

AXIS Camera Station S1296 Rack Recording Server

Spis treści

O urządzeniu	4
Od czego zacząć	5
Instalacja urządzenia.....	6
Przed rozpoczęciem instalacji	6
Konfiguracja urządzenia	7
Wstępna konfiguracja rejestratora Axis.....	7
Konfigurowanie oprogramowania AXIS Camera Station Pro	7
Uruchom system VMS	8
Dodawanie urządzeń.....	8
Dostosowywanie pojemności pamięci masowej.....	8
Konfiguracja metody zapisu.....	8
Oglądaj materiał wideo na żywo.....	8
Wyświetl nagrania.....	9
Dodawanie zakładki	9
Eksportuj nagrania.....	9
Odtwarzanie i weryfikacja zapisów w AXIS File Player.....	9
Network configuration (Konfiguracja sieci).....	10
Konfiguracja portu serwera.....	10
Kwestie dotyczące bezpieczeństwa.....	10
Licencja na system online.....	10
Licencja na system w trybie offline.....	10
Zarządzanie lokalnymi kontami użytkowników systemu Windows®	12
Tworzenie konta użytkownika	12
Utwórz konto administratora.....	12
Tworzenie lokalnej grupy użytkowników	12
Usuwanie konta użytkownika	12
Zmianie hasła do konta użytkownika.....	12
Tworzenie dysku resetowania hasła dla konta użytkownika	13
Zarządzanie kontami użytkowników w oprogramowaniu AXIS Camera Station Pro.....	14
Uprawnienia użytkownika	14
Dodawanie użytkowników lub grup.....	14
Uprawnienia użytkownika/grupy.....	15
Zarządzanie urządzeniem.....	18
Aktualizacja certyfikatów bezpiecznego uruchamiania	18
Sprawdzanie stanu certyfikatu	18
Zalecane działania	19
Aktualizacja certyfikatu poprzez BIOS.....	19
Aktualizacja certyfikatu za pomocą usługi Windows Update.....	19
Sprawdzanie bieżącej wersji systemu BIOS.....	19
Aktualizacja BIOS-u.....	20
Aktualizacja systemu Windows®	20
Konfigurowanie ustawień funkcji Windows® Update.....	20
Dodawanie dysku twardego.....	21
Proces	21
Instalacja dysku twardego w czasie pracy.....	21
Zmiana RAID.....	22
.....	22
Tworzenie nowej macierzy RAID	23
Konfiguracja systemu Microsoft Windows®	24
Konfiguracja iDRAC	25
Cyberbezpieczeństwo	26
Bezpieczny start	26
Moduł TPM (Trusted Platform Module).....	26

Weryfikacja bezpiecznych komponentów (SCV).....	26
Usługa powiadomień w systemach zabezpieczeń Axis.....	26
Postępowanie z lukami w zabezpieczeniach.....	26
Bezpieczne działanie urządzeń Axis	26
Rozwiązywanie problemów –	27
Uruchamianie diagnostyki	27
Przeprowadzanie operacji odzyskiwania systemu	27
Przywracanie wewnętrzne	27
Odzyskiwanie zewnętrzne.....	27
Eksportowanie kolekcji SupportAssist	28
Rozwiązywanie problemów z zasilaczem.....	29
Usuwanie błędów pamięci.....	29
Rozwiązywanie problemów z oprogramowaniem AXIS Camera Station Pro	29
Przegląd produktów	30
Przód i tylne boki	30
Specyfikacje	30
.....	30
Potrzebujesz więcej pomocy?	35
Przydatne łącza.....	35
Kontakt z pomocą techniczną.....	35

O urządzeniu

Seria rejestratorów AXIS Camera Station S12 Recorder składa się z gotowych do użycia serwerów do montażu w szafie aparaturowej i stacji roboczych zweryfikowanych pod kątem niezawodnego dozoru w wysokiej rozdzielczości do 4K. W celu zapewnienia szybkiej i łatwej instalacji seria ta została fabrycznie skonfigurowana i wyposażona w oprogramowanie AXIS Camera Station Pro do zarządzania obrazem, w tym w licencje i pełne niezbędne oprogramowanie systemowe. Konfigurację systemową można bez trudu zaimportować z aplikacji AXIS Site Designer, a AXIS Camera Station Pro umożliwia wykorzystanie szerokiego zakresu wizyjnych urządzeń dozоровych z oferty Axis. Dzięki dyskom twardym klasy Enterprise i dyskowi systemowemu SSD ten rejestrator jest niezawodnym i wydajnym elementem systemu.

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 7.*
4. Skonfiguruj system Windows®. Zalecamy następujące czynności:
 - Zaktualizuj system Windows do najnowszej wersji. Patrz *Aktualizacja systemu Windows®, on page 20.*
 - Utwórz standardowe konto użytkownika. Patrz *Tworzenie konta użytkownika, on page 12.*
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 7.*

Instalacja urządzenia

Przed rozpoczęciem instalacji

- Przygotuj wyposażenie dodatkowe konieczne przy instalacji: monitor, mysz, klawiaturę i kabel sieciowy.
- Uwaga: zestaw nie zawiera kabla zasilającego podłączanego do gniazdka ściennego.
- 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®.
Zarządzanie sprzętem		
iDRAC	Służy do uzyskania dostępu do narzędzia iDRAC (Integrated Dell Remote Access Controller).	Nazwa użytkownika: root Password (Hasło): Nadruk na odwrocie plakietki informacyjnej.
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.

