AXIS Device Manager Extend

Podręcznik użytkownika

Spis treści

Informacje 3
Informacje o organizacjach 4
Informacje o rozwiązaniu 5
Wymagania wstępne 10
Od czego zacząć 12
    Rejestrowanie konta My Axis 12
    Instalowanie klienta i aktywowanie konta 12
    Utwórz organizację 12
    Instalowanie hosta brzegowego 12
    Przypisanie hosta brzegowego 12
Zarządzaj urządzeniami 14
    Dodawanie wykrytych urządzeń do hosta brzegowego 14
        Dodawanie urządzeń z adresów IP 14
        Dodaj urządzenia z zakresu IP 14
        Dodawanie urządzeń z pliku 14
    Usuń urządzenia 15
    Logowanie do urządzeń 15
Konfiguracja 16
    Aktywowanie dostępu zdalnego 16
    Usuwanie lokalizacji 16
    Dodawanie użytkowników do organizacji 16
    Informacje o rolach użytkowników 16
    Podnoszenie roli użytkownika 17
    Usuń użytkowników 17
Zarządzanie systemem operacyjnym AXIS OS 18
    Zarządzanie wersjami systemu AXIS OS na podstawie modelu 18
    Zarządzanie systemem AXIS OS na hoście brzegowym 18
    Wyświetlanie trwających i ukończonych aktualizacji systemu AXIS OS 18
Zasady 19
    Tworzenie i stosowanie zasady zabezpieczeń 19
    Tworzenie i stosowanie zasady dotyczącej aplikacji 19
    Edytowanie zasady 20
    Usuwanie zasady 20
Zarządzaj licencjami 21
    Licencjonowanie produktu 21
Rozwiązywanie problemów – 22
    Konfigurowanie ustawień zapory 22

Informacje

Rozwiązanie AXIS Device Manager Extend zapewnia administratorom systemów interfejs do wykrywania, konfigurowania i obsługi urządzeń Axis w sieciach ich organizacji.

Aplikacja komputerowa AXIS Device Manager Extend

Aplikacja komputerowa to program narzędziowy, który może być używany jako dostępny na żądanie lub przez cały czas interfejs użytkownika do zarządzania systemem. Można ją uruchomić na dedykowanym komputerze wraz z lokalnie zainstalowanym hostem brzegowym lub niezależnie od niego na zdalnie podłączonym laptopie. Klient przedstawia użytkownikowi ogólny stan systemu, dzięki czemu może on podjąć działania związane z zarządzaniem.

Host brzegowy

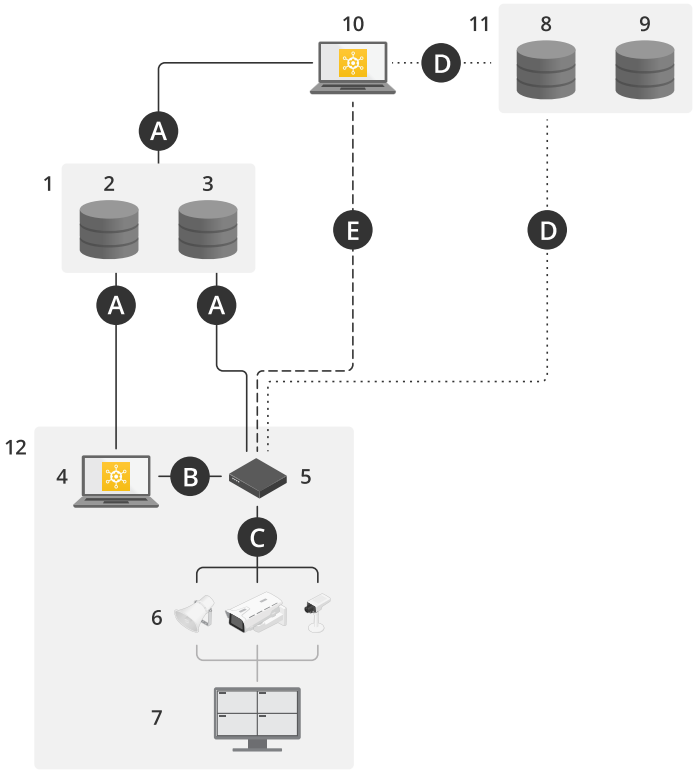
Komponent hosta brzegowego w aplikacji AXIS Device Manager Extend to zawsze dostępna lokalna usługa zarządzania, która jest odpowiedzialna za obsługę urządzeń lokalnych, takich jak kamery. Host brzegowy AXIS Device Manager Extend działa również jako łącze do usługi zdalnego zarządzania Axis, w przypadku której ta sama funkcjonalność API umożliwia zdalną administrację lokalizacjami za pośrednictwem platformy usług Axis.

Informacje o organizacjach

Organizacja jest wirtualną reprezentacją instalacji systemu Axis i centrum Twoich usług chmurowych. Organizacja przechowuje wszystkie urządzenia i konta użytkowników należące do przedsiębiorstwa w usystematyzowanej hierarchii, która umożliwia regulowanie dostępu i zapewnia maksymalne bezpieczeństwo. Jednocześnie pozwala na elastyczne zarządzanie użytkownikami i urządzeniami zarówno w małych firmach, jak i dużych korporacjach.

