

AXIS Device Manager Extend

Podręcznik użytkownika

AXIS Device Manager Extend

Spis treści

O programie	3
Informacje o rozwiązaniu	4
Wymogi wstępne	7
Rozpoczynanie pracy	9
Rejestrowanie konta My Axis	9
Instalowanie klienta i aktywowanie konta	9
Instalowanie hosta na krawędzi systemu	10
Przypisanie hosta na krawędzi systemu	10
Zarządzaj urządzeniami	11
Dodawanie wykrytych urządzeń do hosta na krawędzi systemu	11
Usuń urządzenia	12
Logowanie do urządzeń	12
Konfiguracja	13
Aktywowanie dostępu zdalnego	13
Usuwanie lokalizacji	13
Dodawanie użytkowników do organizacji	13
Podnoszenie roli użytkownika	13
Usuwanie użytkowników	14
Zarządzanie oprogramowaniem sprzętowym	15
Zarządzanie oprogramowaniem sprzętowym z podziałem na modele urządzeń	15
Zarządzaj oprogramowaniem sprzętowym urządzenia na hoście na krawędzi systemu.	15
Wyświetlanie trwających i zakończonych aktualizacji oprogramowania sprzętowego	15
Policies (Polityki)	16
Tworzenie i stosowanie zasady zabezpieczeń	16
Tworzenie i stosowanie zasady dotyczącej aplikacji	16
Edytowanie zasady	17
Usuwanie zasady	17
Rozwiązywanie problemów	18
Konfigurowanie ustawień zapory	18

AXIS Device Manager Extend

O programie

O programie

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 na krawędzi systemu lub niezależnie od niego na zdalnie podłączonym laptopie. Klient przedstawia użytkownikowi ogólny stan systemu, dzięki czemu może on podjąć działania związane z zarządzaniem.

Host na krawędzi systemu

Komponent hosta na krawędzi systemu w aplikacji AXIS Device Manager Extend to zawsze dostępna lokalna usługa zarządzania, która jest odpowiedzialna za obsługę urządzeń lokalnych, takich jak kamery. Host na krawędzi systemu 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.

AXIS Device Manager Extend

Informacje o rozwiązaniu

Informacje o rozwiązaniu

AXIS Device Manager Extend z dostępem lokalnym i zdalnym

- 1 Axis
- 2 IAM (My Axis)
- 3 Dane dotyczące organizacji
- 4 Klient lokalny
- 5 Host na krawędzi systemu
- 6 Urządzenia
- 7 VMS
- 8 TURN
- 9 Sygnalizowanie
- 10 Klient zdalny
- 11 Serwery zdalnego dostępu WebRTC
- 12 Obiekt 1

Połączenie	Adres URL i IP	Port	Protokół	Uwaga
A	prod.adm.connect.axis.com (52.224.128.152 or 40.127.155.231)	443	HTTPS	Wymagane
B	Wykrywanie HTTP (od klienta do hostów na krawędzi systemu) Transfer danych (pomiędzy klientem a hostami na krawędzi systemu). Wykrywanie Multicast (od klienta do hostów na krawędzi systemu) Wykrywanie Multicast (od hostów na krawędzi systemu do klienta)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Wymagane do zainicjowania obsługi administracyjnej lokalizacji. Opcjonalne po zainicjowaniu obsługi administracyjnej.
C	Transfer danych (między hostem na krawędzi systemu a urządzeniami). Wykrywanie Unicast Wykrywanie Multicast Wykrywanie HTTP	80 / port nie-standardowy, 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 dotyczące organizacji
- 4 Klient lokalny
- 5 Host na krawędzi systemu
- 6 Urządzenia
- 7 VMS
- 8 TURN
- 9 Sygnalizowanie

AXIS Device Manager Extend

Informacje o rozwiązaniu

- 10 Klient zdalny
- 11 Serwery zdalnego dostępu WebRTC
- 12 Obiekt 1
- 13 Obiekt 2
- 14 Obiekt 3