Konfiguracja urządzenia

Wstępna konfiguracja rejestratora Axis

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

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

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 8*
4. *Oglądaj materiał wideo na żywo, on page 8*
5. *Wyświetl nagrania, on page 9*
6. *Dodawanie zakładki, on page 9*
7. *Eksportuj nagrania, on page 9*
8. *Odtwarzanie i weryfikacja zapisów w AXIS File Player, on page 9*

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 S1296 Rack Recording Server 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.

Dostosowywanie pojemności pamięci masowej

Uwaga

W systemach wykorzystujących ponad 100 kanałów wideo lub szybkość zapisu przekraczającą 1 Gbit/s zalecamy ustawienie pułapu 95% przestrzeni na nagrania. Wszystkie urządzenia współpracujące z programem AXIS Camera Station w wersji 5.56 lub nowszej mają domyślnie ustawioną wartość 95%.

1. Wybierz kolejno opcje **Configuration > Storage > Management** (Konfiguracja > Pamięć masowa > Zarządzanie).
2. Z listy zasobów pamięci wybierz lokalny zasób lub udostępniony dysk sieciowy.
3. W sekcji **Overview** (Przegląd) przesun suwak, aby ustawić maksymalną ilość miejsca, jaką może wykorzystać program AXIS Camera Station.
4. Kliknij przycisk **Apply** (Zastosuj).

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. 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 S1296 Rack Recording Server, 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 AXIS Camera Station S1296 Rack Recording Server Service Control. Po pomocy zwróć się do administratora sieci.

Konfiguracja portu serwera

Serwer AXIS Camera Station S1296 Rack Recording Server 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 S1296 Rack Recording Server, kamery, kodery wizyjne i urządzenia pomocnicze w zabezpieczonej sieci odseparowanej od sieci biurowej. Klienta AXIS Camera Station S1296 Rack Recording Server 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 S1296 Rack Recording Server.
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 S1296 Rack Recording Server.

Uwaga

Administratorzy komputera, na którym jest uruchomiony serwer AXIS Camera Station S1296 Rack Recording Server, automatycznie otrzymują uprawnienia administratora w AXIS Camera Station S1296 Rack Recording Server. 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 AXIS Camera Station S1296 Rack Recording Server. Aby dodać użytkownika do AXIS Camera Station S1296 Rack Recording Server, 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 S1296 Rack Recording Server 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 roli 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 S1296 Rack Recording Server – 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 AXIS Camera Station S1296 Rack Recording Server.
Edytuj	Umożliwia edycję widoków w AXIS Camera Station S1296 Rack Recording Server.

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 20*.

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.

Dodawanie dysku twardego

Zapotrzebowanie na pamięć masową może być różne. Określenie czasu przechowywania zapisanych danych lub potrzeba przechowywania nagrań o wysokiej rozdzielczości często prowadzi do tego samego wniosku: konieczności rozbudowy pamięci masowej. W tej sekcji wyjaśniono sposoby rozbudowy serwerów zapisu serii AXIS S12 o większą liczbę dysków twardych oraz dodawanie ich do konfiguracji macierzy RAID 5.

Uwaga

Poniższe instrukcje należy stosować przy rozbudowie zasobów w określonych modelach serii AXIS S12. Instrukcje dotyczą stanu bieżącego, a firma Axis Communications AB nie ponosi odpowiedzialności za utratę danych ani błędnie przeprowadzoną konfigurację. 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 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.

Proces

1. *Instalacja dysku twardego w czasie pracy, on page 21*
 - 1.1. *Zdejmowanie ramki, on page 21*
 - 1.2. *Wyjmowanie zaślepki dysku twardego, on page 21*
 - 1.3. *Instalowanie dysku twardego, on page 22*
2. *Tworzenie nowej macierzy RAID, on page 23*
 - 2.1. *Uruchom narzędzie konfiguracyjne Dell PERC 11 Configuration Utility, on page 23*
 - 2.2. *Tworzenie macierzy RAID, on page 23*
 - 2.3. *Ponowna konfiguracja macierzy RAID, on page 23*
- 3.

Instalacja dysku twardego w czasie pracy

Zdejmowanie ramki

1. Odszukaj klucz ramki.
2. Odblokuj ramkę za pomocą klucza.
3. Przesuń zatrzask zwalniający w górę i pociągnij lewy koniec ramki.
4. Odczep prawy koniec i zdejmij ramkę.

Wyjmowanie zaślepki dysku twardego

- Naciśnij przycisk zwalniający z przodu zaślepki i wysuń ją z gniazda dysku twardego.

Instalowanie dysku twardego

▲ UWAGA

- Należy używać wyłącznie dysków twardych, które zostały przetestowane i zatwierdzone do użytku z serią AXIS S12.
 - Podczas instalowania dysku twardego należy się upewnić, że sąsiednie dyski są w pełni zainstalowane. Włożenie kieszeni z dyskiem twardym i próba zablokowania jej uchwytu obok częściowo zainstalowanej kieszeni może spowodować uszkodzenie sprężyny osłony częściowo zainstalowanej kieszeni i uniemożliwić jej dalsze użytkowanie.
 - Łączenie dysków twardych SAS i SATA w tym samym woluminie RAID nie jest obsługiwane.
1. Jeżeli w gnieździe dysku twardego znajduje się zaślepka, wyjmij ją.
 2. Zainstaluj dysk twardy w przeznaczonej na niego kieszeni.
 3. Naciśnij przycisk zwalniający z przodu kieszeni dysku twardego i otwórz uchwyt kieszeni dysku.
 4. Włóż kieszeń dysku twardego do gniazda dysku i wsuń ją tak, aby połączyła się z płytą montażową.
 5. Zamknij uchwyt kieszeni dysku twardego, aby zablokować dysk twardy w obecnym położeniu.