- Osoba tworząca nową organizację staje się jej właścicielem. Organizacja łączy system przedsiębiorstwa z użytkownikami w usłudze chmurowej Axis.
- Do organizacji można zapraszać użytkowników. Zobacz *Dodawanie użytkowników do organizacji, on page 16*.
- Użytkownikom można przypisywać różne role.
- Organizacja zawiera domyślny folder, w którym można rozpocząć tworzenie struktury organizacyjnej odpowiadającej konkretnym potrzebom. Organizację można podzielić na foldery i podfoldery. Z reguły folder odzwierciedla obiekt lub lokalizację fizyczną systemu w obrębie organizacji.
- W organizacji można zarządzać licencjami na system.
- Aby utworzyć organizację, musisz mieć konto My Axis.

Informacje o rozwiązaniu

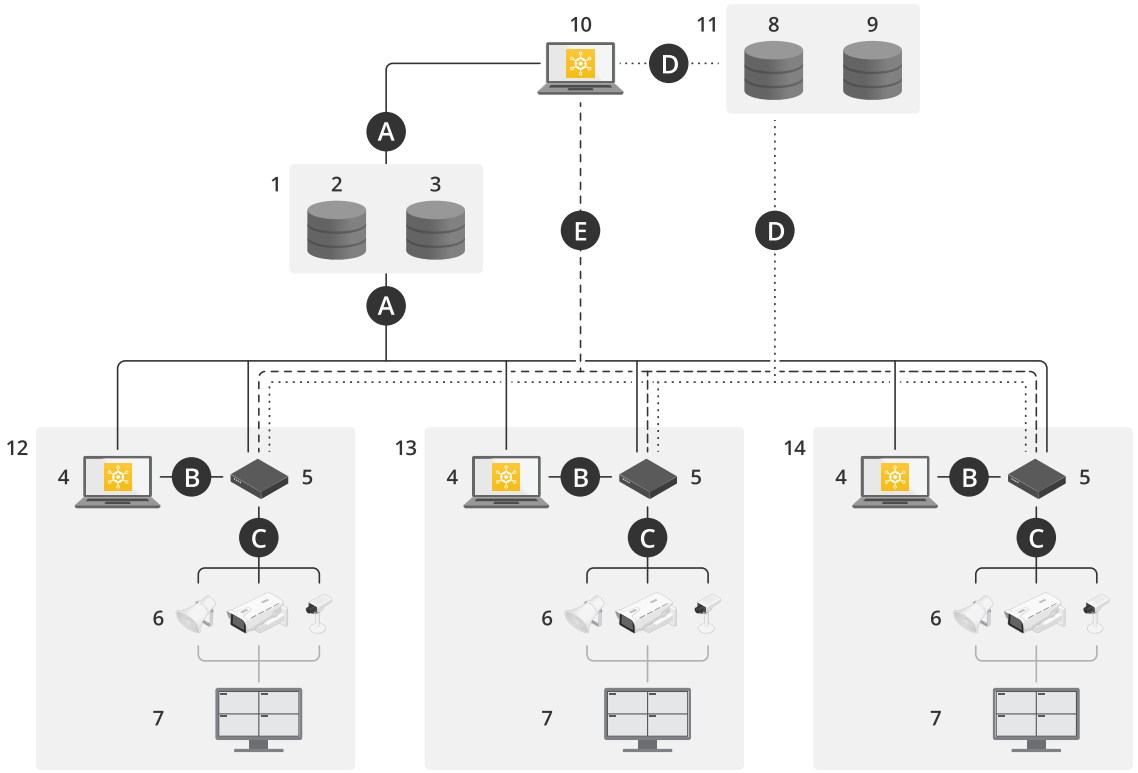


AXIS Device Manager Extend z dostępem lokalnym i zdalnym

1 *Axis*
2 *IAM (My Axis)*
3 *Dane firmy lub instytucji*
4 *Klient lokalny*
5 *Host brzegowy*
6 *Urządzenia*
7 *VMS*
8 *TURN*
9 *Sygnalizacja*
10 *Klient zdalny*
11 *Serwery zdalnego dostępu WebRTC*
12 *Lokalizacja 1*

Połą-czenie	Adres URL i IP	Port	Protokół	Uwagi
A	prod.adm.connect.axis.com, cep.connect.axis.com (52.224.128.152, 40.127.155.231, 75.2.119.140, 99.83.133.42)	443, 8443	HTTPS	Wymagane
B	Wykrywanie HTTP (od klienta do hostów brzegowych) Transfer danych (pomiędzy klientem a hostami brzegowymi). Wykrywanie Multicast (od klienta do hostów brzegowych)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Potrzebne do zainicjowania lokalizacji. Opcjonalne po zainicjowaniu.