Połączenie	Adres URL i IP	Port	Protokół	Uwaga
A	prod.adm.connect.axis.com (52.224.128.152 or 40.127.155.231)	443	HTTPS	Wymagane
B	Wykrywanie HTTP (od klienta do hostów na krawędzi systemu) Transfer danych (pomiędzy klientem a hostami na krawędzi systemu). Wykrywanie Multicast (od klienta do hostów na krawędzi systemu) Wykrywanie Multicast (od hostów na krawędzi systemu do klienta)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Wymagane do zainicjowania obsługi administracyjnej lokalizacji. Opcjonalne po zainicjowaniu obsługi administracyjnej.
C	Transfer danych (między hostem na krawędzi systemu a urządzeniami). Wykrywanie Unicast Wykrywanie Multicast Wykrywanie HTTP	80 / port nie-standardowy, 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 dotyczące organizacji
- 4 Klient lokalny
- 5 Host na krawędzi systemu
- 6 Urządzenia
- 7 VMS
- 8 TURN
- 9 Sygnalizowanie
- 10 Klient zdalny
- 11 Serwery zdalnego dostępu WebRTC
- 12 Obiekt 1
- 13 Obiekt 2
- 14 Obiekt 3

Połączenie	Adres URL i IP	Port	Protokół	Uwaga
A	prod.adm.connect.axis.com (52.224.128.152 or 40.127.155.231)	443	HTTPS	Wymagane

AXIS Device Manager Extend

Informacje o rozwiązaniu

B	Wykrywanie HTTP (od klienta do hostów na krawędzi systemu) Transfer danych (pomiędzy klientem a hostami na krawędzi systemu). Wykrywanie Multicast (od klienta do hostów na krawędzi systemu) Wykrywanie Multicast (od hostów na krawędzi systemu do klienta)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Wymagane do zainicjowania obsługi administracyjnej lokalizacji. Opcjonalne po zainicjowaniu obsługi administracyjnej.
C	Transfer danych (między hostem na krawędzi systemu a urządzeniami). Wykrywanie Unicast Wykrywanie Multicast Wykrywanie HTTP	80 / port nie-standardowy, 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 na krawędzi systemu.

AXIS Device Manager Extend

Wymogi wstępne

Wymogi 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 kontroler lokalizacji aktualizuje się automatycznie tylko w trybie online.

Zsynchronizowana godzina i data

Uwaga

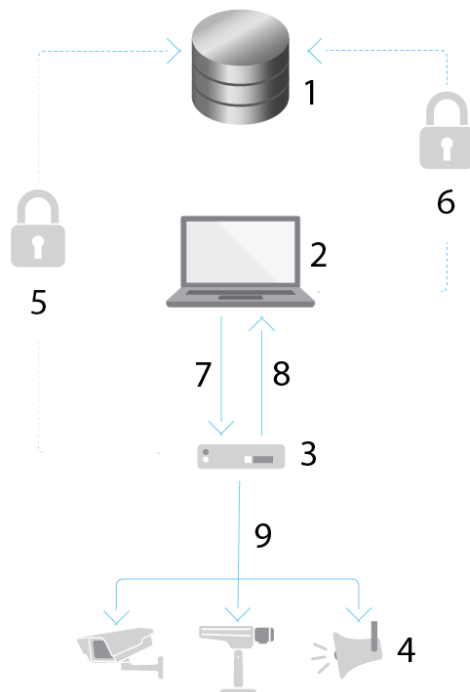
Upewnij się, że wszystkie komponenty systemu są zsynchronizowane – w przeciwnym razie uwierzytelnienie certyfikatu pomiędzy hostem na krawędzi systemu a klientem lub zapleczem może się nie powieść. Zaleca się, aby wszystkie urządzenia-hosty były zsynchronizowane ze wspólnym sieciowym serwerem czasu,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

Otwarte porty sieciowe:

do bezpiecznych połączeń z aplikacji komputerowej AXIS Device Manager Extend desktop do hosta na krawędzi systemu, wykrywania hosta na krawędzi systemu i usługi Axis Remote Service.

AXIS Device Manager Extend

Wymogi wstępne



- 1 *Axis Service Platform*
- 2 *Aplikacja komputerowa AXIS Device Manager Extend*
- 3 *Host na krawędzi systemu*
- 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 na krawędzi systemu.

AXIS Device Manager Extend

Rozpoczynanie pracy

Rozpoczynanie pracy



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

help.axis.com/?Etpiald=63389&tsection=get-started


Instalacja oprogramowania, tworzenie organizacji i dodawanie urządzeń

Rejestrowanie konta My Axis

Zarejestruj konto My Axis na stronie axis.com/my-axis/login.