Zmiana RAID

▲ UWAGA

Zmiana macierzy RAID powoduje usunięcie wszystkich danych z dysków.

1. Uruchamianie narzędzia Lifecycle Controller:
 - 1.1. Włącz urządzenie.
 - 1.2. Po wyświetleniu ekranu powitalnego AXIS naciśnij klawisz F10.
2. W narzędziu Lifecycle Controller przejdź do menu **Hardware Configuration > Configuration Wizards (Konfiguracja sprzętu > Kreatory konfiguracji)** i wybierz **RAID Configuration (Konfiguracja RAID)**.
3. Wybierz **RAID Controller (Kontroler RAID)**, na którym chcesz utworzyć macierz RAID. Szczegóły dotyczące wirtualnych dysków dostępnych na wybranym kontrolerze zostaną przedstawione w tabeli wyświetlonej na stronie poniżej listy kontrolerów. Foreign Configuration (Obca konfiguracja) zostanie wyświetlona, jeśli na serwerze dostępne są obce lub niezainicjowane dyski twarde.

Uwaga

- Wyczyszczenie obcej konfiguracji powoduje wyczyszczenie wszystkich obcych dysków twardych dostępnych na wybranym kontrolerze RAID.
 - Ignorowanie konfiguracji obcej powoduje ignorowanie obcych dysków twardych dostępnych na kontrolerze RAID podczas tworzenia woluminu RAID.
4. Wyczyść lub zignoruj obce dyski twarde i niezainicjowane dyski twarde.
W razie potrzeby można zainicjować dyski niezainicjowane:
 - 4.1. Na liście wszystkich dysków twardych bez RAID (niezainicjowanych) wybierz dyski twarde, które chcesz przekonwertować na obsługujące RAID (zainicjować) i kliknij **Next (Dalej)**, aby je zainicjować.
 - 4.2. Wybierz odpowiednią opcję na stronie Configuration Wizards: RAID Configuration (Kreatory konfiguracji: Konfiguracja RAID).
 5. Wybierz poziom RAID.
 6. Wybierz dyski fizyczne z tabeli i kliknij przycisk **Next (Dalej)**.
W przypadku wybrania opcji **Ignore foreign configuration (ignoruj obce konfiguracje)**, obce dyski twarde nie będą wyświetlane w tabeli.
 7. Wprowadź atrybuty dysku wirtualnego.
 8. Kliknij **Next (Dalej)**.
 9. Przejrzyj ustawienia i kliknij przycisk **Finish (Zakończ)**.

10. Lifecycle Controller wyświetla komunikat informujący, że wszystkie aktualne dane o dyskach wirtualnych dostępnych na kontrolerze zostaną utracone. Kliknij przycisk **OK**, aby kontynuować.
11. Kliknij kolejno **OK** i **Finish** (Zakończ).
12. Zamknij kreatora i uruchom ponownie system.

Tworzenie nowej macierzy RAID

Narzędzie konfiguracyjne Human Interface Infrastructure (HII) to aplikacja do zarządzania pamięcią masową, zintegrowana z systemowym BIOSem. Służy do konfigurowania i zarządzania kontrolerami, dyskami wirtualnymi i dyskami fizycznymi. Jest niezależne od systemu operacyjnego.

Uruchom narzędzie konfiguracyjne Dell PERC 11 Configuration Utility

1. Uruchom system.
2. Podczas uruchamiania systemu naciśnij klawisz F2, aby przejść do ustawień systemu (System Setup).
3. Kliknij **Device Settings** (Ustawienia urządzenia), aby wyświetlić wszystkie kontrolery RAID w systemie.

Tworzenie macierzy RAID

1. *Uruchom narzędzie konfiguracyjne Dell PERC 11 Configuration Utility, on page 23.*
2. Kliknij **Main Menu > Configuration Management > Create Virtual Disk** (Menu główne > Zarządzanie konfiguracją > Utwórz dysk wirtualny) i zdefiniuj następujące parametry dysku wirtualnego.
 - **Select RAID Level** (Wybierz poziom RAID): Zmień poziom RAID.
 - **Zaznacz Physical Disks** (Dyski fizyczne): Wybierz dyski fizyczne, na podstawie których tworzone są dyski wirtualne. Opcja ta jest wyświetlana, jeżeli jako pojemność dysku fizycznego wybierzesz **Unconfigured Capacity** (Nieskonfigurowana pojemność).
 - **Configure Virtual Disk** (Konfiguruj dysk wirtualny): Skonfiguruj następujące parametry dysku wirtualnego.
 - **Virtual Disk Name** (Nazwa dysku wirtualnego): Wpisz nazwę dysku wirtualnego. Dozwolone znaki to litery A – Z, a – z, cyfry 0 – 9, znak podkreślenia (_) oraz myślnik (-).
 - **Virtual Disk Size** (Pojemność dysku wirtualnego): Ustaw pojemność dysku wirtualnego.
3. Kliknij **Create Virtual Disk** (Utwórz dysk wirtualny).

▲ UWAGA

Dostępnych jest więcej parametrów do modyfikacji. Axis Communications AB nie ponosi odpowiedzialności za jakiegokolwiek błędne konfiguracje, które mogą wystąpić w wyniku zmiany tych parametrów. Przy zmianie parametrów należy zawsze zachować ostrożność.

Ponowna konfiguracja macierzy RAID

Wirtualny dysk sieciowy można ponownie skonfigurować w taki sposób, aby zwiększyć jego pojemność i zmienić poziom macierzy RAID.