	Wykrywanie Multicast (od hostów brzegowych do klienta)			
C	Przesyłanie danych (między hostem brzegowym i urządzeniami) Wykrywanie unicast Wykrywanie multicast Wykrywanie HTTP	80 / port niestandardowy, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	Wymagane
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS, DTLS (UDP i TCP)	W oparciu o standard WebRTC Opcjonalne i domyślnie ustawione jako wyłączone
E	Peer-to-Peer (P2P)	49152–65535	DTLS (UDP i TCP)	

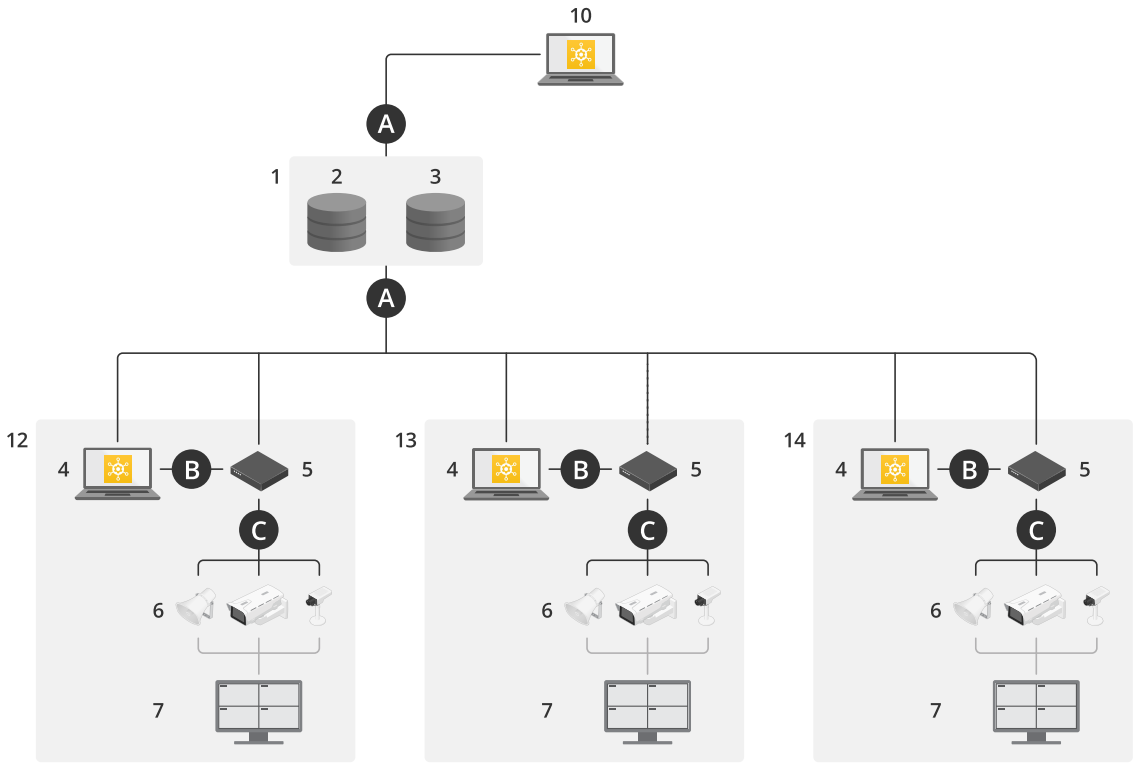


AXIS Device Manager Extend w konfiguracji wielostanowiskowej z wykorzystaniem lokalnego i zdalnego dostępu

1 *Axis*
2 *IAM (My Axis)*
3 *Dane firmy lub instytucji*
4 *Klient lokalny*
5 *Host brzegowy*
6 *Urządzenia*
7 *VMS*
8 *TURN*
9 *Sygnalizacja*
10 *Klient zdalny*
11 *Serwery zdalnego dostępu WebRTC*

12 Lokalizacja 1
13 Lokalizacja 2
14 Lokalizacja 3

Połą-czenie	Adres URL i IP	Port	Protokół	Uwagi
A	prod.adm.connect.axis.com, cep.connect.axis.com (52.224.128.152, 40.127.155.231, 75.2.119.140, 99.83.133.42)	443, 8443	HTTPS	Wymagane
B	Wykrywanie HTTP (od klienta do hostów brzegowych) Transfer danych (pomiędzy klientem a hostami brzegowymi). Wykrywanie Multicast (od klienta do hostów brzegowych) Wykrywanie Multicast (od hostów brzegowych do klienta)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Potrzebne do zainicjowania lokalizacji. Opcjonalne po zainicjowaniu.
C	Przesyłanie danych (między hostem brzegowym i urządzeniami) Wykrywanie unicast Wykrywanie multicast Wykrywanie HTTP	80 / port niestandar-dowy, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	Wymagane
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS, DTLS (UDP i TCP)	W oparciu o standard WebRTC Opcjonalne i domyślnie ustawione jako wyłączone
E	Peer-to-Peer (P2P)	49152–65535	DTLS (UDP i TCP)	



AXIS Device Manager Extend z dostępem lokalnym i zdalnym przez VPN

1 *Axis*
2 *IAM (My Axis)*
3 *Dane firmy lub instytucji*
4 *Klient lokalny*
5 *Host brzegowy*
6 *Urządzenia*
7 *VMS*
8 *TURN*
9 *Sygnalizacja*
10 *Klient zdalny*
11 *Serwery zdalnego dostępu WebRTC*
12 *Lokalizacja 1*
13 *Lokalizacja 2*
14 *Lokalizacja 3*

Połą-czenie	Adres URL i IP	Port	Protokół	Uwagi
A	prod.adm.connect.axis.com, cep.connect.axis.com (52.224.128.152, 40.127.155.231, 75.2.119.140, 99.83.133.42)	443, 8443	HTTPS	Wymagane
B	Wykrywanie HTTP (od klienta do hostów brzegowych) Transfer danych (pomiędzy klientem a hostami brzegowymi). Wykrywanie Multicast (od klienta do hostów brzegowych)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Potrzebne do zainicjowania lokalizacji. Opcjonalne po zainicjowaniu.