Możesz zwiększyć bezpieczeństwo swojego konta My Axis, aktywując uwierzytelnianie wieloskładnikowe (MFA). MFA to system zabezpieczeń, który dodaje kolejną warstwę weryfikacji w celu zapewnienia ochrony tożsamości użytkownika.

Aktywowanie uwierzytelniania MFA:

1. Zaloguj się, używając poświadczeń konta My Axis.
2. Przejdź do strony  i kliknij opcję Account settings (Ustawienia konta).
3. Kliknij opcję Security settings (Ustawienia zabezpieczeń)
4. Włącz opcję 2-Step verification (Weryfikacja dwuetapowa).

Nastąpi przekierowanie na stronę logowania.

5. Zaloguj się, używając poświadczeń konta My Axis.

Uwierzytelnianie MFA jest teraz aktywne.

Logowanie przy aktywnym uwierzytelnianiu MFA:

1. Zaloguj się na swoje konto My Axis.

Zostanie do Ciebie wysłana wiadomość e-mail.

2. Otwórz wiadomość e-mail i kliknij opcję Authenticate (Uwierzytelnij).

Jeżeli nie otrzymano wiadomości e-mail, sprawdź, czy nie trafiła ona do folderu ze spamem. Jeżeli jej tam nie ma, skontaktuj się z działem pomocy IT.

Instalowanie klienta i aktywowanie konta

Przejdź na stronę produktu w witrynie axis.com i pobierz instalator aplikacji AXIS Device Manager Extend.

1. Odszukaj miejsce, w którym została zapisana aplikacja, a następnie kliknij ją i wybierz opcję instalacji.

AXIS Device Manager Extend

Rozpoczynanie pracy

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.

Instalowanie hosta na krawędzi systemu

Zarówno host na krawędzi systemu, jak i klient komputerowy wchodzi w skład instalatora AXIS Device Manager Extend. Zalecamy zainstalowanie kontrolera lokalizacji na serwerze znajdującym się jak najbliżej urządzeń.

1. Wybierz serwer, na którym chcesz zainstalować hosta na krawędzi systemu.
2. Uruchom instalator na serwerze i wybierz instalację tylko hosta na krawędzi systemu.

Przypisanie hosta na krawędzi systemu

Aby utworzyć bezpieczne połączenie z urządzeniami z poziomu aplikacji komputerowej AXIS Device Manager Extend, należy najpierw przypisać do organizacji hosta na krawędzi systemu.

1. Kliknij hosta na krawędzi systemu ze statusem **Unclaimed (Nieprzypisany)**
 - 1.1 Kliknij opcję **Add new edge host (Dodaj nowego hosta na krawędzi systemu)**, jeśli na liście nie ma jeszcze żadnego hosta na krawędzi systemu.
 - 1.2 Wpisz adres IP lokalizacji hosta na krawędzi systemu
2. Wpisz nazwę hosta na krawędzi systemu
3. Dodaj opcjonalny opis (zalecane).
4. Kliknij opcję **Claim edge host (Przypisz hosta na krawędzi systemu)**

AXIS Device Manager Extend

Zarządzaj urządzeniami

Zarządzaj urządzeniami

Dodawanie wykrytych urządzeń do hosta na krawędzi systemu

1. Przejdź do menu Edge hosts (Hosty na krawędzi systemu).
2. Wybierz żądanego hosta na krawędzi systemu 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 na krawędzi systemu).

Urządzenia znajdują się teraz na karcie Managed (Zarządzane), a ich status można sprawdzić w menu Edge host overview (Host na krawędzi systemu: 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 na krawędzi systemu 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 menu Devices > Discovered (Urządzenia > 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 na krawędzi systemu 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).

AXIS Device Manager Extend

Zarządzaj urządzeniami

Uwaga

Plik powinien zawierać:
nagłówek kolumny adresów IP
pojedynczą kolumnę
maksymalnie 25 600 adresów IP.

Usuń urządzenia



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

help.axis.com/?&pid=63389&tsection=remove-devices

Usuwanie urządzeń z hosta na krawędzi systemu

1. Kliknij pozycję **Edge host (Host na krawędzi systemu)**
2. Wybierz hosta na krawędzi systemu.
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 na krawędzi systemu)**.
6. Kliknij przycisk **Remove (Usuń)**.