▲ UWAGA

- Dysków wirtualnych typu RAID 50 i 60 nie można ponownie skonfigurować.
 - Ponowna konfiguracja dysków wirtualnych zazwyczaj wpływa na ich parametry do momentu zakończenia tej operacji. Czas realizacji może się znacznie różnić i trwać nawet kilka dni. Zaleca się przeprowadzenie tej procedury w czasie przeznaczonym na prace utrzymaniowe.
 - Przed podjęciem jakichkolwiek działań należy zawsze wykonać potwierdzoną kopię zapasową danych.
1. *Uruchom narzędzie konfiguracyjne Dell PERC 11 Configuration Utility, on page 23.*
 2. Kliknij **Main Menu > Virtual Disk Management** (Menu główne > Zarządzanie dyskami wirtualnymi). Wyświetlane są wszystkie dyski wirtualne powiązane z kontrolerem RAID.
 3. Aby wyświetlić właściwości, kliknij dysk wirtualny.

4. W menu rozwijalnym **Operations** (Operacje) wybierz **Reconfigure Virtual Disks** (Ponowna konfiguracja dysków wirtualnych), a następnie naciśnij **GO** (Przejdź).
5. Wybierz poziom RAID – **RAID Level** i naciśnij **Choose the Operation** (Wybierz operację).
6. Wybierz dyski do dodania do dysku wirtualnego, a następnie naciśnij **Apply Changes** (Zastosuj zmiany).
7. Potwierdź operację i kliknij **YES** (Tak).
8. Kliknij **Start Operation** (Rozpocznij operację).
9. Kliknij **OK**.

Na stronie Virtual Disk Management (Zarządzanie dyskami wirtualnymi) można sprawdzić stan przebiegu odbudowy zmodyfikowanego dysku wirtualnego.

Po rozpoczęciu odbudowy system można pozostawić w narzędziu Dell PERC 11 Configuration Utility do czasu zakończenia procesu lub uruchomić go ponownie w systemie operacyjnym.

Jeżeli system zostanie uruchomiony ponownie w ramach systemu operacyjnego, jego wydajność będzie ograniczona do czasu zakończenia odbudowy.

NIE można również rozszerzyć dysku w systemie Windows® przed zakończeniem odbudowy.

▲ UWAGA

Czas odbudowy będzie się różnił w zależności od systemu i może trwać nawet kilka dni.

Konfiguracja systemu Microsoft Windows®

Aby skonfigurować nowy wolumin:

1. Kliknij prawym przyciskiem myszy menu Start i wybierz **Disk Management (Zarządzanie dyskami)**.
2. Kliknij prawym przyciskiem myszy nieprzydzielony obszar na dysku twardym i wybierz **New Simple Volume** (Nowy wolumin prosty).
3. W sekcji **New Simple Volume Wizard** (Kreator nowego prostego woluminu) kliknij **Next** (Dalej).
4. Wpisz wielkość woluminu do utworzenia w megabajtach (MB) lub zaakceptuj domyślną wielkość maksymalną, a następnie kliknij **Next** (Dalej).
5. Zaakceptuj domyślną literę dysku lub wybierz inną literę do oznaczenia partycji, a następnie kliknij **Next** (Dalej).
6. W oknie dialogowym **Format Partition** (Formatowanie partycji):
 - Jeżeli nie chcesz sformatować woluminu w tej chwili, zaznacz **Do not format this volume** (Nie formatuj tego woluminu), a następnie kliknij **Next** (Dalej).
 - Aby sformatować wolumin przy użyciu domyślnych ustawień, kliknij **Next** (Dalej).
7. Sprawdź dokonane wybory, a następnie kliknij **Finish** (Zakończ).
W narzędziu Disk Management (Zarządzanie dyskami) widoczny jest teraz nowy wolumin. Możesz teraz zamknąć okno Disk Management (Zarządzanie dyskami) – system jest gotowy do korzystania z nowego woluminu.

Aby skonfigurować istniejący wolumin:

1. Kliknij prawym przyciskiem myszy menu Start i wybierz **Disk Management (Zarządzanie dyskami)**.
2. Kliknij prawym przyciskiem myszy wolumin i wybierz **Extend Volume** (Rozszerz wolumin).
3. W sekcji **Extend Volume Wizard** (Kreator rozszerzonego woluminu) kliknij **Next** (Dalej).
4. Wybierz dysk zawierający nieużywane miejsce i kliknij **Dalej**. Zazwyczaj jest on zaznaczony domyślnie.
5. Sprawdź dokonane wybory, a następnie kliknij **Finish** (Zakończ).
W narzędziu Disk Management (Zarządzanie dyskami) widoczny jest teraz rozszerzony wolumin. Możesz teraz zamknąć okno Disk Management (Zarządzanie dyskami) – system jest gotowy do korzystania z nowego woluminu.

Konfiguracja iDRAC

Zintegrowany kontroler zdalnego dostępu Dell Remote Access Controller 9 (iDRAC9) z technologią Lifecycle Controller został zaprojektowany z myślą o usprawnieniu pracy administratorów systemów i poprawie ogólnej dostępności systemów firmy Dell. iDRAC ostrzega administratorów o problemach z systemem, pomaga im zdalnie zarządzać systemem i zmniejsza wymagania w zakresie fizycznego dostępu do systemu. Aby umożliwić komunikację do iDRAC i z iDRAC, skonfiguruj początkowe ustawienia sieciowe w oparciu o posiadaną infrastrukturę sieciową.

1. Naciśnij klawisz F10 podczas automatycznego testu zasilania (POST).

Uwaga

Kreator konfiguracji początkowej Lifecycle Controller zostanie wyświetlony tylko po raz pierwszy. Użyj kreatora konfiguracji początkowej, aby wybrać język i klawiaturę, skonfigurować ustawienia sieciowe, ustawienia sieciowe iDRAC, konfigurację poświadczeń oraz wyświetlić podsumowanie ustawień. Aby później wprowadzić zmiany w konfiguracji, wybierz **Settings (Ustawienia)** na stronie głównej narzędzia Lifecycle Controller.