	Wykrywanie Multicast (od hostów brzegowych do klienta)			
C	Przesyłanie danych (między hostem brzegowym i urządzeniami) Wykrywanie unicast Wykrywanie multicast Wykrywanie HTTP	80 / port niestandardowy, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	Wymagane
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS, DTLS (UDP i TCP)	W oparciu o standard WebRTC Opcjonalne i domyślnie ustawione jako wyłączone
E	Peer-to-Peer (P2P)	49152–65535	DTLS (UDP i TCP)	

- Dodatkowym wymaganiem jest publiczny DNS, na przykład Google DNS: 8.8.8.8 / 8.8.4.4 lub Cloudflare DNS: 1.1.1.1
- Do zapewnienia pełnej funkcjonalności systemu AXIS Device Manager Extend potrzebne są oba połączenia — A i C.
- Obecnie jesteśmy na etapie rozwoju aplikacji, dlatego zalecamy, aby zezwolić aplikacji AXIS Device Manager Extend i wszystkim kontrolerom lokalizacji na dostęp przez zaporę do dowolnego hosta brzegowego.

Wymagania wstępne

Zgodne systemy operacyjne:

- Windows 10 Pro i Enterprise
- Windows 11 Pro i Enterprise
- Windows Server 2016, 2019 i 2022 (system bazujący na architekturze x64)
- W celu instalacji i wprowadzania zmian w konfiguracji wymagane jest uprawnienie administratora systemu.

Minimalne zalecenia dotyczące systemu:

- Procesor: Intel Core i5
- Pamięć RAM: 4 GB
- Sieć: 100 Mb/s

Łączność internetowa

Uwaga

Aplikacja AXIS Device Manager Extend wymaga zapewnienia łączności z Internetem przy użyciu certyfikatów potwierdzających jej przynależność do organizacji, które zostały utworzone za pomocą konta My Axis użytego podczas instalacji i skojarzone z tym kontem. Jednak w celu korzystania z niektórych funkcji, takich jak informacje o gwarancji i wsparcie dla wielu lokalizacji, wymagane jest połączenie z Internetem. Ponadto klient i/lub host brzegowy aktualizuje się automatycznie tylko w trybie online.

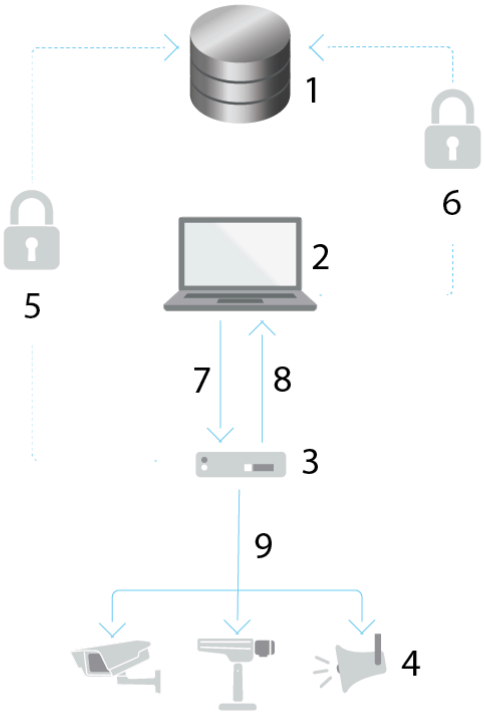
Zsynchronizowana godzina i data

Uwaga

Upewnij się, że wszystkie komponenty systemu są zsynchronizowane — w przeciwnym razie uwierzytelnienie certyfikatu pomiędzy hostem brzegowym a klientem lub zapleczem może się nie powieść. Zaleca się, aby wszystkie urządzenia-hosty były zsynchronizowane ze wspólnym sieciowym serwerem czasu, aby uniknąć potencjalnych problemów.

Otwarte porty sieciowe:

do bezpiecznych połączeń z aplikacji komputerowej AXIS Device Manager Extend do hosta brzegowego, wykrywania hosta brzegowego i usługi Axis Remote Service.



1 Axis Service Platform
2 Aplikacja komputerowa AXIS Device Manager Extend
3 Host brzegowy
4 Urządzenia
5 HTTPS (port 443)
6 HTTPS (port 443)
7 HTTPS (port 37443), wykrywanie UDP Multicast (port 6801), wykrywanie HTTP (port 37080)
8 Wykrywanie UDP Multicast (port 6801)
9 HTTPS i HTTP (port 443 i 80), wykrywanie Multicast —SSDP (port 1900) — Bonjour (port 5353), wykrywanie Unicast (port 1900), wykrywanie HTTP (port 80 i 443)

Wychodzące połączenia sieciowe

Obecnie jesteśmy na etapie rozwoju aplikacji, dlatego zalecamy, aby zezwolić aplikacji AXIS Device Manager Extend i wszystkim kontrolerom lokalizacji na dostęp przez zaporę do dowolnego hosta brzegowego.

Od czego zacząć

Rejestrowanie konta My Axis

1. Zarejestruj konto **MyAxis** na stronie *axis.com/my-axis/login*.
2. Wybierz jedną z metod uwierzytelniania wieloskładnikowego (MFA) **Authenticator App (TOTP) (Aplikacja uwierzytelniająca (TOTP))** lub **Email (E-mail)** i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie. MFA to system zabezpieczeń, który dodaje kolejną warstwę weryfikacji w celu potwierdzenia tożsamości użytkownika.

