

Przewodnika po zabezpieczeniach systemu AXIS OS

Portal AXIS OS | Informacje o wersji systemu AXIS OS | Baza wiedzy dot. systemu AXIS OS | Lista odtwarzania na YouTube AXIS OS | Ostrzeżenia dotyczące bezpieczeństwa

Wprowadzenie

Podczas projektowania, rozwijania i testowania swoich urządzeń Axis Communications stara się stosować najlepsze praktyki z zakresu cyberbezpieczeństwa, aby zminimalizować ryzyko powstania słabych punktów możliwych do wykorzystania w ataku hakerskim. Aby były one skuteczne, w zabezpieczanie sieci, jej urządzeń i dostępnych w niej usług, muszą być zaangażowane cały łańcuch dostaw dostawcy i organizacja użytkownika końcowego. Bezpieczeństwo środowiska zależy od jego użytkowników, procesów i technologii. Ten przewodnik został opracowany jako pomoc w zapewnieniu bezpieczeństwa sieci, urządzeń i usług.

W przypadku urządzeń Axis najbardziej oczywistymi zagrożeniami mogą być fizyczne naruszenia, sabotaż i wandalizm. Aby zabezpieczyć produkt przed tymi zagrożeniami, konieczne jest wybranie modelu urządzenia lub dodatkowej obudowy wzmocnionych na wypadek ewentualnych aktów wandalizmu, następnie zamocowanie rozwiązania zgodnie z zaleceniami producenta i wreszcie – zabezpieczenie sieci przewodów.

Urządzenia Axis to sieciowe punkty końcowe, takie jak komputery czy telefony komórkowe. Wiele z tych urządzeń jest wyposażonych w interfejsy WWW, przez które atakujący mogą odkrywać luki w zabezpieczeniach połączonych systemów. W tym przewodniku opisujemy, jak można ograniczyć tego typu zagrożenia.

Przewodnik ten zawiera porady techniczne dla osób zajmujących się wdrażaniem rozwiązań firmy Axis. Opis konfiguracji podstawowej jest uzupełniony o polecane zabezpieczenia uwzględniające dynamikę krajobrazu zagrożeń. Skonfigurowanie poszczególnych ustawień może wymagać zapoznania się z instrukcją obsługi produktu. Warto mieć na uwadze, że w systemach AXIS OS w wersjach 7.10 i 10.9 wprowadziliśmy uaktualnienie interfejsu WWW urządzeń Axis, co spowodowało zmianę ścieżki konfiguracji.

Ścieżka konfiguracji interfejsu WWW

W niniejszym przewodniku przedstawiamy metody konfiguracji ustawień urządzenia Axis w jego interfejsie WWW. Ścieżka konfiguracji zależy od wersji systemu operacyjnego AXIS OS zainstalowanego na urządzeniu:

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Security > IEEE 802.1X (Ustawienia > Opcje systemu > Zabezpieczenia > IEEE 802.1X)
7.10	Settings > System > Security (Ustawienia > System > Zabezpieczenia)
= 10.9	System > Security (System > Zabezpieczenia)

Scope (Zakres)

Ten przewodnik dotyczy wszystkich produktów z systemem AXIS OS (LTS lub aktywna ścieżka), jak również starszego sprzętu z systemami 4.xx i 5.xx.

Poziomy ochrony CIS

Aby ustrukturyzować nasze zalecenia dotyczące cyberbezpieczeństwa, postępujemy zgodnie z metodami opisanymi w wersji 8 dokumentu Center for Internet Safety (CIS) Controls. Dokument CIS Controls, wcześniej znany pod nazwą SANS Top 20 Critical Security Controls, opisuje 18 kategorii krytycznych kontroli bezpieczeństwa (Critical Security Controls, CSC) skoncentrowanych na radzeniu sobie z najczęściej występującymi kategoriami ryzyka cyberbezpieczeństwa w organizacji.

W tym przewodniku, w każdym temacie poświęconym zabezpieczeniom, znajdują się odniesienia do konkretnych numerów CSC (CSC #). Aby uzyskać więcej informacji na temat kategorii CSC, zobacz *18 CIS Critical Security Controls* na [cisecurity.org](https://www.cisecurity.org).

Domyślne zabezpieczenia

Urządzenia Axis są oferowane z domyślnymi ustawieniami zabezpieczeń. Wiele funkcji zabezpieczeń nie wymaga konfigurowania przez użytkownika. Funkcje te zapewniają podstawową warstwę zabezpieczenia urządzenia oraz fundament bardziej zaawansowanych mechanizmów ochrony.

Schemat architektury bezpieczeństwa systemu AXIS OS nakreśla potencjał bezpieczeństwa cybernetycznego systemu AXIS OS w różnych warstwach. Stanowi kompleksowy przegląd podstaw bezpieczeństwa, zabezpieczeń wspomaganych sprzętowo, systemu operacyjnego AXIS OS oraz warstwy aplikacji i kontroli dostępu.

Access control	Access control management Local user device management with password complexity indicator Federated user device management through OpenID Connect (RFC6749, 1.3.1 Authorization Code) providing ADFS-integration that unlocks features such as password complexity enforcement, rotation, automatic account lock-out Multi-factor authentication (MFA), Microsoft AD entitlement functionality		Privacy Use of diagnostics data Minimalistic approach to how much customer-specific data should be stored
	Application security TLS-based application security (MQTT, SFTP, NTS, HTTPS, WebRTC) Encrypted video streaming (RTSPS/SRTP, HTTPS), Secure remote syslog		
Operating system	Encryption and data protection OpenSSL 1.1.1 and 3.0 X.509 certificate PKI and cryptography Transport layer security (TLS 1.2/TLS 1.3) SD card encryption (AES-XTS-Plain64 256bit) Encrypted file system (AES-XTS-Plain64 256bit), Signed video	Default security HTTPS enabled by default Brute-Force Delay Protection Host-based Firewall Network time security (NTS) Insecure TLS versions disabled UART/Debug port disabled	Enterprise network security IEEE 802.1X (network access control) IEEE 802.1AR (secure device identity) IEEE 802.1AE (MAC security, MACsec)
AXIS OS Operating System Common Linux-based operating system with more than 95% industry-standard open-source software components such as OpenSSL, Apache, Curl and others. Active track for feature growth and 5-year long-term support tracks (LTS) for 3rd party integration and backwards-compatibility use cases.			
Silicon assisted security (chip)	Hardware root-of-trust ARM-based system-on-chip (SoC) security Trusted Execution Environment (TEE/OP-TEE) Trusted platform module (TPM 2.0), Secure element		Secure key storage Tamper-protected storage and operation of cryptographic keys such as customer uploaded private keys, video signing keys and the Axis Device ID.
Security foundation	Axis Security Development Model Axis security development model (ASDM) 3rd party penetration tests Bug bounty program with Bugcrowd Software Bill of Material (SBOM)	Compliance Common Criteria EAL FIPS 140 ETSI EN 303 645	Trusted device identity Axis Edge Vault cybersecurity platform Secure boot with Signed OS (code-signing) Axis Device ID (IEEE 802.1AR)

Kliknij prawym przyciskiem myszy i otwórz obraz w nowej karcie, aby uzyskać bardziej czytelny widok.

Uwierzytelnianie

Domyślnie wyłączone

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy

Urządzenie Axis nie działa, dopóki nie zostanie ustawione hasło administratora.

Gdy zostanie ustawione hasło administratora, uzyskanie dostępu do funkcji administratora lub strumieni wideo, będzie wymagało podania poprawnego hasła i nazwy użytkownika. Nie zalecamy korzystania z funkcji pozwalających na dostęp bez uwierzytelniania, takich jak anonimowe wyświetlanie czy zawsze aktywny tryb multicast.

Instrukcje konfigurowania dostępu do urządzeń można znaleźć w temacie *Dostęp do urządzeń w AXIS OS Knowledge base* (Bazie wiedzy o systemie AXIS OS).

Uwierzytelnianie szyfrowane

CSC #3: Ochrona danych

Klienci uzyskujące dostęp do urządzenia będą uwierzytelniać się za pomocą hasła, które powinno być szyfrowane podczas przesyłania przez sieć. W związku z tym zalecamy korzystanie wyłącznie z uwierzytelniania szyfrowanego zamiast podstawowego lub korzystanie z obu tych mechanizmów szyfrowania jednocześnie. Zmniejsza to ryzyko przejęcia hasła przez programy do szpiegowania sieci.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Advanced > Plain Config > Network > Network HTTP Authentication policy (Konfiguracja > Opcje systemowe > Zaawansowane > Zwykła konfiguracja > Sieć > Zasady uwierzytelniania sieciowego HTTP)
7.10	Settings > System > Plain config > Network > Network HTTP Authentication policy (Konfiguracja > System > Zwykła konfiguracja > Sieć > Zasady uwierzytelniania sieciowego HTTP)
= 10.9	System > Plain config > Network > Network HTTP Authentication policy (System > Zwykła konfiguracja > Sieć > Zasady uwierzytelniania sieciowego HTTP)

Ochrona przed atakami powtórzeniowymi na ONVIF

CSC #3: Ochrona danych

Zabezpieczenie przed atakiem powtórzeniowym należy do standardowych zabezpieczeń domyślnie włączonych w urządzeniach Axis. Ma ono na celu odpowiednie zabezpieczenie uwierzytelniania użytkownika opartego na ONVIF za pomocą dodatkowego nagłówka bezpieczeństwa zawierającego token nazwy użytkownika, ważny znacznik czasu, identyfikator jednorazowy (nonce) i skrót hasła. Skrót hasła jest obliczany na podstawie hasła (które jest już przechowywane w systemie), identyfikatora jednorazowego i znacznika czasu. Skróty haseł służą do uwierzytelnienia użytkowników i zapobiegania atakom powtórzeniowym, dlatego są one przechowywane w pamięci podręcznej. Zalecamy niewyłączanie tego ustawienia.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Advanced > Plain Config > System > Enable Replay Attack Protection (Konfiguracja > Opcje systemowe > Zaawansowane > Zwykła konfiguracja > System > Włącz ochronę przed atakami powtórzeniowymi)
7.10	Settings > System > Plain config > WebService > Enable Replay Attack Protection (Konfiguracja > System > Zwykła konfiguracja > Usługa sieciowa > Włącz ochronę przed atakami powtórzeniowymi)
= 10.9	System > Plain config > WebService > Enable Replay Attack Protection (System > Zwykła konfiguracja > Usługa sieciowa > Włącz ochronę przed atakami powtórzeniowymi)

Zapobiegaj atakom typu brute force

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy

CSC #13: Monitorowanie i ochrona sieci IP

Urządzenia Axis są wyposażone w mechanizm identyfikowania i blokowania sieciowych ataków typu brute-force, w tym zgadywania haseł. Funkcja ta, zwana ochroną przed atakami brute-force, jest dostępna w systemie AXIS OS 7.30 i nowszych.