2. Skonfiguruj język i klawiaturę, kliknij przycisk **Next (Dalej)**.
3. Zapoznaj się z informacjami ogólnymi o produkcie i kliknij przycisk **Next (Dalej)**.
4. Konfiguracja ustawień sieciowych narzędzia Lifecycle Controller:
 - 4.1. Na liście rozwijanej **NIC Card (Karta NIC)** wybierz port NIC, który chcesz skonfigurować.
 - 4.2. Na liście rozwijanej **IPV4 Network Settings > IP Address Source (Ustawienia sieci IPV4 > Źródło adresu IP)** wybierz jedną z następujących opcji:
 - **DHCP**: wskazuje, że karta sieciowa musi zostać skonfigurowana z wykorzystaniem adresu IP z serwera DHCP. DHCP jest opcją domyślną, a adres IP DHCP jest wyświetlany na stronie Network Settings (Ustawienia sieciowe).
 - **Static IP (Statyczny adres IP)**: wskazuje, że karta sieciowa musi zostać skonfigurowana przy użyciu statycznego adresu IP. Wpisz właściwości adresu IP, czyli **IP Address (Adres IP)**, **Subnet Mask (Maska podsieci)**, **Default Gateway (Brama domyślna)** i **DNS Address (Adres DNS)**. Jeżeli nie masz tych informacji, skontaktuj się z administratorem sieci.
 - **No Configuration (Brak konfiguracji)**: oznacza, że nie można konfigurować karty sieciowej.
 - 4.1. Jeżeli używana jest sieć VLAN, kliknij opcję **Enabled (Włączone)** i wpisz **VLAN ID (ID sieci VLAN)** oraz **Priority (Priorytet)** w menu Lifecycle Controller VLAN Settings (Ustawienia VLAN narzędzia Lifecycle Controller), aby skonfigurować ustawienia sieci VLAN karty NIC.
 - 4.2. Kliknij **Next (Dalej)**. Jeśli ustawienia narzędzia Lifecycle Controller nie są prawidłowo skonfigurowane, zostanie wyświetlony komunikat o błędzie.
5. Konfigurowanie sieci iDRAC i poświadczeń:
 - 5.1. Otwórz menu **IPV4 Configuration > IP Address Source (Konfiguracja IPV4 > Źródło adresu IP)** i wybierz jedną z następujących opcji:
 - **Static (Adres statyczny)**: wskazuje, że sieć musi zostać skonfigurowana przy użyciu statycznego adresu IP. Wpisz właściwości adresu IP, czyli **IP Address (Adres IP)**, **Subnet Mask (Maska podsieci)**, **Default Gateway (Brama domyślna)**, **DNS Address Source (Źródło adresu DNS)** oraz **DNS Address (Adres DNS)**. Jeżeli nie masz tych informacji, skontaktuj się z administratorem sieci.
 - **DHCP**: wskazuje, że karta sieciowa musi zostać skonfigurowana z wykorzystaniem adresu IP z serwera DHCP. DHCP jest opcją domyślną, a adres IP DHCP jest wyświetlany na stronie Network Settings (Ustawienia sieciowe).
 - 5.1. W menu **Credentials (Poświadczenia)** wpisz **Account Username (Nazwę użytkownika konta)** oraz **Password (Hasło)** w celu uzyskania dostępu do sieci iDRAC.
 - 5.2. Kliknij **Next (Dalej)**.
6. Zweryfikuj podsumowanie konfiguracji narzędzia Lifecycle Controller oraz sieci iDRAC i kliknij przycisk **Finish (Zakończ)**.

Cyberbezpieczeństwo

Informacje na temat cyberbezpieczeństwa dotyczące poszczególnych produktów można znaleźć w opisie produktu na stronie [Axis.com](https://axis.com).

Aby uzyskać szczegółowe informacje na temat cyberbezpieczeństwa w systemie AXIS OS, zapoznaj się z *przewodnikiem po zabezpieczeniach systemu operacyjnego AXIS OS*.

Bezpieczny start

Funkcja bezpiecznego uruchamiania zapobiega uruchamianiu złośliwego oprogramowania i niebezpiecznego oprogramowania w systemie. Uruchamia się przy rozruchu systemu i wykorzystuje podpisy cyfrowe do weryfikacji certyfikatów oprogramowania i systemu operacyjnego (OS). W systemie mogą działać wyłącznie zaufane oprogramowanie i system operacyjny (OS).

Moduł TPM (Trusted Platform Module)

Moduł TPM to składnik udostępniający funkcje kryptograficzne umożliwiające ochronę informacji przed nieupoważnionym dostępem. Jest domyślnie włączony i nie zaleca się jego wyłączenia.

Weryfikacja bezpiecznych komponentów (SCV)

Kiedy urządzenie zostało wyprodukowane w fabryce, utworzono dla niego certyfikat, aby zagwarantować, że otrzymasz to, co zostało zamówione, i że nikt nie dopuścił się sabotażu wobec urządzenia od czasu, gdy opuściło ono fabrykę. Fabryka podpisuje certyfikat i zapisuje go w iDRAC. Po otrzymaniu urządzenia przejdź do oprogramowania AXIS Recorder Toolbox, aby sprawdzić, czy urządzenie ma SCV, i zweryfikować certyfikat. W ramach weryfikacji inwentaryzacja systemu zakończy się wynikiem pozytywnym lub negatywnym. Więcej informacji na temat SCV można znaleźć w witrynie internetowej dell.com.