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

Logowanie do urządzeń

1. Kliknij pozycję **Edge hosts (Hosty na krawędzi systemu)**
2. Wybierz hosta na krawędzi systemu.
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 **Log in (Zaloguj się)**.

Uwaga

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

AXIS Device Manager Extend

Konfiguracja

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 na krawędzi systemu, dla którego chcesz uaktywnić funkcję zdalnego dostępu.
2. Przejdź do menu **Settings > Edge hosts connections** (Ustawienia > Połączenia hostów na krawędzi systemu).
3. Włącz **Allow remote access to edge host** (Zezwalaj na zdalny dostęp do hosta na krawędzi systemu).
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 umożliwić połączenie z hostami na krawędzi systemu w innych sieciach, może być konieczne dodanie poniższej konfiguracji do listy dozwolonych elementów zapory sieciowej: Endpoint Port Protocol signaling.prod.webrtc.connect.axis.com 443 HTTPS *.turn.prod.webrtc.connect.axis.com 443 HTTPS webrtc (włącz obsługę protokołu P2P) 5349, 49152 – 65535 DTLS (UDP i TCP)

Usuwanie lokalizacji

Przed usunięciem hosta na krawędzi systemu z organizacji należy *Usuń urządzenia na stronie 12* należące do hosta na krawędzi systemu. Usunięte urządzenia można znaleźć w obszarze **Devices > Discovered** (Urządzenia > Wykryte).

1. Kliknij pozycję **Edge hosts** (Hosty na krawędzi systemu).
2. Wybierz hosta na krawędzi systemu przy użyciu przycisków strzałek lub umieść nad nim wskaźnik myszy.
3. Kliknij pozycję ... i z rozwijalnego menu wybierz opcję **Remove edge host** (Usuń hosty na krawędzi systemu).
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 menu **Users** (Użytkownicy).
3. Kliknij opcję **Invite to organization** (Zaproś do organizacji).
4. Wpisz adres e-mail użytkownika, którego chcesz zaprosić do swojej organizacji.
5. Kliknij opcję **Send invite** (Wyślij zaproszenie).

Uwaga

Użytkownik otrzyma wiadomość e-mail z zaproszeniem, którą może wykorzystać do zalogowania się do AXIS Device Manager Extend. Domyślna rola użytkownika to **Viewer** (Dozorca). 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.

AXIS Device Manager Extend

Konfiguracja

Podnoszenie roli użytkownika

1. Wybierz organizację, w której chcesz skonfigurować ustawienia użytkownika.
2. Przejdź do menu Users (Użytkownicy).
3. Przejdź do pozycji Role (Rola) powiązanej z użytkownikiem, którego rolę chcesz podnieść.
4. Kliknij rozwijalne menu i wybierz nową rolę.

Uwaga

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

Usuwanie użytkowników

1. Wybierz organizację, w której chcesz skonfigurować ustawienia użytkownika.
2. Przejdź do menu Users (Użytkownicy).
3. Po najechniu kursorem myszy na użytkownika, którego chcesz usunąć, zostanie wyświetlone nowe menu opcji: ...
4. Kliknij pozycję ... i wybierz opcję Remove user (Usuń użytkownika) z rozwijalnego menu.

AXIS Device Manager Extend

Zarządzanie oprogramowaniem sprzętowym

Zarządzanie oprogramowaniem sprzętowym

AXIS Device Manager Extend umożliwia zarządzanie oprogramowaniem sprzętowym wielu urządzeń w każdej organizacji.

Lista aktualizacji oprogramowania sprzętowego dostępnych dla każdego urządzenia w organizacji, pogrupowanych według modelu, znajduje się w oknie Home > Firmware inventory (Strona główna > Spis oprogramowania sprzętowego). Aby zapoznać się z listą aktualizacji oprogramowania sprzętowego dostępnych w określonym hoście na krawędzi systemu, zaznacz hosta na krawędzi systemu i przejdź do menu Firmware inventory (Spis oprogramowania sprzętowego).

Zarządzanie oprogramowaniem sprzętowym z podziałem na modele urządzeń

Aby zarządzać oprogramowaniem sprzętowym według modelu urządzenia w całej organizacji:

1. Przejdź do Home > Firmware inventory (Strona główna > Spis oprogramowania sprzętowego)
2. Zaznacz model, którym chcesz zarządzać.
3. Kliknij rozwijalne menu Upgrade to (Zaktualizuj do), aby wyświetlić dostępne możliwości. Najnowsze istniejące oprogramowanie sprzętowe będzie wstępnie zaznaczone.
4. Kliknij polecenie Upgrade (Aktualizuj).