Ochrona przed atakami typu brute force jest domyślnie włączona, począwszy od wersji systemu operacyjnego AXIS OS 11.5. Szczegółowe przykłady konfiguracji i zalecenia znajdują się na stronie *Ochrona przed atakami typu brute force* w bazie wiedzy dot. systemu operacyjnego AXIS OS.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	n/d
7.10	Settings > System > Plain config > System > PreventDosAttack (Ustawienia > System > Zwykła konfiguracja > System > Zapobieganie atakom Dos)
= 10.9	System > Security > Prevent brute-force attacks (System > Zabezpieczenia > Zapobieganie atakom brute-force)

Pamięć masowa typu Edge

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy

CSC #3: Ochrona danych

Od wersji AXIS OS 12.0, opcja montowania noexec została dodana jako opcja domyślna dla zamontowanych udziałów sieciowych. Spowoduje to wyłączenie bezpośredniego wykonywania plików binarnych z zamontowanego udziału sieciowego. Tę opcję miała już karta SD we wcześniejszych wersjach systemu operacyjnego AXIS OS.

Dodatkowo urządzenia Axis z systemem AXIS OS 10.10 i nowszymi obsługują szyfrowany eksport nagrań z urządzeń na krawędzi systemu. Zalecamy korzystanie z tej funkcji, ponieważ zapobiega ona odtwarzaniu wyeksportowanych materiałów wideo przez nieupoważnione osoby.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	n/d
7.10	n/d
= 10.9	Nagrania

Bezpieczeństwo sieci

Protokoły sieciowe

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy

Urządzenia Axis mają domyślnie włączoną obsługę minimalnej liczby protokołów sieciowych i usług. Te domyślnie włączone opcje zostały wyszczególnione w tabeli poniżej.

Protokół	Port	Transport	Uwagi
HTTP	80	TCP	Ogólny ruch HTTP, w tym dostęp do interfejsów WWW, interfejsy VAPIX, interfejs programowania aplikacji (API) ONVIF i komunikacja edge-to-edge.*
HTTPS	443	TCP	Ogólny ruch HTTPS, w tym dostęp do

Protokół	Port	Transport	Uwagi
			interfejsów WWW, interfejsy VAPIX, interfejs programowania aplikacji (API) ONVIF i komunikacja edge-to-edge.*
RTSP	554	TCP	Używany przez urządzenie Axis do przesyłania strumieniowego obrazu wideo lub dźwięku.
RTP	Zasięg portu efemerycznego**	UDP	Używany przez urządzenie Axis do przesyłania strumieniowego obrazu wideo lub dźwięku.
UPnP	49152	TCP	Używany przez aplikacje zewnętrzne do wykrywania urządzenia Axis za pomocą protokołu UPnP discovery. UWAGA: Wyłączony domyślnie począwszy od systemu AXIS OS 12.0.
Bonjour	5353	UDP	Używany przez aplikacje zewnętrzne do wykrywania urządzenia Axis za pomocą protokołu mDNS discovery (Bonjour).
SSDP	1900	UDP	Używany przez aplikacje zewnętrzne do wykrywania urządzenia Axis za pomocą protokołu SSDP (UPnP). UWAGA: Wyłączony domyślnie począwszy od systemu AXIS OS 12.0.
WS-Discovery***	3702	UDP	Używany przez aplikacje zewnętrzne do wykrywania urządzenia Axis za pomocą protokołu WS-Discovery (ONVIF).

* Więcej informacji na temat technologii edge-to-edge można znaleźć w białej księdze. *Technologia edge-to-edge*.

** Przydzielany automatycznie w ramach predefiniowanego zakresu numerów portów zgodnie z RFC 6056. Więcej informacji można znaleźć w artykule Wikipedii *Port efemeryczny*.

*** Protokół WebService Discovery (WS-Discovery) jest domyślnie wyłączony w systemie operacyjnym AXIS OS 12.1 i nowszych.

Gdy tylko jest to możliwe, zalecamy wyłączenie nieużywanych protokołów i usług sieciowych. Pełną listę usług, które są używane domyślnie lub mogą być włączone na podstawie konfiguracji, można znaleźć w artykule *Często używane porty sieciowe w AXIS OS Knowledge base* (Bazie wiedzy o systemie AXIS OS).

Na przykład w produktach Axis do systemu dozoru wizyjnego, takich jak kamery sieciowe, trzeba ręcznie włączyć funkcję wejścia/wyjścia audio i mikrofonu, natomiast w interkomach i głośnikach sieciowych Axis funkcja wejścia/wyjścia audio oraz mikrofonu są funkcjami najważniejszymi, więc są włączone domyślnie.

Włączony protokół HTTPS

CSC #3: Ochrona danych

W systemie AXIS OS 7.20 i nowszych protokół HTTPS jest domyślnie włączony wraz z certyfikatem z własnym podpisem, który umożliwia bezpieczne skonfigurowanie hasła urządzenia. W systemach AXIS OS 10.10 i nowszych certyfikat samopodpisany został zastąpiony certyfikatem bezpiecznego identyfikatora urządzenia IEEE 802.1AR.

W systemie AXIS OS najpopularniejsze nagłówki HTTP związane z zabezpieczeniami są domyślnie włączone, aby zapewnić wyższy podstawowy poziom cyberbezpieczeństwa w domyślnym stanie fabrycznym. Począwszy od systemu AXIS OS 9.80, można konfigurować dodatkowe nagłówki HTTP(S) za pomocą niestandardowego nagłówka HTTP interfejsu API VAPIX.

Aby uzyskać więcej informacji na temat nagłówka HTTP interfejsu programowania aplikacji (API) VAPIX, zobacz temat *VAPIX Library (Biblioteka VAPIX)*.

Aby dowiedzieć się więcej o domyślnych nagłówkach HTTP(S), zobacz temat *Default HTTP(S) headers (Domyślne nagłówki HTTP(S))* w AXIS OS Knowledge base (Bazie wiedzy o systemie AXIS OS).

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Security > HTTPS (Konfiguracja > Opcje systemowe > Zabezpieczenia > HTTPS)
7.10	Settings > System > Security > HTTP and HTTPS (Ustawienia > System > Zabezpieczenia > HTTP i HTTPS)
= 10.9	System > Network > HTTP and HTTPS (System > Sieć > HTTP i HTTPS)

Kontrola dostępu do sieci w standardzie IEEE 802.1X

CSC #6: Zarządzanie kontrolą dostępu

CSC #13: Monitorowanie i ochrona sieci IP

Urządzenia Axis obsługują kontrolę dostępu do sieci opartą na portach IEEE 802.1X za pomocą metody EAP-TLS. W celu zapewnienia optymalnej ochrony zalecamy używanie certyfikatów klientów podpisanych przez zaufany urząd certyfikacji do uwierzytelniania urządzenia Axis.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Security > IEEE 802.1X (Ustawienia > Opcje systemu > Zabezpieczenia > IEEE 802.1X)
7.10	Settings > System > Security > IEEE 802.1X (Ustawienia > System > Zabezpieczenia > IEEE 802.1X)
= 10.9	System > Security > IEEE 802.1X (System > Zabezpieczenia > IEEE 802.1X)

IEEE 802.1AE MACsec

CSC #3: Ochrona danych

CSC #6: Zarządzanie kontrolą dostępu

Urządzenia Axis obsługują IEEE 802.1AE MACsec (Media Access Control Security) – dobrze zdefiniowany protokół sieciowy, który kryptograficznie zabezpiecza łącza Ethernet typu punkt-punkt w warstwie sieci 2. Zapewnia poufność i integralność transmisji danych pomiędzy dwoma hostami. Ze względu na to, że MACsec działa w niższej warstwie 2 stosu sieciowego, dodaje warstwę zabezpieczeń do protokołów sieciowych niewyposażonych w natywne opcje szyfrowania (ARP, NTP, DHCP, LLDP, CDP...), jak również tych, które stosują te same rozwiązania (HTTPS, TLS).

Standard IEEE 802.1AE MACsec opisuje dwa tryby działania: manualnie konfigurowalny Pre-Shared Key (PSK)/Static CAK oraz automatyczny Master Session/Dynamic CAK, wykorzystujący sesje IEEE 802.1X EAP-TLS. Urządzenie Axis obsługuje oba tryby.

Więcej informacji na temat protokołu 802.1AE MACsec i jego konfiguracji w urządzeniach AXIS OS można znaleźć w temacie *IEEE 802.1AE* w bazie wiedzy AXIS OS.

Bezpieczna tożsamość urządzeń zgodnie z normą IEEE 802.1AR

CSC #1: Inwentaryzacja i kontrola zasobów firmy

CSC #13: Monitorowanie i ochrona sieci IP

Urządzenia Axis wyposażone w cyberzabezpieczenia z funkcją Axis Edge Vault obsługują standard sieciowy IEEE 802.1AR. Pozwala to na zautomatyzowane i bezpieczne dołączanie urządzeń Axis do sieci IP z wykorzystaniem identyfikatora urządzenia Axis – niepowtarzalnego certyfikatu instalowanego w urządzeniu na etapie produkcji. Przykład bezpiecznego wdrożenia urządzeń został szczegółowo opisany w przewodniku *Secure integration of Axis devices into Aruba networks (Bezpieczna integracja urządzeń Axis w sieciach Aruba)*.

Więcej informacji znajduje się w oficjalnym dokumencie *Axis Edge Vault*. Aby pobrać łańcuch certyfikatów ID urządzenia Axis do weryfikacji tożsamości urządzenia Axis, zobacz temat *Public Key Infrastructure Repository (Repozytorium infrastruktury kluczy publicznych)* w witrynie axis.com.

Interfejs UART/debugowania

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy

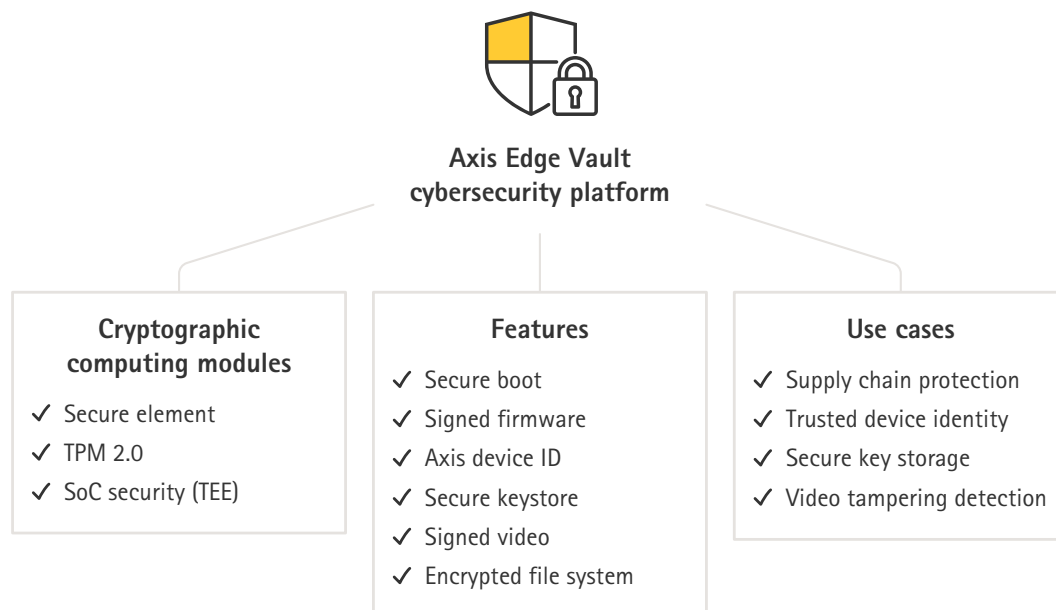
Każde urządzenie Axis jest wyposażone w fizyczny interfejs UART (Universal Asynchronous Receiver Transmitter) określany niekiedy jako „port debugowania” lub „konsola szeregową”. Sam interfejs jest fizycznie dostępny tylko po gruntownym rozebraniu urządzenia Axis. Interfejs UART/debugowania jest wykorzystywany wyłącznie na etapie opracowywania produktu i debugowania podczas wewnętrznych projektów inżynierskich realizowanych przez dział badań i rozwoju firmy Axis.