Usługa powiadomień w systemach zabezpieczeń Axis

Axis świadczy usługę powiadamiania z informacjami o lukach w zabezpieczeniach i innych sprawach dotyczących bezpieczeństwa urządzeń Axis. Aby otrzymywać powiadomienia, możesz aktywować subskrypcję na stronie axis.com/security-notification-service.

Postępowanie z lukami w zabezpieczeniach

Aby maksymalnie ograniczyć narażenie rozwiązań klientów na ataki, firma Axis, będąca **organem numeracji w programie CVE (Common Vulnerability and Exposures)**, przestrzega standardów branżowych w zakresie zarządzania wykrytymi lukami w naszych urządzeniach, oprogramowaniu i usługach oraz reagowania w takich przypadkach. Aby uzyskać więcej informacji na temat zasad zarządzania lukami w zabezpieczeniach rozwiązań Axis, sposobu zgłaszania luk w zabezpieczeniach, wykrytych luk w zabezpieczeniach i odpowiednich porad dotyczących bezpieczeństwa, zob. axis.com/vulnerability-management.

Bezpieczne działanie urządzeń Axis

Urządzenia Axis z domyślnymi ustawieniami fabrycznymi są wstępnie skonfigurowane z zabezpieczonymi domyślnymi mechanizmami ochrony. Zalecamy korzystanie z lepiej zabezpieczonej konfiguracji podczas instalowania urządzenia. Aby dowiedzieć się więcej o podejściu Axis do cyberbezpieczeństwa, w tym o najlepszych praktykach, zasobach i wytycznych dotyczących zabezpieczania urządzeń, odwiedź stronę axis.com/about-axis/cybersecurity.

Aby dowiedzieć się więcej o funkcjach cyberbezpieczeństwa stosowanych w urządzeniach Axis, przejdź do strony axis.com/learning/white-papers i poszukaj według hasła „cybersecurity”.

Rozwiązywanie problemów –

Uruchamianie diagnostyki

Włączenie diagnostyki pomaga zidentyfikować przyczynę problemu z systemem. Diagnostyka przeprowadza testy osprzętu systemowego bez konieczności stosowania dodatkowych urządzeń ani zagrożenia utraty danych.

1. Podczas uruchamiania systemu naciśnij klawisz F10, aby przejść do narzędzia Lifecycle Controller.
2. Przejdź do menu **Hardware Diagnostics (Diagnostyka sprzętu)** i kliknij **Run Hardware Diagnostics (Uruchom diagnostykę sprzętu)**.
3. Zapisz kod błędu i skontaktuj się z działem pomocy technicznej firmy Axis.

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.

Eksportowanie kolekcji SupportAssist

Kolekcję SupportAssist można wyeksportować na dysk USB lub do udziału sieciowego (CIFS/NFS). Kolekcja obejmuje następujące dane:

- Sprzęt
- Dzienniki kontrolera RAID

Aby wyeksportować kolekcję SupportAssist:

1. Podczas automatycznego testu zasilania (POST) naciśnij klawisz **F10**, aby uruchomić narzędzie Lifecycle Controller.
2. Otwórz menu **Hardware Diagnostics > Export SupportAssist collection** (Diagnostyka sprzętu > Eksport kolekcji SupportAssist).
3. Zapoznaj się z warunkami i kliknij przycisk **Next (Dalej)**.
Zaakceptowanie warunków jest konieczne, aby pomoc techniczna mogła korzystać z danych zbieranych przez SupportAssist.
4. Wybierz opcje danych, które chcesz dołączyć do kolekcji SupportAssist i kliknij przycisk **Next (Dalej)**.
5. Wprowadź wymagane informacje dotyczące ustawień eksportu i kliknij **Next (Dalej)**.
 - Aby wyeksportować na dysk USB: wybierz opcję dysku USB, następnie wybierz nazwę dysku USB i wprowadź dane dotyczące ścieżki do pliku, do którego ma zostać wyeksportowana kolekcja.
 - Aby wyeksportować do NFS: wybierz opcję NFS i wprowadź wymagane informacje.
 - Aby wyeksportować do CIFS: wybierz opcję CIFS i wprowadź wymagane informacje. Kliknij **Test Network Connection (Testuj połączenie sieciowe)**, aby sprawdzić, czy Lifecycle Controller może połączyć się z podanym adresem IP. Domyślnie pinguje IP bramy, IP serwera DNS, IP hosta i IP proxy.
6. Sprawdź wybrane opcje i kliknij przycisk **Finish (Zakończ)**.
Lifecycle Controller pobiera wybrane dane kolekcji i eksportuje do określonej lokalizacji. Może to potrwać kilka minut.

Rozwiązywanie problemów z zasilaczem

Uwaga

Po zainstalowaniu zasilacza należy odczekać kilka sekund, aby system go rozpoznał i określił, czy działa prawidłowo.

1. Upewnij się, że nie ma żadnych luźnych połączeń. Na przykład luźne przewody zasilające.
2. Upewnij się, że dioda LED uchwytu zasilacza wskazuje prawidłowe działanie zasilacza.
3. Sprawdź stan wskaźnika zasilania na zasilaczu. Patrz *Specyfikacje, on page 30*.
4. W przypadku konfiguracji z zasilaczem nadmiarowym upewnij się, że oba zasilacze są tego samego typu i o tej samej mocy.
5. Upewnij się, że używane są wyłącznie zasilacze z etykietą Extended Power Performance (EPP) umieszczoną z tyłu.
6. Zresetuj moduł zasilacza.
7. Jeżeli problem nie ustąpi, skontaktuj się z pomocą techniczną Axis.