Instalowanie klienta i aktywowanie konta

Przejdź do strony produktu w witrynie axis.com i pobierz klienta Axis Device Management.

1. Odszukaj miejsce, w którym została zapisana aplikacja, a następnie kliknij ją i wybierz opcję instalacji.
2. Wybierz **klienta** i kliknij opcję **Install (Zainstaluj)**.
3. Zaloguj się na swoje konto My Axis.
4. Potwierdź swój adres e-mail, aby ukończyć aktywację.
5. Utwórz organizację lub dołącz do istniejącej organizacji.

Utwórz organizację

Aby dodawać urządzenia do systemu, musisz należeć do organizacji. Takie rozwiązanie umożliwia bezpieczne utrzymywanie i ochronę urządzeń w jednej lub wielu lokalizacjach. Jeśli jeszcze nie należysz do organizacji, pojawi się asystent konfiguracji, który przeprowadzi Cię przez cały proces.

Aby utworzyć organizację:

1. Zaloguj się przy użyciu konta My Axis.
2. Postępuj zgodnie z instrukcjami asystenta konfiguracji.

Aby utworzyć dodatkowe organizacje:

- Przejdź do menu rozwijanego z nazwą Twojej organizacji.
- Wybierz **+ Create new organization (Utwórz nową organizację)**.
- Postępuj zgodnie z instrukcjami asystenta konfiguracji.

Instalowanie hosta brzegowego

Przejdź do strony produktu w witrynie axis.com i pobierz host brzegowy (Axis Device Management Server)..

1. Wybierz serwer, na którym chcesz zainstalować hosta brzegowego. Zalecamy zainstalowanie hosta brzegowego na serwerze znajdującym się jak najbliżej urządzeń.
2. Uruchom instalator w serwerze.

Przypisanie hosta brzegowego

Aby utworzyć bezpieczne połączenie z urządzeniami z poziomu klienta Axis Device Management, należy najpierw przypisać host brzegowy do organizacji.

1. Kliknij hosta brzegowego ze statusem **Unclaimed (Nieprzypisany)**
   1.1. Kliknij opcję **Add new edge host (Dodaj nowego hosta brzegowego)**, jeśli na liście nie ma jeszcze żadnego hosta brzegowego.
   1.2. Wpisz adres IP lokalizacji hosta brzegowego
2. Wpisz nazwę hosta brzegowego

3. Dodaj opcjonalny opis (zalecane).
4. Kliknij opcję **Claim edge host (Przypisz hosta brzegowego)**

Zarządzaj urządzeniami

Dodawanie wykrytych urządzeń do hosta brzegowego

1. Przejdź do menu **Edge hosts (Hosty brzegowe)**.
2. Wybierz żądanego hosta brzegowego z listy, do której chcesz dodać urządzenia.
3. Przejdź do menu **Devices > Discovered (Urządzenia > Wykryte)**.
4. Wybierz urządzenia, które chcesz dodać, lub wybierz wszystkie urządzenia, zaznaczając pole u góry kolumny wyboru.
5. Kliknij polecenie **Add devices to edge host (Dodaj urządzenia do hosta brzegowego)** .

Urządzenia znajdują się teraz na karcie **Managed (Zarządzane)**, a ich status można sprawdzić w menu **Edge host overview (Host brzegowy: przegląd)**.

Dodawanie urządzeń z adresów IP

Można dodawać urządzenia, które nie są automatycznie wykrywane z podsieci, indywidualnych adresów IP lub zakresu adresów IP.

Dodaj urządzenia z zakresu IP

1. Przejdź do hosta brzegowego przypisanego do Twojej organizacji.
2. Przejdź do menu **Settings > Device discovery (Ustawienia > Wykrywanie urządzeń)**.
3. Kliknij polecenie **Add by IP (Dodaj na podstawie adresu IP)**
4. Wybierz opcję **Manual entry (Wprowadzanie ręczne)**
5. Wpisz zakres adresów IP
6. Kliknij przycisk **Add IP addresses (Dodaj adresy IP)**
7. Przejdź do obszaru **Devices (Urządzenia) > Discovered (Wykryte)**.
8. Wybierz urządzenia, które chcesz dodać, lub wybierz wszystkie urządzenia, zaznaczając pole u góry kolumny wyboru.
9. Kliknij opcję **Add devices (Dodaj urządzenia)** .

Dodawanie urządzeń z pliku

1. Przejdź do hosta brzegowego przypisanego do Twojej organizacji.
2. Przejdź do menu **Settings > Device discovery (Ustawienia > Wykrywanie urządzeń)**.
3. Kliknij polecenie **Add by IP (Dodaj na podstawie adresu IP)**
4. Kliknij opcję **Import from file (Importuj z pliku)**.
5. Wybierz plik o wartościach rozdzielanych przecinkami (.CSV) zawierający adresy IP
6. Kliknij przycisk **Import (Importuj)**
7. Przejdź do menu **Devices > Discovered devices (Urządzenia > Wykryte urządzenia)**.
8. Wybierz urządzenia, które chcesz dodać, lub wybierz wszystkie urządzenia, zaznaczając pole u góry kolumny wyboru.
9. Kliknij opcję **Add devices (Dodaj urządzenia)** .

Uwaga

Plik powinien zawierać:

Nagłówek kolumny adresów IP

Pojedynczą kolumnę

maksymalnie 25 600 adresów IP.