Interfejs UART/debugowania jest domyślnie włączony w urządzeniach Axis z systemem AXIS OS 10.10 lub starszym, ale wymaga uwierzytelnionego dostępu. Bez uwierzytelnienia żadne informacje poufne nie zostaną podane. W urządzeniach z systemem AXIS OS 10.11 lub nowszym interfejs UART/debugowania jest domyślnie wyłączony. Do aktywowania tego interfejsu konieczne jest jego odblokowanie za pomocą certyfikatu unikalnego dla urządzenia dostarczonego przez Axis.

Axis Edge Vault

Axis Edge Vault zapewnia sprzętową platformę cyberbezpieczeństwa chroniącą urządzenia Axis. Rozwiązanie to jest oparte na mocnych podstawach zapewnianych przez kryptograficzne moduły obliczeniowe (bezpieczny element i TPM) oraz zabezpieczenia procesora SoC (TEE i bezpieczny start), a także na specjalistycznej wiedzy z zakresu bezpieczeństwa urządzeń brzegowych. Axis Edge Vault opiera się na wysokim poziomie zaufania zapewnianym przez bezpieczny rozruch i podpisane oprogramowanie układowe. Funkcje te zapewniają ciągły łańcuch zweryfikowanego kryptograficznie oprogramowania, co jest podstawą łańcucha zaufania, od którego zależą wszystkie wymagające bezpieczeństwa operacje.

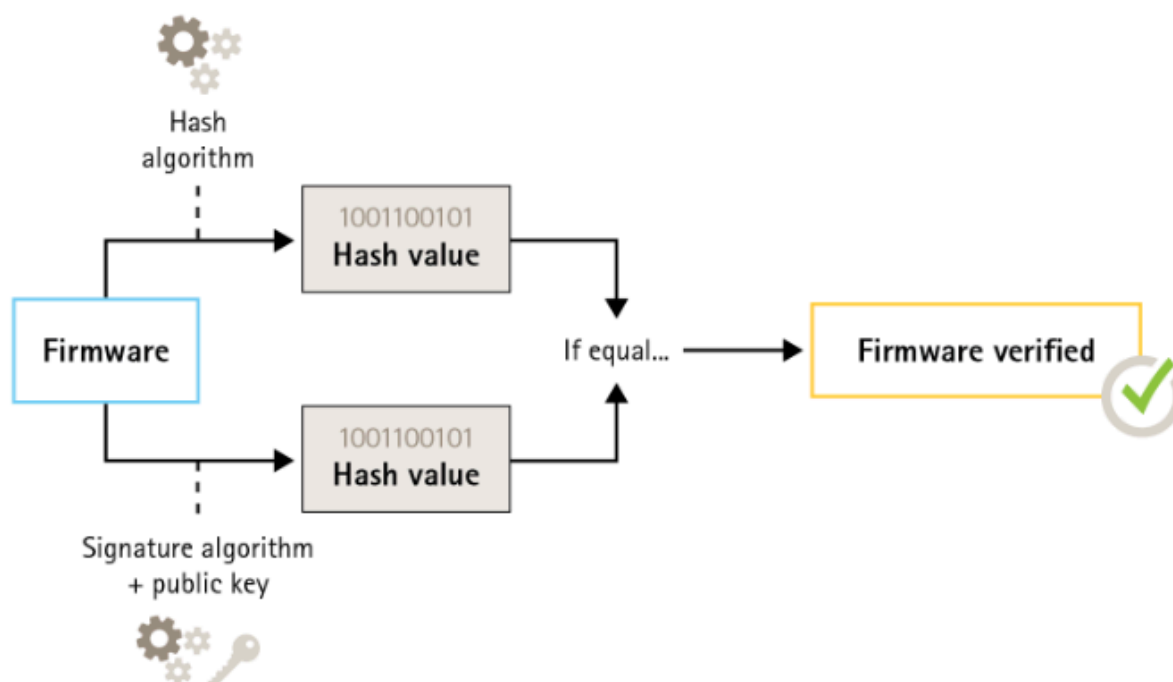
Urządzenia Axis z rozwiązaniem Axis Edge Vault minimalizują narażenie klientów na ryzyko związane z cyberbezpieczeństwem, zapobiegając podsłuchiwananiu i złośliwemu wykradaniu wrażliwych danych. Axis Edge Vault zapewnia też, że urządzenie Axis jest w sieci klienta jednostką zaufaną i niezawodną.



Podpisane oprogramowanie sprzętowe

CSC #2: Inwentaryzacja i kontrola zasobów oprogramowania

System AXIS OS jest podpisany od wersji 9.20.1. Przy każdej aktualizacji systemu AXIS OS na urządzeniu sprawdzana jest integralność plików aktualizacji poprzez weryfikację szyfrowanego podpisu; oznacza to, że wszelkie sfałszowane pliki zostaną odrzucone. Dzięki temu hakerzy nie są w stanie nakłonić użytkownika do instalacji niebezpiecznych plików.

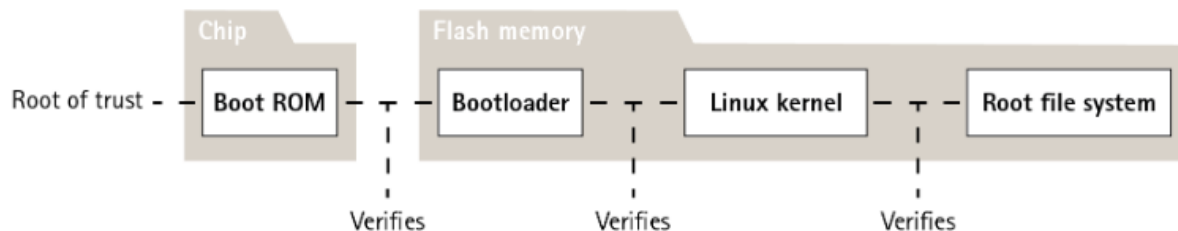


Więcej informacji znajduje się w oficjalnym dokumencie *Axis Edge Vault*.

Bezpieczny start

CSC #2: Inwentaryzacja i kontrola zasobów oprogramowania

Większość urządzeń Axis ma bezpieczną sekwencję rozruchową chroniącą ich integralność. Bezpieczny rozruch uniemożliwia wdrożenie urządzeń Axis, w przypadku których doszło do sabotażu.



Więcej informacji znajduje się w oficjalnym dokumencie *Axis Edge Vault*.

Bezpieczny magazyn kluczy

CSC #6: Zarządzanie kontrolą dostępu

bezpieczny magazyn kluczy zapewnia sprzętowe, zabezpieczone przed manipulacją przechowywanie informacji kryptograficznych. Chroni identyfikator urządzenia Axis, a także informacje kryptograficzne przesłane przez klienta. Jednocześnie blokuje nieautoryzowany dostęp i uniemożliwia złośliwe wydobywanie danych w przypadku naruszenia zabezpieczeń. Zależnie od wymaganego poziomu bezpieczeństwa urządzenie Axis może być wyposażone w jeden lub kilka takich modułów, np. TPM 2.0 (Trusted Platform Module), zabezpieczony element lub TEE (Trusted Execution Environment).



Więcej informacji znajduje się w oficjalnym dokumencie *Axis Edge Vault*.

Zaszyfrowane systemy plików

CSC #3: Ochrona danych

Intruz może próbować wydobyć informacje z systemu plików poprzez zdemontowanie pamięci flash i uzyskanie do niej dostępu przy użyciu czytnika pamięci flash. Można jednak zabezpieczyć system plików przed złośliwym wyciekiem danych i sabotażu konfiguracji w razie fizycznego dostępu do urządzenia Axis lub jego kradzieży. Po wyłączeniu urządzenia Axis informacje w systemie plików są szyfrowane 256-bitowym algorytmem AES-XTS-Plain64. Podczas bezpiecznego rozruchu system plików z uprawnieniami odczytu/zapisu jest odszyfrowywany, po czym można go zamontować i używać na urządzeniu Axis.

Więcej informacji znajduje się w oficjalnym dokumencie *Axis Edge Vault*.

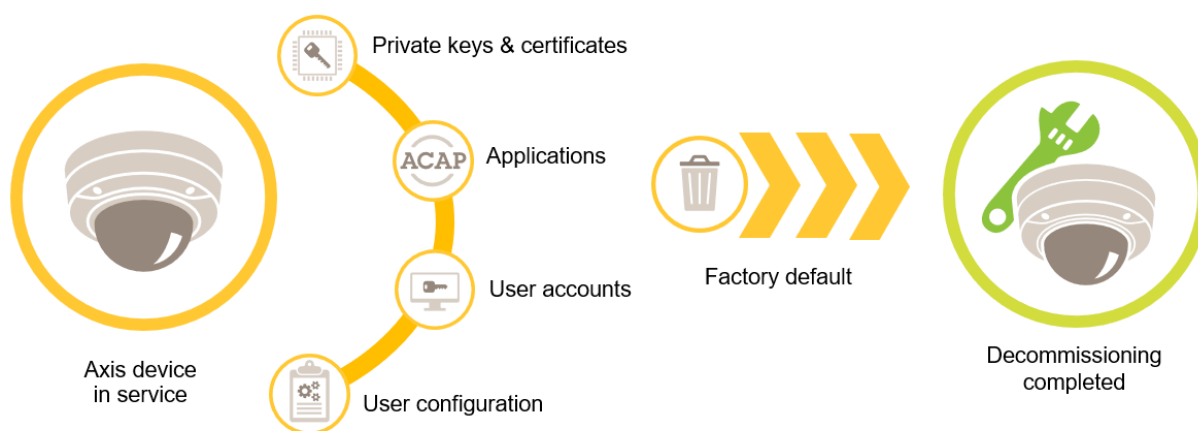
Wycofanie z eksploatacji

CSC #3: Ochrona danych

Urządzenia Axis wykorzystują zarówno pamięć tymczasową, jak i stałą. Zawartość pamięci tymczasowej jest usuwana po odłączeniu urządzenia od źródła zasilania, natomiast informacje przechowywane w pamięci trwałej są zapisywane i ponownie dostępne po włączeniu urządzenia. Staramy się nie stosować powszechnej praktyki, która sprowadza się do usuwania wskaźników danych, aby przechowywane dane były niewidoczne dla systemu plików, dlatego konieczne jest przywrócenie ustawień fabrycznych. W przypadku pamięci NAND-flash używana jest funkcja UBI Remove Volume (Usuń wolumin), odpowiadająca jej funkcja jest używana w przypadku pamięci eMMC-flash, sygnalizując, że bloki zasobu pamięci nie są już używane. Następnie kontroler zasobu pamięci odpowiednio wyczyści te bloki pamięci.