Zarządzaj oprogramowaniem sprzętowym urządzenia na hoście na krawędzi systemu.

Aby zarządzać oprogramowaniem sprzętowym niektórych lub wszystkich urządzeń na hoście na krawędzi systemu:

1. Przejdź do menu Edge hosts (Hosty na krawędzi systemu)
2. Kliknij hosta na krawędzi systemu, do którego chcesz uzyskać dostęp.
3. Przejdź do opcji Devices (Urządzenia)
4. Zaznacz wszystkie urządzenia lub tylko te, którymi chcesz zarządzać.
5. W menu Action (Akcja) kliknij ikonę Firmware (Oprogramowanie sprzętowe).
6. Zaznacz wszystkie lub wybrane modele na liście.
7. Jeżeli chcesz zmienić zaznaczone oprogramowanie sprzętowe, kliknij sugerowane oprogramowanie, a zobaczysz, jakie inne opcje są dostępne dla każdego urządzenia. Najnowsze istniejące oprogramowanie sprzętowe będzie wstępnie zaznaczone.
8. Kliknij opcję Upgrade (Aktualizuj).

Wyświetlanie trwających i zakończonych aktualizacji oprogramowania sprzętowego

Aby zobaczyć ukończone aktualizacje oprogramowania sprzętowego:

1. Wybierz opcję Sites (Lokalizacje).
2. Kliknij lokalizację, do której chcesz uzyskać dostęp.
3. Wybierz opcję Tasks (Zadania)

Aby zobaczyć trwające aktualizacje oprogramowania sprzętowego:

4. Wybierz opcję Sites (Lokalizacje).
5. Kliknij lokalizację, do której chcesz uzyskać dostęp.
6. Wybierz kolejno opcje Tasks > Ongoing tasks (Zadania > Trwające zadania)

AXIS Device Manager Extend

Policies (Polityki)

Policies (Polityki)

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 na krawędzi systemu.

Tworzenie podstawowej zasady zabezpieczeń:

1. Przejdź do menu **Edge hosts (Hosty na krawędzi systemu)**
2. Kliknij hosta na krawędzi systemu, 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 na krawędzi systemu.

1. Przejdź do menu **Edge hosts (Hosty na krawędzi systemu)**
2. Kliknij hosta na krawędzi systemu, 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.

AXIS Device Manager Extend

Policies (Polityki)

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 **Save (Zapisz)**.

Uwaga

Zaznaczone aplikacje w razie usunięcia zostaną automatycznie ponownie zainstalowane.

Edytowanie zasady

Aby edytować istniejącą zasadę:

1. Przejdź do menu **Edge hosts (Hosty na krawędzi systemu)**
2. Kliknij hosta na krawędzi systemu, 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 **Save (Zapisz)**

Usuwanie zasady

Aby usunąć istniejącą zasadę:

- Przejdź do menu **Edge hosts (Hosty na krawędzi systemu)**
- Kliknij hosta na krawędzi systemu, 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.

AXIS Device Manager Extend

Rozwiązywanie problemów

Rozwiązywanie problemów

Konfigurowanie ustawień zapory

Klient AXIS Device Manager Extend wymaga dostępu do domeny axis.com i dowolnej poddomeny.

Aby klient i host na krawędzi systemu AXIS Device Manager Extend mógł komunikować się z usługą Axis, należy dodać następujące adresy IP i porty do listy dozwolonych przez zaporę organizacji:

- 40.127.155.231 (EU), port 443
- 52.224.128.152 i 40.127.155.231 (US), port 443
- Adres IP publicznego serwera DNS, port 53

Domena prod.adm.connect.axis.com (która jest rekordem DNS A wskazującym na powyższe adresy IP) może być też używana w ustawieniach zapory.

Host na krawędzi systemu AXIS Device Manager Extend używa nazwy domeny prod.adm.connect.axis.com dla wszystkich żądań wychodzących.

Aby ta funkcja działała, sieć będzie musiała korzystać z publicznego serwera DNS i zezwalać na ruch do adresu IP serwera DNS (i domyślnego portu 53).