Usuwanie błędów pamięci

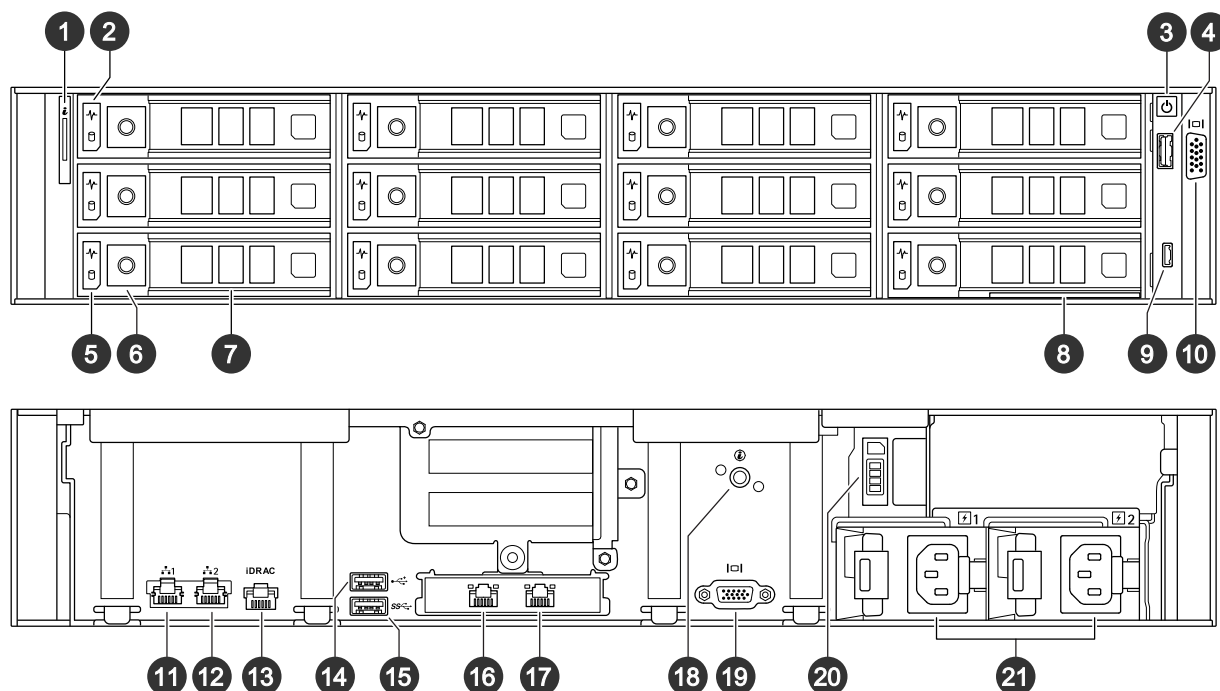
1. Uaktualnij system BIOS do najnowszej wersji.
2. Jeżeli błędy nadal będą występować, skontaktuj się z działem pomocy technicznej firmy Axis.

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*.

Przegląd produktów

Przód i tylne boki



- 1 Przycisk identyfikacji systemu i wskaźnik
- 2 Wskaźnik LED stanu dysku twardego
- 3 Wskaźnik LED przycisku zasilania/zasilania
- 4 Port USB 2.0
- 5 Wskaźnik LED aktywności dysku twardego
- 6 Przycisk zwalniający tarcę dysku twardego
- 7 Taca dysku twardego
- 8 Plakietka informacyjna
- 9 Port iDRAC direct
- 10 Port VGA
- 11 Port Ethernet 1 – 1 GbE (nie używać)
- 12 Port Ethernet 2 – 1 GbE (nie używać)
- 13 dedykowany port Ethernet iDRAC
- 14 Port USB 2.0
- 15 Port USB 3.0
- 16 Port Ethernet 1 – 10 GbE
- 17 Port Ethernet 2 – 10 GbE
- 18 Przycisk identyfikacji systemu i wskaźnik
- 19 Port VGA
- 20 Taca dysku SSD
- 21 Zespoły zasilające

Specyfikacje

Wskaźnik LED stanu

dioda LED	Opis	Akcja
Wskaźnik dysku	Wskaźnik zmienia kolor na bursztynowy, jeśli wystąpi błąd dysku.	Sprawdź Dziennik zdarzeń systemowych, aby określić, czy wystąpił błąd dysku.

Wskaźnik temperatury	Wskaźnik zmienia kolor na bursztynowy, jeśli w systemie wystąpi błąd związany z temperaturą. Na przykład temperatura otoczenia jest poza zakresem lub nastąpiła awaria wentylatora.	Upewnij się, że nie występuje żaden z poniższych warunków: • Wentylator chłodzący został usunięty lub uległ awarii. • Zdjęto pokrywę systemu, osłony powietrza lub wspornik tylnego wypełniacza. • Temperatura otoczenia jest zbyt wysoka. • Zewnętrzny przepływ powietrza jest utrudniony.
Wskaźnik elektryczny	Wskaźnik zmienia kolor na bursztynowy, jeśli w systemie wystąpi błąd związany z elektrycznością. Na przykład, napięcie poza zakresem lub uszkodzony zasilacz lub regulator napięcia.	Sprawdź Dziennik zdarzeń systemowych lub komunikaty systemowe dotyczące konkretnego problemu. Jeżeli problem dotyczy zasilacza, sprawdź wskaźnik LED na zasilaczu. Zresetuj zasilacz.
Wskaźnik pamięci	W przypadku wystąpienia błędu pamięci wskaźnik zmienia kolor na bursztynowy.	Sprawdź lokalizację uszkodzonej pamięci w dzienniku zdarzeń systemowych lub komunikatach systemowych. Ponownie podłącz moduł pamięci.
Wskaźnik PCIe	Jeśli wystąpi błąd karty PCIe, wskaźnik zmieni kolor na bursztynowy.	Uruchom ponownie system. Zaktualizuj wymagane sterowniki karty PCIe. Ponownie uruchom kartę.