Zalecamy, aby przed wycofaniem urządzenia Axis z użytku zresetować je do ustawień fabrycznych, ponieważ pozwoli to usunąć z niego wszystkie dane przechowane w pamięci stałej.

Wydanie polecenia resetowania do ustawień fabrycznych nie spowoduje natychmiastowego usunięcia danych; w jego wyniku urządzenie uruchomi się ponownie, a usunięcie danych nastąpi podczas uruchamiania systemu. W związku z tym nie wystarczy samo wydanie polecenia resetowania do ustawień fabrycznych. Urządzenie musi również mieć możliwość ponownego uruchomienia i zakończenia sekwencji uruchamiania zanim zostanie odłączone zasilanie, aby zagwarantować, że kasowanie danych zostało zakończone.



Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Maintenance > Default (Konfiguracja > Opcje systemowe > Konserwacja > Domyślne ustawienia)
7.10	Settings > System > Maintenance > Default (Ustawienia > System > Konserwacja > Domyślne ustawienia)
= 10.9	Maintenance > Default (Konserwacja > Domyślne ustawienia)

Więcej informacji na temat pamięci trwałej można znaleźć w tej tabeli.

Informacje i dane	Wymazane po przywróceniu ustawień fabrycznych
Nazwy użytkowników oraz hasła VAPIX i ONVIF	Tak
Certyfikaty i klucze prywatne	Tak
Certyfikat z własnym podpisem	Tak
Zapisane informacje o TPM i Axis Edge Vault	Tak

Ustawienia sieci WLAN i użytkownicy/hasła	Tak
Certyfikaty niestandardowe*	Nie
Klucz szyfrowania karty SD	Tak
Dane karty SD**	Nie
Ustawienia udziałów sieciowych i użytkowników/ haseł	Tak
Dane udziału sieciowego**	Nie
Konfiguracja użytkownika***	Tak
Przesłane aplikacje (ACAPs)****	Tak
Dane produkcyjne i statystyki dotyczące cyklu życia*****	Nie
Przesłane grafiki i nakładki	Tak
Dane zegara RTC	Tak

* Proces podpisanego oprogramowania układowego korzysta z certyfikatów niestandardowych umożliwiających pobieranie (między innymi) systemu operacyjnego AXIS OS.

** Nagrania i obrazy zapisane w pamięci urządzenia brzegowego (karta SD, zasób sieciowy) muszą zostać skasowane przez użytkownika ręcznie. Dalsze informacje znajdują się w pkt *Formatowanie kart SD Axis* w bazie wiedzy dot. systemu operacyjnego AXIS OS.

*** Wszystkie konfiguracje wykonane przez użytkownika, od tworzenia kont do konfiguracji sieciowych, O3C, zdarzeń, obrazów, PTZ i systemowych.

**** Urządzenie zachowuje wszystkie zainstalowane fabrycznie aplikacje, ale usuwa wszystkie konfiguracje wprowadzone do nich przez użytkownika.

***** Dane produkcyjne (kalibracja, certyfikaty produkcyjne 802.1AR) i statystyki czasu eksploatacji zawierają informacje niewrażliwe i niezwiązane z użytkownikiem.

Podstawowe zabezpieczenia

Podstawowe zabezpieczenia to minimalny zalecany poziom ochrony urządzeń Axis. Podstawowe ustawienia zabezpieczeń są konfigurowalne w urządzeniu brzegowym. Oznacza to, że można konfigurować je bezpośrednio w urządzeniu Axis niezależnie od zewnętrznej infrastruktury sieciowej, systemów zarządzania obrazem lub materiałem dowodowym (VMS, EMS), sprzętu czy aplikacji.

Ustawienia fabryczne

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy

Przed skonfigurowaniem urządzenia należy przywrócić w nim ustawienia fabryczne. Przywrócenie ustawień fabrycznych jest też konieczne do skasowania z niego danych użytkownika lub przed wycofaniem urządzenia z użytku. Więcej informacji znajduje się w rozdziale .

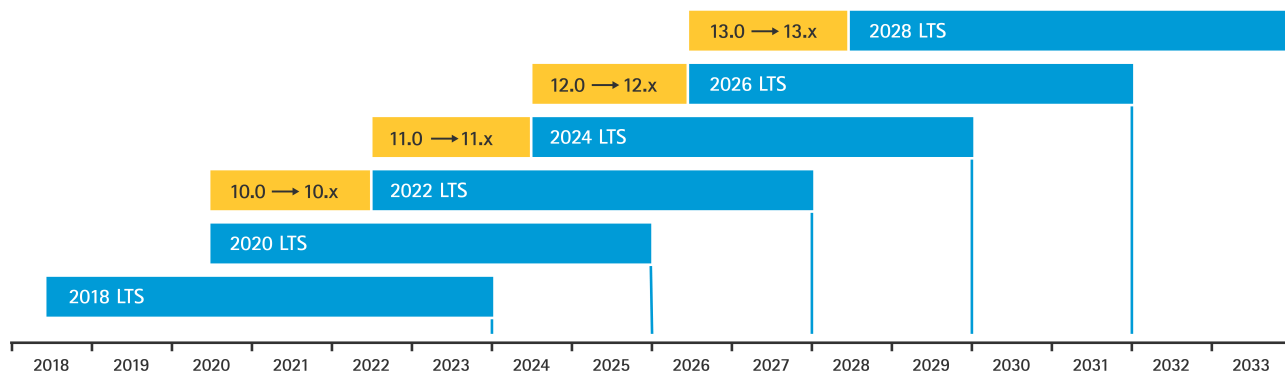
Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Maintenance > Default (Konfiguracja > Opcje systemowe > Konserwacja > Domyślne ustawienia)
7.10	Settings > System > Maintenance > Default (Ustawienia > System > Konserwacja > Domyślne ustawienia)
= 10.9	Maintenance > Default (Konserwacja > Domyślne ustawienia)

Uaktualnienie do najnowszej wersji systemu AXIS OS

CSC #2: Inwentaryzacja i kontrola zasobów oprogramowania

Ważnym aspektem dbania o cyberbezpieczeństwo jest instalowanie poprawek oprogramowania. Cyberprzestępcy często próbują wykorzystywać znane luki w zabezpieczeniach, aby uzyskać dostęp do sieci przez niezabezpieczoną usługę, a brak zainstalowanej poprawki może bardzo im to ułatwić. Korzystanie wyłącznie z najnowszych wersji systemu AXIS OS jest w związku z tym bardzo ważne, ponieważ mogą one zawierać poprawki eliminujące znane luki w zabezpieczeniach. W informacjach dotyczących konkretnej wersji mogą być wyraźnie wymienione poprawki o znaczeniu krytycznym; nie będą natomiast wyszczególnione poprawki ogólnie poprawiające działanie systemu.

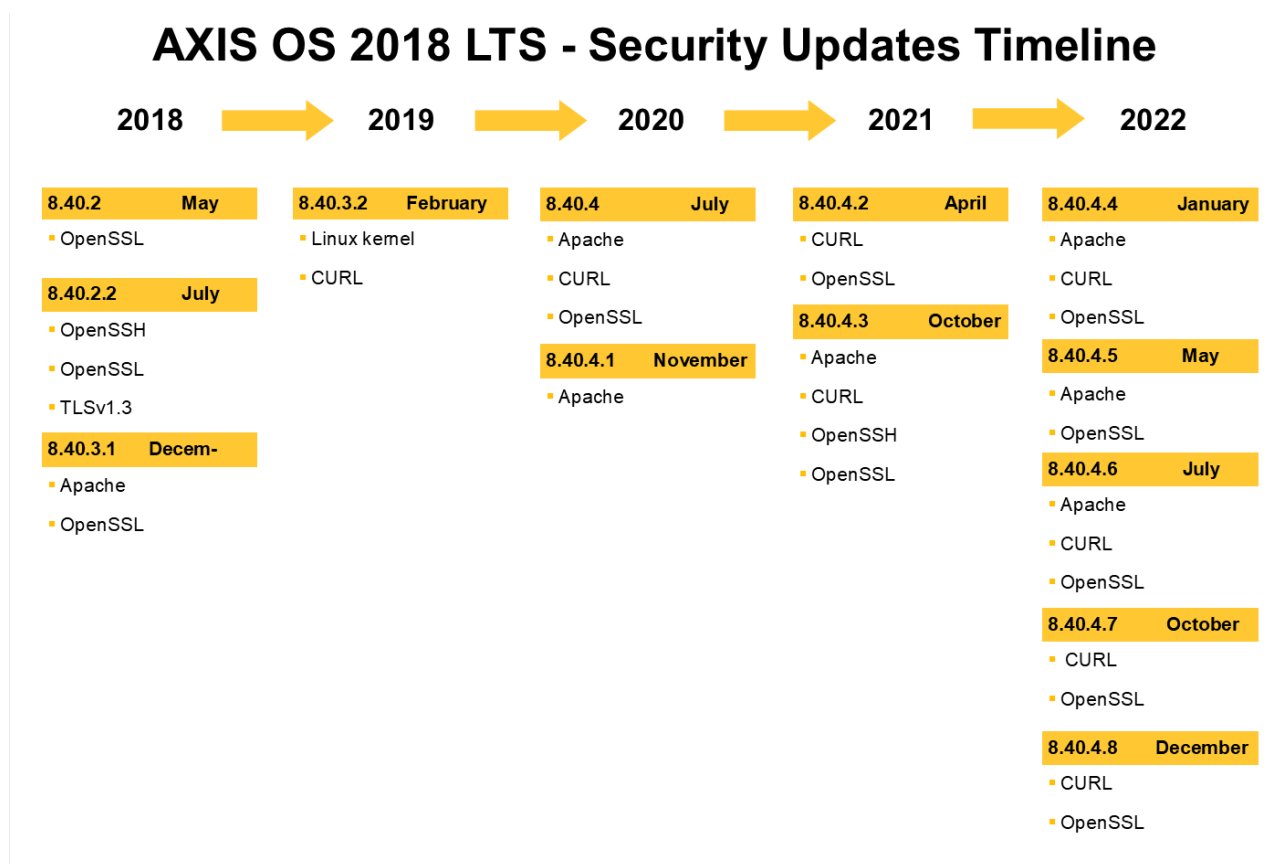
Axis zapewnia dwa rodzaje ścieżek systemu AXIS OS: ścieżkę aktywną i ścieżkę wsparcia długoterminowego (LTS). Oba te tryby uwzględniają najnowsze poprawki o znaczeniu krytycznym, lecz LTS nie zawiera nowych funkcji. Jest to podyktowane troską o maksymalne wyeliminowanie ryzyka niezgodności. Więcej informacji można znaleźć w temacie *AXIS OS lifecycle (Cykl życia systemu AXIS OS)* w informacjach na temat systemu AXIS OS.



Axis z wyprzedzeniem informuje o planowanych wydaniach, w tym o ważnych nowych funkcjach, poprawkach błędów i łatkach bezpieczeństwa. Więcej informacji można znaleźć w temacie *Upcoming releases (Planowane*

wydania) w informacjach na temat systemu AXIS OS. System AXIS OS na poszczególne urządzenia można pobrać sekcji *Firmware (Oprogramowanie układowe)* na axis.com.

Na tym wykresie pokazano, jak ważne jest regularne aktualizowanie urządzeń Axis.



Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Maintenance > Upgrade Server (Konfiguracja > Opcje systemowe > Konserwacja > Aktualizacja serwera)
7.10	Settings > System > Maintenance > Firmware upgrade (Ustawienia > System > Konserwacja > Aktualizacja oprogramowania układowego)
= 10.9	Maintenance > Firmware upgrade (Konserwacja > Aktualizacja oprogramowania układowego).

Tworzenie dedykowanych kont

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy

CSC #5: Zarządzanie kontem

Urządzenia Axis mogą zawierać dwa rodzaje kont: konto administratora oraz konto użytkownika. Konto administratora jest podstawowym kontem służącym do zarządzania urządzeniem; konto to powinno służyć wyłącznie do zadań administracyjnych. Przy konfigurowaniu urządzenia należy utworzyć nazwę użytkownika i hasło z przeznaczeniem dla konta administratora.

Oprócz konta administratora na potrzeby codziennych zadań zaleca się utworzenie konta użytkownika z ograniczonymi uprawnieniami. Pozwoli to bezpiecznie zarządzać urządzeniem i zmniejszyć ryzyko wycieku hasła

administratora urządzenia. Do zadań, które nie wymagają całościowych uprawnień administracyjnych, należy używać konta użytkownika.

Przy tworzeniu haseł dla podanych kont zaleca się stosowanie wytycznych, takich jak wytyczne NIST lub BSI dotyczące haseł, które wymagają, aby nowe hasła miały odpowiednią długość i złożoność. W urządzeniach Axis można ustawiać hasła mające maks. 64 znaki. Hasła krótsze niż 8 znaków są uznawane za słabe.

Aby uzyskać więcej informacji, zobacz *sekcję zarządzania tożsamością i dostępem w Bazie wiedzy AXIS OS*.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > Basic Setup > Users (Konfiguracja > Konfiguracja podstawowa > Użytkownicy)
7.10	Settings > System > Users (Ustawienia > System > Użytkownicy)
= 10.9	System > Users (System > Użytkownicy)
= 11.6	System > Accounts (System > Konta)

Wyłączanie dostępu do interfejsu WWW

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy

CSC #5: Zarządzanie kontem

Urządzenia Axis mają serwer sieciowy umożliwiający użytkownikom dostęp do nich za pomocą standardowej przeglądarki internetowej. Interfejs WWW służy do konfiguracji, konserwacji i rozwiązywania problemów. Nie jest przeznaczony do codziennej pracy, np. jako klient do oglądania materiałów wideo.

Jedynymi klientami, którym należy zezwolić na interakcję z urządzeniami Axis podczas codziennej pracy, są systemy zarządzania materiałem wizyjnym (VMS) oraz narzędzia do administrowania i zarządzania urządzeniami, takie jak AXIS Device Manager. Użytkownicy systemu nigdy nie powinni mieć bezpośredniego dostępu do urządzeń Axis.

W systemach AXIS OS 9.50 i nowszych można wyłączyć interfejs WWW urządzenia Axis. Po wdrożeniu urządzenia Axis w systemie (lub dodaniu go w aplikacji AXIS Device Manager) najlepiej zablokować osobom w organizacji możliwość uzyskania dostępu do urządzenia za pomocą przeglądarki internetowej. Pozwoli to zapewnić dodatkową warstwę zabezpieczeń, jeśli hasło do konta urządzenia jest udostępniane w organizacji. Bezpieczniejszym rozwiązaniem jest ustawienie dostępu do urządzeń Axis wyłącznie poprzez dedykowane aplikacje, które oferują zaawansowaną architekturę zarządzania dostępem do tożsamości (IAM), lepsze możliwości w zakresie identyfikacji oraz solidniejsze zabezpieczenia przed wyciekami dotyczącymi kont.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	n/d
7.10	Settings > System > Plain config > System > Web Interface Disabled (Ustawienia > System > Zwykła konfiguracja > System > Interfejs WWW wyłączony)
= 10.9	System > Plain config > System > Web Interface Disabled (System > Zwykła konfiguracja > System > Interfejs WWW wyłączony)

Konfigurowanie ustawień sieci IP, daty i godziny

CSC #4: CSC #8: Zarządzanie dziennikiem kontroli

CSC #12: Zarządzanie infrastrukturą siecią

Ważne jest, aby prawidłowo skonfigurować ustawienia sieci IP, daty i godziny w urządzeniu Axis celem zapewnienia jego funkcjonalności i bezpieczeństwa. Ustawienia te wpływają na różne aspekty działania urządzenia, w tym komunikację w sieci IP, rejestrowanie i weryfikację certyfikatów.

Konfiguracja IP urządzenia zależy od konfiguracji sieci, takiej jak IPv4/IPv6, statyczny lub dynamiczny (DHCP) adres sieciowy, maska podsieci i domyślny router. Przy każdorazowym dodawaniu nowych komponentów należy sprawdzić topologię sieci. Zaleca się korzystanie ze statycznych adresów IP celem zapewnienia dostępności sieci i zminimalizowania zależności od serwerów sieciowych, takich jak serwery DHCP, które mogą być podatne na ataki.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > Basic Setup > TCP/IP (Konfiguracja > Podstawowa konfiguracja > TCP/IP)
7.10	Settings > System > TCP/IP (Ustawienia > System > TCP/IP)
= 10.9	System > Network (System > Sieć)

Dokładne wskazanie czasu jest niezbędne do prowadzenia dzienników systemowych, weryfikacji certyfikatów cyfrowych i włączenia usług takich jak HTTPS, IEEE i 802.1x. Zaleca się synchronizację zegara urządzenia z serwerami NTP (Network Time Protocol) lub NTS (Network Time Security). NTS, szyfrowany i bezpieczny wariant protokołu NTP, został dodany w systemie operacyjnym AXIS OS 11.1. Zaleca się konfigurację wielu serwerów czasu celem zwiększenia dokładności i zmniejszenia zależności od potencjalnych awarii. W razie braku możliwości hostingu lokalnych serwerów czasu należy rozważyć użycie publicznych serwerów NTP lub NTS. Więcej informacji na temat NTP/NTS w urządzeniach Axis można znaleźć w temacie *NTP and NTS (NTP i NTS)* w AXIS OS Knowledge base (Bazie wiedzy o systemie AXIS OS).

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > Basic Setup > Date & Time (Konfiguracja > Ustawienia podstawowe > Data i godzina)
7.10	Settings > System > Date and time (Ustawienia > System > Data i godzina)
= 10.9	System > Date and time (System > Data i godzina)
= 11.6	System > Time and location (System > Czas i lokalizacja)

Szyfrowanie zasobu lokalnego

CSC #3: Ochrona danych

Karta SD

Jeżeli urządzenie Axis obsługuje i wykorzystuje karty SD do przechowywania nagrań, zaleca się ich szyfrowanie. Uniemożliwi to nieupoważnionym osobom odtwarzanie materiału wideo zapisanego na wyjętej karcie SD.

Więcej informacji na temat szyfrowania kart SD w urządzeniach Axis można znaleźć w temacie *Obsługa kart SD* w AXIS OS Knowledge base (Bazie wiedzy o systemie AXIS OS).

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Storage (Konfiguracja > Opcje systemowe > Zasób)
7.10	Settings > System > Storage (Ustawienia > System > Zasób)
= 10.9	System > Storage (System > Zasób)

Udział sieciowy (NAS)

Jeżeli udział sieciowy (NAS) wykorzystywany jest jako urządzenie zapisujące, zaleca się umieszczenie go w zamkniętym pomieszczeniu bądź szafie o ograniczonym dostępie i włączenie w nim szyfrowania dysku twardego. Urządzenia Axis wykorzystują SMB jako protokół sieciowy do łączenia się z sieciowym zasobem dyskowym w celu przechowywania nagrań wideo. Wcześniejsze wersje SMB (1.0 i 2.0) nie zapewniają żadnych zabezpieczeń ani szyfrowania, ale późniejsze (2.1 i nowsze) już tak, dlatego zalecamy korzystanie z tych drugich.

Aby dowiedzieć się więcej na temat prawidłowej konfiguracji SMB po podłączeniu urządzenia Axis do udziału sieciowego, zob. *Network share (Udział sieciowy)* w AXIS OS Knowledge base (Bazie wiedzy o systemie AXIS OS).

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Storage (Konfiguracja > Opcje systemowe > Zasób)
7.10	Settings > System > Storage (Ustawienia > System > Zasób)
= 10.9	System > Storage (System > Zasób)

Aplikacje (ACAP)

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy

Na urządzeniach Axis można instalować aplikacje w celu rozszerzenia ich funkcjonalności. Wiele z takich aplikacji ma wbudowany interfejs użytkownika do obsługi konkretnych funkcji. Aplikacje mogą korzystać z funkcji zabezpieczeń zapewnianych przez system AXIS OS.

W urządzeniach Axis fabrycznie instalowane są różne aplikacje firmy Axis zgodnie z *Modelem rozwoju zabezpieczeń AXIS (ASDM)*. Więcej informacji o aplikacjach Axis można znaleźć w temacie *Analytics (Analizy)* w witrynie axis.com.

W przypadku aplikacji innych firm zalecamy skontaktowanie się z ich dostawcami, aby uzyskać specyfikacje zabezpieczeń tych aplikacji w kontekście działania i dowiedzieć się, czy dana aplikacja została opracowana zgodnie z przyjętymi najlepszymi modelami rozwoju zabezpieczeń. W przypadku wykrycia luk w zabezpieczeniach aplikacji zewnętrznej należy zgłaszać je do dostawcy takiego oprogramowania.

Zalecamy korzystanie tylko z zaufanych aplikacji i usuwanie z urządzeń Axis nieużywanego oprogramowania.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > Applications (Konfiguracja > Aplikacje)
7.10	Settings > Apps (Ustawienia > Aplikacje)
= 10.9	Aplikacje

Wyłączanie nieużywanych usług lub funkcji

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy

Nawet jeśli nieużywane usługi i funkcje nie stanowią bezpośredniego zagrożenia dla bezpieczeństwa, warto je wyłączać, aby maksymalnie ograniczać niepotrzebne ryzyko. Czytaj dalej, aby dowiedzieć się więcej o usługach i funkcjach, które można wyłączyć, jeśli nie są używane.