Usuń urządzenia

1. Kliknij pozycję **Edge host (Host brzegowy)**
2. Wybierz hosta brzegowego.
3. Przejdź do opcji **Devices (Urządzenia)**.
4. Wybierz urządzenia, które chcesz usunąć, lub wybierz wszystkie urządzenia, zaznaczając pole u góry kolumny wyboru.
5. W menu kliknij ikonę **Remove devices from edge host (Usuń urządzenia z hosta brzegowego)**.
6. Kliknij przycisk **Remove (Usuń)**.

Usunięte urządzenia można znaleźć w obszarze **Devices >Discovered (Urządzenia > Wykryte)**.

Logowanie do urządzeń

1. Kliknij pozycję **Edge hosts (Hosty brzegowe)**
2. Wybierz hosta brzegowego.
3. Przejdź do menu **Devices > Managed (Urządzenia > Zarządzane)**
4. Wybierz urządzenia, do których chcesz uzyskać dostęp, lub wybierz wszystkie urządzenia, zaznaczając pole u góry kolumny wyboru.
5. Kliknij opcję **Log in (Zaloguj się)**, aby automatycznie zalogować się na wielu urządzeniach.
6. Wprowadź nazwę użytkownika i hasło.
7. Kliknij przycisk **Login (Zaloguj)**

Uwaga

Jeżeli nazwa użytkownika i hasło są prawidłowe, przy pozycji **Status (Stan)** będzie widoczny komunikat **Reachable (Osiągalne)**.

Konfiguracja

Aktywowanie dostępu zdalnego

Jeśli ustawienia zapory blokują połączenia wychodzące, może być konieczne wprowadzenie połączenia proxy w celu uzyskania zdalnego dostępu do lokalizacji.

1. Wybierz hosta brzegowego, dla którego chcesz uaktywnić funkcję zdalnego dostępu.
2. Przejdź do menu **Settings >Edge hosts connections (Ustawienia >Połączenia hostów brzegowych)**.
3. Włącz **Allow remote access to edge host (Zezwalaj na zdalny dostęp do hosta brzegowego)**.
4. W razie konieczności wprowadzenia adresu serwera proxy w celu połączenia z Internetem, wpisz odpowiedni adres w polu **Proxy address (Adres serwera proxy)**.

Po aktywowaniu połączenia zostanie wyświetlone powiadomienie.

Uwaga

Aby zapewnić obsługę połączenia z hostami brzegowymi w innych sieciach, konieczne może być dodanie następującej konfiguracji do „listy dozwolonych" w zaporze w sieci firmowej: Endpoint Port Protocol signaling.prod.webrtc.connect.axis.com 443 HTTPS *.turn.prod.webrtc.connect.axis.com 443 HTTPS webRTC (Turn i P2P) 5349, 49152 - 65535 DTLS (UDP i TCP)

Usuwanie lokalizacji

Przed usunięciem hosta brzegowego z organizacji należy *Usuń urządzenia, on page 15* należące do hosta brzegowego. Usunięte urządzenia można znaleźć w obszarze **Devices > Discovered (Urządzenia > Wykryte)**.

1. Kliknij pozycję **Edge hosts (Hosty brzegowe)**.
2. Wybierz hosta brzegowego przy użyciu przycisków strzałek lub umieść nad nim wskaźnik myszy.
3. Kliknij pozycję **...** i z rozwijalnego menu wybierz opcję **Remove edge host (Usuń hosty brzegowe)**.
4. Zaznacz pole wyboru **I'm aware of the risks (Mam świadomość zagrożeń)**.
5. Kliknij przycisk **Remove (Usuń)**.

Dodawanie użytkowników do organizacji

1. Wybierz organizację, w której chcesz skonfigurować ustawienia użytkownika.
2. Przejdź do panelu My Systems (Moje systemy).
3. Przejdź do obszaru **ORGANIZATION (Organizacja) > Users (Użytkownicy)**.
4. Kliknij przycisk **Invite users (Zaproś użytkowników)**.
5. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie przez asystenta instalacji.
   - Jeśli została wybrana opcja **Operator** lub **Viewer (Dozorca)**, wybierz foldery, do których użytkownicy będą mieli dostęp. Pamiętaj, że użytkownicy z rolą **Admin (Administrator)** mają dostęp do wszystkich folderów w organizacji.

Uwaga

Użytkownik otrzyma wiadomość e-mail z zaproszeniem, którą może wykorzystać do zalogowania się w oknie My Systems (Moje systemy). Jeśli użytkownik nie ma konta My Axis, musi użyć tej wiadomości e-mail do zarejestrowania się w celu uzyskania dostępu do organizacji. Zaproszenia można cofnąć podczas oczekiwania na ich przyjęcie.

Informacje o rolach użytkowników

Role użytkowników określają stopień dostępu użytkownika do systemów w organizacji. Dostępne funkcje różnią się w zależności od roli użytkownika.

Admin

Administratorzy mają dostęp do całego systemu. Obejmuje to zarządzanie użytkownikami, urządzeniami, licencjami, plikami wideo i inną zawartością.

Administratorzy mogą również dołączać urządzenia za pomocą systemu AXIS Camera Station Pro. Administratorzy mogą zarządzać monitorowaniem serwera AXIS Camera Station Pro w oknie My Systems (Moje systemy).