Wskaźniki identyfikatorów i stanu systemu

dioda LED	Opis	Akcja
Światło ciągle niebieskie	System jest włączony, w dobrym stanie, a tryb ID systemu nie jest aktywny.	Naciśnij przycisk stanu systemu i ID systemu, aby przejść do trybu ID systemu.
Migotanie, niebieskie	Tryb ID systemu jest aktywny.	Naciśnij przycisk stanu systemu i ID systemu, aby przejść do trybu stanu systemu.
Światło ciągle bursztynowe	System działa w trybie awaryjnym.	
Migotanie, bursztynowe	Wystąpił błąd systemu.	Sprawdź dziennik zdarzeń systemowych pod kątem konkretnego komunikatu o błędzie.

Wskaźniki LED iDRAC direct

dioda LED	Opis
Światło ciągle zielone świeci przez dwie sekundy	Został podłączony komputer typu laptop lub tablet.

Migający zielony (włączony na dwie sekundy i wyłączony na dwie sekundy)	Został rozpoznany podłączony laptop lub tablet.
Wył.	Laptop lub tablet zostały odłączone.

Wskaźniki NIC

dioda LED	Opis
Wskaźniki połączenia i aktywności są wyłączone	Karta NIC nie jest podłączona do sieci.
Wskaźnik połączenia świeci na zielono, a wskaźnik aktywności miga na zielono.	Karta NIC jest podłączona do prawidłowej sieci z maksymalną prędkością portu i dane są wysyłane lub odbierane.
Wskaźnik połączenia świeci na bursztynowo, a wskaźnik aktywności miga na zielono.	Karta NIC jest podłączona do prawidłowej sieci z prędkością portu poniżej maksymalnej i dane są wysyłane lub odbierane.
Wskaźnik połączenia jest zielony, a wskaźnik aktywności jest wyłączony	Karta NIC jest podłączona do prawidłowej sieci z maksymalną prędkością portu, a dane nie są wysyłane lub odbierane.
Wskaźnik połączenia jest bursztynowy, a wskaźnik aktywności jest wyłączony	Karta NIC jest podłączona do prawidłowej sieci z prędkością portu poniżej maksymalnej, a dane nie są wysyłane lub odbierane.

Wskaźniki zasilacza (PSU)

dioda LED	Opis
Zielony	Prawidłowe źródło zasilania jest podłączone do zasilacza i zasilacz działa.
Migotanie, bursztynowe	Wystąpił problem z zasilaczem.
Brak zasilania	Zasilacz nie ma podłączonego źródła zasilania.

Migotanie, zielone	Trwa aktualizacja oprogramowania sprzętowego zasilacza. ▲ UWAGA Podczas aktualizacji oprogramowania układowego nie odłączaj kabla zasilającego ani zasilacza. Jeżeli aktualizacja oprogramowania układowego zostanie przerwana, zasilacze przestaną działać.
Miga na zielono i wyłącza się	Po podłączeniu zasilacza w czasie pracy, miga on na zielono pięć razy z częstotliwością 4 Hz i wyłącza się. Oznacza to niedopasowanie zasilacza pod względem wydajności, zestawu funkcji, stanu lub obsługiwanego napięcia. ▲ UWAGA • Jeśli zainstalowane są dwa zasilacze, oba muszą mieć ten sam typ etykiety. Na przykład etykietę Extended Power Performance (EPP). Łączenie zasilaczy z poprzednich generacji serwerów PowerEdge nie jest obsługiwane, nawet jeśli zasilacze mają taką samą moc znamionową. Powoduje to stan niedopasowania zasilacza lub brak możliwości włączenia systemu. • W przypadku stosowania dwóch zasilaczy muszą one być tego samego typu i mieć taką samą maksymalną moc wyjściową. • Aby rozwiązać problem niedopasowania zasilacza, należy wymienić zasilacz z migającym wskaźnikiem. Zamiana zasilaczy w celu uzyskania dopasowanej pary może spowodować wystąpienie błędu i nieoczekiwane zamknięcie systemu. Aby zmienić konfigurację wysokiej mocy na konfigurację niskiej mocy lub odwrotnie, należy wyłączyć system.

Wskaźniki dysku

dioda LED	Opis
Miga na zielono dwa razy na sekundę	Trwa identyfikowanie dysku lub przygotowywanie go do usunięcia.
Wył.	Dysk jest gotowy do wyjęcia. Uwaga Wskaźnik stanu dysku pozostaje wyłączony do momentu zainicjowania wszystkich dysków po włączeniu zasilania systemu. W tym czasie dyski nie są gotowe do wyjęcia.
Miga na zielono, a następnie wyłącza się	Wystąpił nieoczekiwany błąd dysku.
Miga na bursztynowo cztery razy na sekundę	Dysk uległ awarii.
Powoli miga na zielono	Dysk się odbudowuje.

Światło ciągle zielone	Dysk jest w trybie online.
Miga na zielono przez trzy sekundy, na bursztynowo przez trzy sekundy, a następnie wyłącza się po sześciu sekundach.	Odbudowywanie zostało zatrzymane.

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.

T10177844_pl

2026-07 (M7.2)

© 2022 – 2026 Axis Communications AB