Nieużywane fizyczne porty sieciowe

Urządzenia z wieloma portami sieciowymi i systemem AXIS OS 11.2 lub nowszym, takie jak AXIS S3008, są wyposażone w opcję wyłączenia na portach sieciowych zarówno PoE, jak i ruchu sieciowego. Pozostawienie tych portów włączonych i bez nadzoru stwarza poważne zagrożenie bezpieczeństwa.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	n/d
7.10	n/d
= 11.2	System > Power over Ethernet

Protokoły wykrywania sieci

Protokoły wykrywania, takie jak Bonjour, UPnP, ZeroConf, WS-Discovery i LLDP/CDP, pełnią funkcję pomocniczą, ułatwiając znalezienie w sieci urządzenia Axis i jego usług. Po wdrożeniu urządzenia i dodaniu go w VMS zalecamy wyłączenie protokołu wykrywania, aby urządzenie Axis przestało rozgłaszać swoją obecność w sieci.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Advanced > Plain Config > Network > Network Bonjour Enabled, Network UPnP Enabled, Network ZeroConf Enabled, Network UPnP NATTraversal Enabled* (Konfiguracja > Opcje systemowe > Zaawansowane > Zwykła konfiguracja > Sieć > Sieć Bonjour włączony, Sieć UPnP włączony, Sieć ZeroConf włączony, Sieć UPnP NATTraversal włączony*)
	n/d
7.10	Settings > System > Plain Config > Network > Network Bonjour Enabled, Network UPnP Enabled, Network ZeroConf Enabled, Network UPnP NATTraversal Enabled* (Ustawienia > System > Zwykła konfiguracja > Sieć > Sieć Bonjour włączony, Sieć UPnP włączony, Sieć ZeroConf włączony, Sieć UPnP NATTraversal włączony*)
	Settings > System > Plain config > WebService > Discovery Mode (Ustawienia > System > Zwykła konfiguracja > Usługa sieciowa > Tryb wykrywania)

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
= 10.9	Settings > Plain config > Network > Bonjour Enabled, UPnP Enabled, ZeroConf Enabled (Ustawienia > Zwykła konfiguracja > Sieć > Bonjour włączony, UPnP włączony, ZeroConf włączony)
	System > Plain config > WebService > DiscoveryMode > Enable WS-Discovery discoverable mode (System > Zwykła konfiguracja > Usługa sieciowa > Tryb wykrywania > Włącz tryb wykrywania za pomocą protokołu WS-Discovery)
≥ 11.11	System > Network > Network discovery protocols > LLDP and CDP (System > Sieć > Protokoły wykrywania sieci > LLDP i CDP)**

* Ta funkcja została wycofana z systemu AXIS OS 10.12 i nie jest dostępna w nowszych wersjach.

** Wyłączenie funkcji LLDP and CDP może wpływać na negocjowanie zasilania z PoE.

Przestarzałe wersje TLS

Przed rozpoczęciem korzystania z urządzenia Axis, zalecamy wyłączenie starych, przestarzałych i niezabezpieczonych wersji TLS. Przestarzałe wersje TLS są zazwyczaj domyślnie wyłączone. Można je jednak włączyć w urządzeniach Axis, aby zapewnić zgodność wsteczną z aplikacjami zewnętrznymi, które jeszcze nie obsługują protokołów TLS 1.2 i TLS 1.3.

Przestarzałe wersje TLS zostały usunięte z systemu AXIS OS 12.0 i nie są dostępne w nowszych wersjach.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Advanced > Plain Config > HTTPS > Allow TLSv1.0 (Konfiguracja > Opcje systemowe > Zaawansowane > Zwykła konfiguracja > HTTPS > Zezwalaj na TLSv1.0) i/lub Allow TLSv1.1 (Zezwalaj na TLSv1.1)
7.10	Settings > System > Plain config > HTTPS > Allow TLSv1.0 (Konfiguracja > System > Zwykła konfiguracja > HTTPS > Zezwalaj na TLSv1.0) i/lub Allow TLSv1.1 (Zezwalaj na TLSv1.1)
= 10.9	System > Plain config > HTTPS > Allow TLSv1.0 (System > Zwykła konfiguracja > HTTPS > Zezwalaj na TLSv1.0) i/lub Allow TLSv1.1 (Zezwalaj na TLSv1.1)

Środowisko edytora skryptów

Zalecamy wyłączenie dostępu do środowiska edytora skryptów. Edytor skryptów służy wyłącznie do rozwiązywania problemów i debugowania.

Edytor skryptów został wycofany z systemu AXIS OS w wersji 10.11 i nie jest dostępny w nowszych wersjach.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	n/d
7.10	Settings > System > Plain config > System > Enable the script editor (editcgi) (Ustawienia > System > Zwykła konfiguracja > System > Włącz opcję edytora skryptów (editcgi))
= 10.9	System > Plain config > System > Enable the script editor (editcgi) (System > Zwykła konfiguracja > System > Włącz opcję edytora skryptów (editcgi))

Nagłówki serwerów HTTP(S)

Domyślnie urządzenia Axis ogłaszają swoje bieżące wersje Apache i OpenSSL podczas połączeń HTTP(S) z klientami w sieci. Informacje te przydają się podczas regularnego korzystania ze skanerów bezpieczeństwa sieci, ponieważ zapewniają bardziej szczegółowy raport o istniejących lukach w określonej wersji systemu AXIS OS.

Można wyłączyć nagłówki serwera HTTP(S), aby ograniczyć ryzyko ujawnienia informacji podczas połączeń HTTP(S). Zalecamy jednak wyłączanie nagłówków tylko pod warunkiem przestrzegania naszych zaleceń i regularnego aktualizowania urządzenia.

Opcja wyłączenia nagłówków serwera HTTP(S) jest dostępna w wersji AXIS OS 10.6 i nowszych.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	n/d
7.10	Settings > System > Plain config > System > HTTP Server Header Comments (Ustawienia > System > Zwykła konfiguracja > System > Komentarze nagłówka serwera HTTP)
= 10.9	System > Plain config > System > HTTP Server Header Comments (System > Zwykła konfiguracja > System > Komentarze nagłówka serwera HTTP)

Dźwięk

W produktach Axis do systemu dozoru wizyjnego, takich jak kamery sieciowe, funkcje wejścia/wyjścia audio i mikrofonu są domyślnie wyłączone. Aby korzystać z funkcji audio, trzeba je włączyć. W produktach Axis, w których najważniejszymi funkcjami są wejście/wyjście audio oraz mikrofon, np. w interkomach i głośnikach sieciowych Axis, funkcje audio są domyślnie włączone.

Zalecamy wyłączanie nieużywanych funkcji audio.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Advanced > Plain Config > Audio > Audio A* > Enabled (Konfiguracja > Opcje systemowe > Zaawansowane > Zwykła konfiguracja > Audio > Audio A* > Włączone)
7.10	Settings > Audio > Allow audio (Ustawienia > Audio > Zezwalaj na audio)
= 10.9	Audio > Device settings (Audio > Ustawienia urządzenia)

Sloty kart SD

Zazwyczaj urządzenia Axis obsługują co najmniej jedną kartę SD, aby zapewnić możliwość przechowywania nagrań wideo w zasobie lokalnym. W przypadku niekorzystania z kart SD zalecamy całkowite wyłączenie ich slotów. Opcja wyłączenia slotów kart SD jest dostępna w systemie AXIS OS 9.80 i nowszych

Więcej informacji można znaleźć w temacie *Disabling the SD card (Wyłączanie obsługi kart SD)* w AXIS OS Knowledge base (Bazie wiedzy o systemie AXIS OS).

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	n/d
7.10	Settings > System > Plain config > Storage > SD Disk Enabled (Ustawienia > System > Zwykła konfiguracja > Zasób > Dysku SD włączony)
= 10.9	System > Plain config > Storage > SD Disk Enabled (Ustawienia > Zwykła konfiguracja > Zasób > Dysku SD włączony)

Dostęp przez FTP

FTP to niezabezpieczony protokół komunikacyjny używany wyłącznie w celu rozwiązywania problemów i debugowania. Usunięto do niego dostęp począwszy od systemu operacyjnego AXIS OS 11.1, tak że nie jest dostępny w późniejszych wersjach. Zalecamy wyłączenie dostępu przez FTP i korzystanie z bezpiecznego dostępu przez SSH do celów rozwiązywania problemów.

Więcej informacji na temat protokołu SSH można znaleźć w temacie *SSH access (Dostęp przez SSH)* w AXIS OS Portal. Więcej informacji o opcjach debugowania za pomocą FTP można znaleźć w temacie *FTP access (Dostęp przez FTP)* w AXIS OS Portal.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Plain Config > Network > FTP Enabled (Konfiguracja > Opcje systemowe > Zwykła konfiguracja > Sieć > FTP włączony)
7.10	Settings > System > Plain config > Network > FTP Enabled (Ustawienia > System > Zwykła konfiguracja > Sieć > FTP włączony)
= 10.9	System > Plain config > Network > FTP Enabled (System > Zwykła konfiguracja > Sieć > FTP włączony)

Dostęp przez SSH

SSH jest zabezpieczonym protokołem komunikacyjnym, który służy wyłącznie do debugowania i rozwiązywania problemów. Jest obsługiwany przez urządzenia Axis, począwszy od systemu operacyjnego AXIS OS 5.50. Zaleca się wyłączenie dostępu SSH.

Więcej informacji o opcjach debugowania przy użyciu protokołu SSH można znaleźć w temacie *SSH access (Dostęp przez SSH)* w AXIS OS Knowledge base (Bazie wiedzy o systemie AXIS OS).

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Plain Config > Network > SSH Enabled (Konfiguracja > Opcje systemowe > Zwykła konfiguracja > Sieć > SSH włączony)
7.10	Settings > System > Plain config > Network > SSH Enabled (Ustawienia > System > Zwykła konfiguracja > Sieć > SSH włączony)
= 10.9	System > Plain config > Network > SSH Enabled (System > Zwykła konfiguracja > Sieć > SSH włączony)

Dostęp przez Telnet

Telnet jest niezależnym protokołem komunikacji przeznaczonym wyłącznie do debugowania i rozwiązywania problemów. Jest obsługiwany przez urządzenia Axis w wersjach wcześniejszych niż system operacyjny AXIS OS 5.50. Zaleca się wyłączenie dostępu Telnet.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 5.50	Szczegółowe instrukcje można znaleźć w temacie <i>Device access (Dostęp do urządzeń)</i> w AXIS OS Knowledge base (Bazie wiedzy o systemie AXIS OS).
< 7.10	n/d
7.10	n/d
= 10.9	n/d

ARP/Ping

ARP/Ping jest metodą ustawiania adresu IP urządzenia Axis za pomocą narzędzi, takich jak AXIS IP Utility. Ta funkcja została wycofana z systemu AXIS OS 7.10 i w nowszych wersjach nie jest dostępna. Zalecamy wyłączenie jej w urządzeniach Axis z systemem AXIS OS 7.10 lub starszym.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Advanced > Plain Config > Network > ARP/Ping (Konfiguracja > Opcje systemowe > Zaawansowane > Zwykła konfiguracja > Sieć > ARP/Ping)
7.10	n/d
= 10.9	n/d

USB

Począwszy od systemu operacyjnego w wersji AXIS OS 12.1 dekodery AXIS D1110 wyposażony jest w opcję wyłączenia portu USB. Pozostawienie nieużywanych portów USB włączonych i bez nadzoru stwarza poważne zagrożenie bezpieczeństwa.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	n/d
7.10	n/d
≥ 12.1	System > > Accessories (Akcesoria) > USB Configuration (Konfiguracja USB)

Hostowana zaporą sieciowa

CSC #1: Inwentaryzacja i kontrola zasobów firmy

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy

CSC #13: Monitorowanie i ochrona sieci IP

Wprowadzona w systemie operacyjnym w wersji AXIS OS 11.9 zaporą sieciowa oparta na hoście to funkcja zabezpieczeń umożliwiająca tworzenie zasad regulujących ruch przychodzący według adresów IP lub numerów portów TCP / UDP. Zaporą wspomaga ochronę przed nieautoryzowanym dostępem do urządzenia lub jego usług.