Operator

Operatorzy mogą monitorować obraz wideo na żywo, sterować urządzeniami i uzyskiwać dostęp do nagrań w celu odtwarzania. Uzyskują przegląd użytkowników w organizacji i ich ról. Operatorzy mogą również zarządzać monitorowaniem serwera AXIS Camera Station Pro w oknie My Systems (Moje systemy).

Dozorca

Dozorcy mogą monitorować transmisję wideo na żywo, ale nie mogą kontrolować urządzeń ani uzyskiwać dostępu do nagrań. Uzyskują przegląd użytkowników w organizacji i ich ról.

Podnoszenie roli użytkownika

1. Wybierz organizację, w której chcesz skonfigurować ustawienia użytkownika.
2. Przejdź do panelu My Systems (Moje systemy).
3. W obszarze **ORGANIZATION (Organizacja)** przejdź do pozycji **Users (Użytkownicy)**.
4. Kliknij użytkownika, którego rolę chcesz podnieść, i kliknij **Roles and access (Role i dostęp)**.
5. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie przez asystenta instalacji.

Uwaga

Rola zostanie zmieniona bezpośrednio po jej wybraniu. Ze względów bezpieczeństwa zaproszenia są ograniczone do roli dozorcy.

Usuń użytkowników

1. Wybierz organizację, w której chcesz skonfigurować ustawienia użytkownika.
2. Przejdź do panelu My Systems (Moje systemy).
3. W obszarze **ORGANIZATION (Organizacja)** przejdź do pozycji **Users (Użytkownicy)**.
4. Po najechaniu wskaźnikiem myszy na użytkownika, którego chcesz usunąć, zostanie wyświetlone nowe menu opcji: **...**
5. Kliknij pozycję **...** i wybierz opcję **Remove user (Usuń użytkownika)** z rozwijalnego menu.

Usuwanie wielu użytkowników

1. Wybierz użytkowników, których chcesz usunąć.
2. Kliknij kosz w menu akcji.
3. Kliknij przycisk **Remove (Usuń)**.

Zarządzanie systemem operacyjnym AXIS OS

Klient Axis Device Management umożliwia zarządzanie systemami operacyjnymi wielu urządzeń w każdej organizacji.

Lista aktualizacji systemu AXIS OS dostępnych dla każdego urządzenia w organizacji, pogrupowanych według modelu, znajduje się w obszarze **Home (Strona główna) > AXIS OS versions (Wersje systemu AXIS OS)**. Aby zapoznać się z listą aktualizacji systemu AXIS OS dostępnych na określonym hoście brzegowym, zaznacz hosta brzegowego i przejdź do obszaru **AXIS OS inventory (Spis systemu AXIS OS)**.

Zarządzanie wersjami systemu AXIS OS na podstawie modelu

Zarządzanie systemem AXIS OS według modelu w całej organizacji:

1. Wybierz kolejno opcje **Home > AXIS OS versions (Strona główna > Wersje systemu operacyjnego AXIS OS)**
2. Kliknij łącze zalecanej wersji systemu AXIS OS. Spowoduje to otwarcie opcji aktualizacji systemu AXIS OS.
3. Kliknij rozwijalne menu **Upgrade to (Zaktualizuj do)**, aby wyświetlić dostępne możliwości. Wstępnie zostanie wybrana najnowsza wersja systemu AXIS OS.
4. Kliknij polecenie **Upgrade (Aktualizuj)**.

Zarządzanie systemem AXIS OS na hoście brzegowym

Aby zarządzać systemem AXIS OS na niektórych lub wszystkich urządzeniach dodanych do hosta brzegowego:

1. Przejdź do menu **Edge hosts (Hosty brzegowe)**
2. Kliknij hosta brzegowego, do którego chcesz uzyskać dostęp.
3. Przejdź do opcji **Devices (Urządzenia)**
4. Zaznacz wszystkie urządzenia lub tylko te, którymi chcesz zarządzać.
5. Kliknij ikonę **AXIS OS** w menu akcji.
6. Zaznacz wszystkie lub wybrane modele na liście.
7. Jeżeli chcesz zmienić wersję systemu AXIS OS, kliknij sugerowaną wersję, a zobaczysz możliwości dostępne dla każdego urządzenia. Wstępnie zostanie wybrana najnowsza wersja systemu AXIS OS.
8. Kliknij **Aktualizuj**.

Wyświetlanie trwających i ukończonych aktualizacji systemu AXIS OS

Aby wyświetlić trwające aktualizacje oprogramowania urządzeń podłączonych do określonego hosta brzegowego:

1. Kliknij pozycję **Edge hosts (Hosty brzegowe)**.
2. Kliknij hosta brzegowego, do którego chcesz uzyskać dostęp.
3. Przejdź do obszaru **Log (Dziennik)**.

Aby zobaczyć trwające aktualizacje oprogramowania:

4. Przejdź do obszaru **Log (Dziennik) > Ongoing tasks (Trwające zadania)**.

Zasady

Zasady służą do automatycznego zarządzania urządzeniami. Tworząc zasady, można sprawnie zarządzać cyberbezpieczeństwem w całej lokalizacji. Można również skonfigurować zasadę powodującą automatyczne instalowanie i aktualizowanie aplikacji na urządzeniach.

Tworzenie i stosowanie zasady zabezpieczeń

W tym przykładowym przypadku użycia utworzymy i zastosujemy podstawową zasadę zabezpieczeń do wybranej liczby urządzeń połączonych z hostem brzegowym.

