Aktualizacja BIOS-u

1. Przejdź do *Dell support* (Pomoc techniczna Dell).
2. W polu **Service tag** (Kod serwisowy) wpisz 7 ostatnich znaków numeru seryjnego Twojego urządzenia. Na przykład: HW030ABC1234.
3. Przejdź do **Drivers & Downloads** (Sterowniki i pobieranie) i wyszukaj hasło „BIOS”.
4. Jeżeli nie pojawi się nowsza wersja nazwy OEM Twojego produktu (na przykład „OEMR XL R760xs”), wyszukaj ponownie, używając ogólnej nazwy platformy Dell zamiast numeru seryjnego (na przykład „R760xs”).
5. Pobierz i zainstaluj najnowszą wersję BIOS-u wydaną po kwietniu 2026 r.

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).

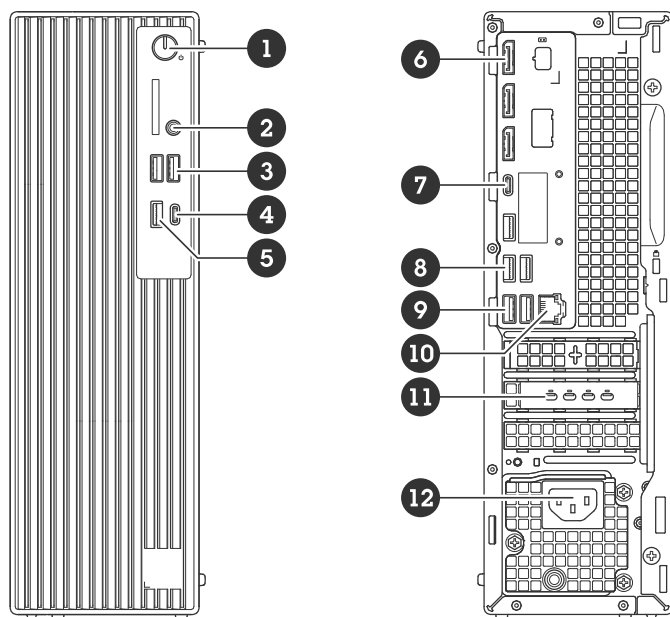
Przykład:

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.

Przegląd produktów



- 1 Wskaźnik LED przycisku zasilania/zasilania
- 2 Uniwersalne złącze audio
- 3 Porty USB 2.0
- 4 Port USB 3.2 gen 2x2 USB-C
- 5 Port USB 3.2 gen 2x1
- 6 Porty DisplayPorts™
- 7 Port USB 3.2 gen 2x1 USB-C
- 8 Porty USB 3.2 gen 1x1
- 9 Porty USB 2.0
- 10 Port Ethernet 1 GbE
- 11 Porty Mini DisplayPorts™
- 12 Złącze zasilania

Rozwiązywanie problemów –

Przeprowadzanie operacji odzyskiwania systemu

Przywracanie wewnętrzne

Jeżeli w urządzeniu doszło do awarii systemu, należy wykonać przywracanie wewnętrzne, aby odzyskać system.

1. Otwórz stronę **Windows Settings** (Ustawienia systemu Windows).
2. Wybierz **System**.
3. W menu wybierz **Recovery** (Przywracanie).
4. W sekcji **Recovery options** (Opcje odzyskiwania) wybierz **Reset this PC** (Resetuj ten komputer).
5. Wybierz **Keep my files** (Zachowaj moje pliki) lub **Remove everything** (Usuń wszystko).
 - Funkcja **Keep my files** (Zachowaj moje pliki) umożliwia zachowanie wszystkich plików osobistych i danych użytkownika, a także całego zainstalowanego oprogramowania Axis.
 - Funkcja **Remove everything** (Usuń wszystko) spowoduje usunięcie wszystkich plików osobistych i danych użytkownika, ale zachowa całe zainstalowane oprogramowanie Axis (ustawienia fabryczne).
6. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Uwaga

Przed kliknięciem przycisku **Reset** możesz wyświetlić listę aplikacji, które będą usunięte w następstwie procesu. Aplikacje Axis zostaną odzyskane po przywróceniu systemu, ale wszelkie inne zainstalowane aplikacje nie zostaną odzyskane.

Ważne

Po pomyślnym przywróceniu należy zalogować się do systemu Windows przy użyciu konta administratora w celu dokończenia procesu przywracania.

Odzyskiwanie zewnętrzne

Jeśli wystąpi całkowita awaria systemu, do odtworzenia systemu Windows® należy użyć obrazu odzyskiwania. W celu pobrania zestawu **AXIS Network Video Recovery Kit** skontaktuj się ze *wsparciem technicznym Axis* i podaj 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.

1. Pobierz zestaw **AXIS Network Video Recovery Kit** i wybrane narzędzie do zapisywania obrazów ISO na nośnikach USB.
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 do zapisywania obrazów ISO na nośnikach USB i postępuj zgodnie z instrukcjami na ekranie.

- Zapis danych na nośniku USB zajmuje około 10 – 15 minut. Nie wyjmuj nośnika USB przed zakończeniem zapisu.
- 4. Po zakończeniu pracy narzędzia do zapisywania obrazów ISO na nośnikach USB dołącz nośnik USB do urządzenia.
- 5. Uruchom urządzenie. Gdy pojawi się ekran powitalny Axis, naciśnij klawisz F12, aby otworzyć menu startowe.
- 6. Wybierz nośnik USB i naciśnij klawisz **Enter**. System zostanie uruchomiony w zestawie AXIS Network Video Recorder Recovery Kit.
- 7. Kliknij **Start** i postępuj zgodnie z instrukcjami na ekranie.
 - Odzyskiwanie trwa 10 – 15 minut.

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.

T10231344_pl

2026-07 (M2.2)

© 2025 – 2026 Axis Communications AB