Jeśli ustawisz zasadę domyślną „Odmów”, pamiętaj o dodaniu do listy wszystkich autoryzowanych klientów (VMS i klientów administracyjnych) lub portów.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
≥ 11.9	Ustawienia > Bezpieczeństwo > Zaporą sieciowa

Filtrowanie adresów IP

Urządzenia z systemem operacyjnym w wersji AXIS OS 11.8 i wersjach wcześniejszych wykorzystują filtrowanie adresów IP celem odmowy dostępu nieautoryzowanym klientom. Zaleca się skonfigurowanie urządzenia w taki sposób, aby zezwalało na adresy IP autoryzowanych hostów albo odrzucało adresy nieautoryzowane.

W przypadku zezwolenia na obsługę adresów IP należy dodać wszystkich autoryzowanych klientów (obejmujących serwery VMS i klientów administracyjnych) do listy.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Security > IP Address Filter (Konfiguracja > Opcje systemowe > Zabezpieczenia > Filtr adresów IP)
7.10	Settings > System > TCP/IP > IP address filter (Ustawienia > System > TCP/IP > Filtr adresów IP)
10.9 – 11.8	Settings > Security > IP address filter (Ustawienia > Zabezpieczenia > Filtr adresów IP)

Uwaga

Można włączyć bardziej szczegółowe dzienniki prób dostępu do sieci IP, by móc identyfikować niepożądane próby dostępu z innych hostów sieciowych. Aby włączyć dzienniki, przejdź do **System > Plain config** (Prosta konfiguracja) > **Network** (Sieć IP) i **Network Filter Log** (Dziennik filtrów sieciowych).

HTTPS

CSC #3: Ochrona danych

Protokoły HTTP i HTTPS są domyślnie włączone w urządzeniach Axis, począwszy od systemu operacyjnego w wersji AXIS OS 7.20. O ile dostęp przez protokół HTTP jest niezabezpieczony żadnym szyfrowaniem, protokół

HTTPS szyfruje ruch pomiędzy klientem a urządzeniem Axis. Do realizacji wszystkich zadań administracyjnych w urządzeniu Axis zalecamy używanie protokołu HTTPS.

Instrukcje konfiguracji można znaleźć na stronach i .

Tylko HTTPS

Zalecamy skonfigurowanie w urządzeniach Axis korzystania tylko z protokołu HTTPS (bez obsługi dostępu HTTP). Takie ustawienie powoduje automatyczne włączenie HSTS (HTTP Strict Transport Security) i dodatkowo wzmacnia zabezpieczenia urządzenia.

Urządzenia Axis z systemem AXIS OS 7.20 i nowszymi są wyposażone w certyfikat z własnym podpisem. Mimo że z założenia certyfikat z własnym podpisem nie jest zaufany, zapewnia on bezpieczny dostęp do urządzenia Axis w fazie początkowej konfiguracji oraz w scenariuszach bez dostępnej infrastruktury klucza publicznego (PKI). Jeśli klucz publiczny jest dostępny, certyfikat z własnym podpisem należy usunąć i zastąpić go odpowiednimi podpisanymi certyfikatami klienta wystawionymi przez wybrany PKI. W systemach AXIS OS 10.10 i nowszych certyfikat z własnym podpisem został zastąpiony certyfikatem bezpiecznego identyfikatora urządzenia IEEE 802.1AR.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Security > HTTPS (Konfiguracja > Opcje systemowe > Zabezpieczenia > HTTPS)
7.10	Settings > System > Security > HTTP and HTTPS (Ustawienia > System > Zabezpieczenia > HTTP i HTTPS)
= 10.9	System > Network > HTTP and HTTPS (System > Sieć > HTTP i HTTPS)

Szyfry HTTPS

Urządzenia Axis obsługują i wykorzystują zestawy szyfrów TLS 1.2 i TLS 1.3 do bezpiecznego szyfrowania połączeń HTTPS. Konkretna wersja protokołu TLS oraz używany zestaw szyfrów zależą od klienta łączącego się z urządzeniem Axis i są one odpowiednio wynegocjowane. Podczas regularnych aktualizacji systemu operacyjnego AXIS OS lista dostępnych szyfrów urządzenia Axis może być aktualizowana bez zmiany rzeczywistej konfiguracji szyfru. Zmiana konfiguracji szyfru musi być zainicjowana przez użytkownika, poprzez zastosowanie fabrycznych ustawień domyślnych urządzenia Axis lub poprzez ręczną konfigurację. Od wersji AXIS OS 10.8 lista szyfrów jest automatycznie aktualizowana, gdy użytkownik wykona aktualizację AXIS OS.

TLS 1.2 i starsze

W przypadku korzystania z protokołu TLS 1.2 lub starszego można określić szyfry HTTPS, które będą używane przez urządzenie Axis po ponownym uruchomieniu. Nie ma ograniczeń co do szyfrów, które można wybrać, ale zalecamy wybranie dowolnego z lub wszystkich poniższych silnych szyfrów:

ECDHE-ECDHE-AES128-GCM-SHA256 : ECDHE-RSA-AES128-GCM-SHA256 : ECDHE-ECDHE-AES256-GCM-SHA384 : ECDHE-RSA-AES256-GCM-SHA384 : ECDHE-ECDHE-CHACHA20-POLY1305 : ECDHE-RSA-CHACHA20-POLY1305

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Advanced > Plain Config > HTTPS > Ciphers (Konfiguracja > Opcje systemowe > Zaawansowane > Zwykła konfiguracja > HTTPS > Szyfry)
7.10	Settings > System > Plain config > HTTPS > Ciphers (Ustawienia > System > Zwykła konfiguracja > HTTPS > Szyfry)
= 10.9	System > Plain config > HTTPS > Ciphers (System > Zwykła konfiguracja > HTTPS > Szyfry)

TLS 1.3

Domyślnie dostępne są tylko silne zestawy szyfrów zgodne ze specyfikacją TLS 1.3:

TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_256_GCM_SHA384

Użytkownik nie może ich konfigurować.

Dziennik dostępu

CSC #1: Inwentaryzacja i kontrola zasobów firmy

CSC #8: Zarządzanie dziennikiem kontroli

Dziennik dostępu zawiera szczegółowe dzienniki użytkowników uzyskujących dostęp do urządzenia Axis, co ułatwia zarówno przeprowadzanie audytów, jak i zarządzanie kontrolą dostępu. Zalecamy włączenie tej funkcji i połączenie jej ze zdalnym serwerem dziennika systemowego. Dzięki temu urządzenie Axis będzie mogło wysyłać swoje dzienniki do centralnego środowiska rejestracji. Ułatwia to przechowywanie komunikatów dziennika i przestrzeganie reguł dotyczących czasu ich przechowywania.

Więcej informacji można uzyskać, przechodząc do tematu *Device access logging (Rejestrowanie dostępu do urządzenia)* w AXIS OS Knowledge base (Bazie wiedzy o systemie AXIS OS).

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Advanced > Plain Config > System > Access log (Konfiguracja > Opcje systemowe > Zaawansowane > Zwykła konfiguracja > System > Dziennik dostępu)
7.10	Settings > System > Plain config > System > Access log (Ustawienia > System > Zwykła konfiguracja > System > Dziennik dostępu)
= 10.9	System > Plain config > System > Access log (System > Zwykła konfiguracja > System > Dziennik dostępu)

Fizyczne akcesoria antysabotażowe

CSC #1: Inwentaryzacja i kontrola zasobów firmy

CSC #12: Zarządzanie infrastrukturą sieciową

Aby wzmocnić fizyczną ochronę urządzeń Axis, można dodać do nich fizyczne przełączniki antywłamaniowe lub antysabotażowe. Przełączniki te mogą wyzwać alarmy, co pozwala urządzeniom Axis wysyłać powiadomienia lub alarmy do wybranych klientów.

Więcej informacji o ofercie akcesoriów antysabotażowych można znaleźć w tematach:

- *AXIS TA8501 Physical Tampering Switch*
- *AXIS Dome Intrusion Switch C*
- *Wyłącznik drzwiowy AXIS A*

Rozszerzone zabezpieczenia

Instrukcje rozszerzania zabezpieczeń można znaleźć w poświęconych im tematach na stronach i . Instrukcje wdrażania zabezpieczeń domyślnych i podstawowych można zastosować bezpośrednio w urządzeniu Axis, natomiast zbudowanie rozszerzonych zabezpieczeń wymaga aktywnego udziału całego łańcucha dostaw dostawcy, organizacji użytkownika końcowego oraz odpowiedniej infrastruktury informatycznej lub sieciowej.

Ograniczenie narażenia w internecie i sieci IP

CSC #12: Zarządzanie infrastrukturą sieciową

Zaleca się nie udostępniać (a tym samym nie powodować narażenia na ataki) urządzenia Axis jako publicznego serwera WWW lub w jakikolwiek inny sposób zezwalać nieznanym klientom na dostęp przez sieć IP do urządzenia. Na potrzeby małych firm i osób prywatnych, które nie korzystają z oprogramowania do zarządzania obrazem (VMS) lub oczekują zdalnego dostępu do obrazu, dobrym rozwiązaniem jest oprogramowanie AXIS Camera Station Edge.

AXIS Camera Station Edge dostępne jest bezpłatnie na systemy Windows, iOS oraz Android i zapewnia bezpieczny dostęp do obrazu z systemu dozorowego bez udostępniania urządzenia w internecie. Dalsze informacje znajdują się na stronie axis.com/products/axis-camera-station-edge.

Uwaga

W przypadku korzystania z systemu VMS należy zwrócić się do dostawcy systemu VMS po wytyczne w zakresie zdalnego dostępu do obrazu.

Odizolowanie urządzeń sieciowych oraz powiązanej infrastruktury i aplikacji zmniejsza ryzyko narażenia na ataki przy pracy w sieci IP.

Zaleca się odizolowanie urządzeń Axis oraz powiązanej infrastruktury i aplikacji w sieci lokalnej, która nie ma połączenia z siecią wykorzystywaną w środowisku produkcyjnym i biznesowym.

Aby zapewnić podstawowy poziom zabezpieczeń, należy chronić sieć lokalną i jej infrastrukturę (ruter, przełączniki sieciowe) przed nieautoryzowanym dostępem, dodając wielowarstwowe mechanizmy bezpieczeństwa sieciowego. Mogą one obejmować segmentację na sieć VLAN, ograniczone możliwości routingu, VPN dla dostępu lokalizacja-lokalizacja lub WAN, zapory sieciowe warstwy 2 / 3 oraz listy kontroli dostępu (ACL).

Aby rozszerzyć podstawowy poziom zabezpieczeń, należy zastosować zaawansowane techniki inspekcji sieci w rodzaju głębokiej inspekcji pakietów i wykrywania włamań. Zwiększy to ochronę przed zagrożeniami w sieci IP. Rozszerzony poziom zabezpieczeń sieciowych wymaga zazwyczaj specjalistycznego oprogramowania lub sprzętu.

Skanowanie luk w zabezpieczeniach sieci

CSC #1: Inwentaryzacja i kontrola zasobów firmy

CSC #12: Zarządzanie infrastrukturą sieciową

Skanery zabezpieczeń sieci pozwalają oceniać podatność urządzeń sieciowych na zagrożenia. Ocena podatności na zagrożenia zapewnia systematyczne sprawdzanie potencjalnych luk w zabezpieczeniach i nieprawidłowych konfiguracji.