Tworzenie podstawowej zasady zabezpieczeń:

1. Przejdź do menu **Edge hosts (Hosty brzegowe)**
2. Kliknij hosta brzegowego, do którego chcesz uzyskać dostęp.
3. Przejdź do opcji **Devices (Urządzenia)**
4. Kliknij ikonę **+** obok pozycji **Policies (Zasady)**
5. Zaznacz opcję **Basic security (Podstawowe zabezpieczenia)** i kliknij przycisk **Continue (Kontynuuj)**
6. Nazwij zasadę
7. Zaznacz ustawienia spełniające potrzeby Twojej firmy w zakresie bezpieczeństwa. Aby używać zalecanego poziomu bezpieczeństwa, pozostaw domyślne ustawienie.
   - Aby zmienić hasło główne dla wybranych urządzeń, kliknij przycisk **Device root password (Główne hasło urządzenia)** i wpisz nowe hasło główne.
8. Kliknij polecenie **Create (Utwórz)**.

Nadawanie nazwy zasadzie:

1. Zaznacz urządzenia, do których chcesz zastosować zasadę.
2. Kliknij ikonę **Policy options (Opcje zasad)** w menu akcji.
3. Zaznacz zasadę zabezpieczeń i kliknij przycisk **Save (Zapisz)**.

Tworzenie i stosowanie zasady dotyczącej aplikacji

W tym przykładowym przypadku użycia utworzymy i zastosujemy zasadę aplikacji do wybranej liczby urządzeń połączonych z hostem brzegowym.

1. Przejdź do menu **Edge hosts (Hosty brzegowe)**
2. Kliknij hosta brzegowego, do którego chcesz uzyskać dostęp.
3. Przejdź do opcji **Devices (Urządzenia)**
4. Kliknij ikonę **+** obok pozycji **Policies (Zasady)**
5. Zaznacz opcję **Apps (Aplikacje)** i kliknij przycisk **Continue (Kontynuuj)**
6. Nazwij zasadę
7. Zaznacz aplikacje, które chcesz zainstalować i zaktualizować na urządzeniach.
8. W menu rozwijanym kliknij okno aktualizacji.
9. Kliknij polecenie **Create (Utwórz)**.

Nadawanie nazwy zasadzie:

1. Zaznacz urządzenia, do których chcesz zastosować zasadę.
2. Kliknij ikonę **Policy options (Opcje zasad)** w menu akcji.
3. Zaznacz zasadę dotyczącą aplikacji, którą chcesz zastosować.
4. Kliknij przycisk **Zapisz**.

Uwaga

Zaznaczone aplikacje w razie usunięcia zostaną automatycznie ponownie zainstalowane.

Edytowanie zasady

Aby edytować istniejącą zasadę:

1. Przejdź do menu **Edge hosts (Hosty brzegowe)**
2. Kliknij hosta brzegowego, do którego chcesz uzyskać dostęp.
3. Przejdź do opcji **Devices (Urządzenia)**
4. Kliknij przycisk **...** obok zasady, którą chcesz edytować, a następnie z menu rozwijanego wybierz polecenie **Edit policy (Edytuj zasadę)**.
5. Edytuj ustawienia zasad, dopasowując konfigurację do własnych potrzeb.
6. Kliknij przycisk **Zapisz**

Usuwanie zasady

Aby usunąć istniejącą zasadę:

- Przejdź do menu **Edge hosts (Hosty brzegowe)**
- Kliknij hosta brzegowego, do którego chcesz uzyskać dostęp.
- Przejdź do opcji **Devices (Urządzenia)**
- Kliknij przycisk **...** obok zasady, którą chcesz edytować, a następnie z menu rozwijanego wybierz polecenie **Delete policy (Usuń zasadę)**.
- Kliknij przycisk **Delete (Usuń)**

Uwaga

Wszystkie urządzenia, do których ta zasada została zastosowana, zachowują ustawienia zasady, ale ustawienia te nie będą już nadrzędne.

Zarządzaj licencjami

Licencjonowanie produktu

Aby uzyskać licencję na produkt, przejdź do obszaru *My Systems (Moje systemy) > Licenses (Licencje)*. Aby dowiedzieć się więcej o licencjach na produkty i usługi Axis, patrz *Instrukcja użytkownika My Systems*.

Rozwiązywanie problemów –

Konfigurowanie ustawień zapory

Klient Axis Device Management wymaga dostępu do domeny axis.com i poddomen.

Aby host brzegowy był w stanie komunikować się z usługami Axis, dodaj następujące adresy IP i porty do listy zezwoleń zapory sieciowej w organizacji:

- 40.127.155.231 (EU), port 443
- 52.224.128.152 i 40.127.155.231 (US), port 443
- 75.2.119.140, port 443 i 8443
- 99.83.133.42, port 443 i 8443

Jako alternatywę można wykorzystać następujące nazwy domen (przekierowujące do powyższych adresów IP):

- prod.adm.connect.axis.com, port 443
- cep.connect.axis.com, port 443 i 8443

Należy również zezwolić na ruch DNS dla adresu IP serwera DNS oraz domyślnego portu 53

Uwaga

Dalsze informacje na temat konfiguracji portów znajdują się w białej księdze aplikacji AXIS Device Manager Extend: *Typowe konfiguracje systemu*.

T10153497_pl

2026-04 (M23.2)