Zalecamy regularne sprawdzanie urządzeń Axis i powiązanej z nimi infrastruktury pod kątem podatności na ataki. Przed skanowaniem warto upewnić się, że w urządzeniach Axis zostały zainstalowane najnowsze wersje systemu AXIS OS (LTS lub aktywna ścieżka).

Zalecamy także przejrzanie raportu skanowania i odfiltrowanie znanych fałszywych alarmów występujących w urządzeniach Axis, które można znaleźć w *AXIS OS Vulnerability Scanner Guide (Przewodniku do skanera podatności systemu AXIS OS na ataki)*. Raport i ewentualne dodatkowe uwagi należy dołączyć do zgłoszenia pomocy technicznej i przesłać do *Axis support (Pomoc techniczna Axis)* w witrynie axis.com.

Zaufana infrastruktura kluczy publicznych (PKI)

CSC #3: Ochrona danych

CSC #12: Zarządzanie infrastrukturą sieciową

Zalecamy wdrożenie na urządzeniach Axis certyfikatów serwera WWW i klienta, które są zaufane i podpisane przez publiczne lub prywatne centrum certyfikacji (CA). Certyfikat podpisany przez Urząd Certyfikacji (UC) wraz ze zweryfikowanym łańcuchem zaufania pozwala usunąć ostrzeżenia o certyfikatach przeglądarki przy połączeniu przez protokół HTTPS. Certyfikat podpisany przez UC zapewnia również uwierzytelnienie urządzenia Axis przy wdrażaniu rozwiązania kontroli dostępu sieciowego (NAC). Zmniejsza to ryzyko ataków ze strony komputera podszywającego się pod urządzenie Axis.

Aplikacja AXIS Device Manager z wbudowaną usługą CA umożliwia wystawianie urządzeniom Axis podpisanych certyfikatów.

Zdalny dziennik systemowy

CSC #8: Zarządzanie dziennikiem kontroli

W urządzeniu Axis można skonfigurować wysyłanie wszystkich komunikatów dziennika w formie zaszyfrowanej do centralnego serwera dziennika systemowego. Ułatwia to przeprowadzanie audytów i zapobiega celowemu, złośliwemu lub przypadkowemu usunięciu komunikatów dziennika z urządzenia Axis. W zależności od zasad firmy opcja ta może również zapewniać dłuższy czas przechowywania dzienników urządzeń.

Więcej informacji o włączaniu zdalnego serwera dziennika systemowego w różnych wersjach systemu AXIS OS można znaleźć w temacie *Syslog (Dziennik systemu)* w AXIS OS Knowledge base (Bazie wiedzy o systemie AXIS OS).

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Instrukcje można znaleźć w temacie <i>Syslog (Dziennik systemu)</i> w AXIS OS Portal
7.10	Settings > System > TCP/IP (Ustawienia > System > TCP/IP)
= 10.9	System > Logs (System > Dzienniki)

Zabezpieczone przesyłanie strumienia wideo (SRTP/RTSPS)

CSC #3: Ochrona danych

Począwszy od wersji systemu operacyjnego AXIS OS 7.40 urządzenia Axis obsługują bezpieczne strumieniowanie wizyjne przez protokół RTP, określane również jako SRTP / RTSPS. SRTP / RTSPS wykorzystuje bezpieczną, szyfrowaną metodę transportu end-to-end, po to by strumień wizyjny z urządzenia Axis otrzymali wyłącznie autoryzowani klienci. Jeśli VMS go obsługuje, zalecamy włączenie protokołu SRTP/RTSPS. Jeśli tylko jest to możliwe, należy używać protokołu SRTP zamiast nieszyfrowanego przesyłania strumienia wideo RTP.

Uwaga

Protokół SRTP/RTSPS szyfruje tylko dane strumienia wideo. Jeżeli chodzi o zadania konfiguracji administracyjnej, to zalecamy włączenie protokołu HTTPS tylko w celu szyfrowania tego typu komunikacji.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Advanced > Plain Config > Network > RTSPS (Konfiguracja > Opcje systemowe > Zaawansowane > Zwykła konfiguracja > Sieć > RTSPS)
7.10	Settings > System > Plain config > Network > RTSPS (Ustawienia > System > Zwykła konfiguracja > Sieć > RTSPS)
= 10.9	System > Plain config > Network > RTSPS (System > Zwykła konfiguracja > Sieć > RTSPS)

Podpisany materiał wizyjny

CSC #3: Ochrona danych

Podpisane wideo jest obsługiwane na urządzeniach Axis z systemem AXIS OS 10.11 lub nowszym i rozwiązaniem Axis Edge Vault. Urządzenia Axis obsługujące podpisane wideo mogą dodawać podpis do swojego strumienia wideo, aby zapewnić, że materiał wizyjny jest przekazywany w stanie nienaruszonym. Mogą również weryfikować jego pochodzenie poprzez prześledzenie jego ścieżki wstecz, aż do urządzenia źródłowego, które zarejestrowało nagranie. Systemy zarządzania materiałem wizyjnym (VMS) lub dowodami (EMS) mogą także weryfikować autentyczność obrazu wideo dostarczonego przez urządzenie Axis.

Więcej informacji znajduje się w oficjalnym dokumencie *Axis Edge Vault*. Aby znaleźć główne certyfikaty Axis używane do weryfikacji autentyczności podpisanego wideo, zobacz *Device access (Dostęp do urządzeń)* w AXIS OS Knowledge base (Bazie wiedzy o systemie AXIS OS).

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	n/d
7.10	n/d
= 10.9	System > Plain config > Image > SignedVideo (System > Zwykła konfiguracja > Obraz > Podpisane wideo)

Instrukcja szybkiego startu

W Skróconym przewodniku można znaleźć podsumowanie ustawień, które należy skonfigurować na etapie zabezpieczania urządzeń Axis z systemem AXIS OS 5.51 lub nowszym. Obejmuje on tematy dotyczące zabezpieczeń, o których można przeczytać na stronie , ale nie omawia tematów zawartych na stronie , ponieważ wymagają one zaawansowanej konfiguracji specyficznej dla klienta.

W celu szybkiego i ekonomicznego zabezpieczenia wielu urządzeń Axis zalecamy korzystanie z narzędzia AXIS Device Manager. W razie konieczności użycia innej aplikacji do konfiguracji urządzenia lub jeśli chcesz wzmocnić zabezpieczenia tylko kilku urządzeń Axis, zalecamy skorzystanie z interfejsu programowania aplikacji (API) VAPIX.

Typowe błędy konfiguracji

Uwaga

Typowe błędy konfiguracji wymienione poniżej potencjalnie zwiększają podatność urządzenia Axis na ataki i zmniejszają jego warstwy cyberbezpieczeństwa, co skutkuje wyższym ryzykiem wykorzystania luk, niewłaściwego użycia lub niezabezpieczonej obsługi urządzenia.

Urządzenia narażone na zagrożenia w internecie

CSC #12: Zarządzanie infrastrukturą sieciową

Nie zalecamy udostępniania urządzeń Axis jako publicznych serwerów WWW ani w inny sposób udzielania nieznanym klientom dostępu sieciowego do urządzenia. Więcej informacji znajduje się w rozdziale .

Jedno hasło do wszystkich urządzeń

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy

CSC #5: Zarządzanie kontem

Zdecydowanie zalecamy używanie unikalnego hasła dla każdego urządzenia zamiast jednego hasła do wszystkich urządzeń. Instrukcje można znaleźć na stronach i .

Anonimowy dostęp

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy

CSC #5: Zarządzanie kontem.

Nie zalecamy zezwalania użytkownikom na dostęp do ustawień wideo i konfiguracji urządzenia bez logowania się. Więcej informacji znajduje się w rozdziale .

Wyłączenie bezpiecznej komunikacji

CSC #3: Ochrona danych

Nie zalecamy korzystania z urządzenia przy użyciu niezabezpieczonych metod komunikacji i dostępu, takich jak HTTP lub podstawowe uwierzytelnianie obejmujące przesyłanie nieszyfrowanych haseł. Więcej informacji znajduje się w rozdziale . Zalecenia dotyczące konfiguracji: .

Nieaktualna wersja systemu operacyjnego AXIS OS

CSC #2: Inwentaryzacja i kontrola zasobów oprogramowania

Zdecydowanie zalecamy korzystanie z urządzenia Axis z najnowszą wersją systemu operacyjnego AXIS OS, na ścieżce LTS lub aktywnej. Obie ścieżki zawierają najnowsze łatki zabezpieczeń i poprawki błędów. Więcej informacji znajduje się w rozdziale .

Wdrażanie podstawowych zabezpieczeń za pomocą interfejsu programowania aplikacji (API) VAPIX

Za pomocą interfejsu programowania aplikacji (API) VAPIX można wzmocnić zabezpieczenia urządzeń Axis na podstawie informacji podanych na stronie . W tej tabeli znajdują się wszystkie podstawowe ustawienia konfiguracji zabezpieczeń obowiązujące bez względu na wersję systemu AXIS OS urządzenia Axis.

Niektóre ustawienia konfiguracji mogą nie być już dostępne w wersji systemu AXIS OS urządzenia. Jest to spowodowane wycofaniem części funkcji w celu poprawy bezpieczeństwa. Jeśli próba wywołania VAPIX powoduje błąd, może to oznaczać, że ta funkcja nie jest już dostępna w zainstalowanej wersji systemu AXIS OS.

Przeznaczenie	Wywołanie interfejsu programowania aplikacji (API) VAPIX
Wyłączanie POE w nieużywanych portach sieciowych*	<code>http://ip-address/axis-cgi/nvr/poe/setportmode.cgi?port=X&enabld=no</code>
Wyłączenie ruchu sieciowego w nieużywanych portach sieciowych**	<code>http://ip-address/axis-cgi/network_settings.cgi</code> <code>{ "apiVersion": "1.17", "method": "setDeviceConfiguration", "params": { "deviceName": "eth1.1", "staticState": "down" } }</code>
Wyłączanie protokołu wykrywania Bonjour	<code>https://ip-address/axis-cgi/param.cgi?action=update&Network.Bonjour.Enabled=no</code>
Wyłączanie protokołu wykrywania UPnP	<code>https://ip-address/axis-cgi/param.cgi?action=update&Network.UPnP.Enabled=no</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&Network.UPnP.NATTraversal.Enabled=no</code>
Wyłączanie protokołu wykrywania WebService	<code>https://ip-address/axis-cgi/param.cgi?action=update&WebService.DiscoveryMode.Discoverable=no</code>
Wyłączanie łączenia z chmurą jednym kliknięciem (O3C)	<code>https://ip-address/axis-cgi/param.cgi?action=update&RemoteService.Enabled=no</code>
Wyłączanie dostępu serwisowego do urządzenia przez SSH	<code>https://ip-address/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no</code>
Wyłączanie dostępu serwisowego do urządzenia przez FTP	<code>https://ip-address/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no</code>
Wyłączanie konfiguracji adresu IP ARP-Ping	<code>https://ip-address/axis-cgi/param.cgi?action=update&Network.ARPPingIPAddress.Enabled=no</code>
Wyłączanie konfiguracji adresu IP Zero-Conf	<code>http://ip-address/axis-cgi/param.cgi?action=update&Network.ZeroConf.Enabled=no</code>
Włączanie tylko HTTPS	<code>https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.admin=https</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.operator=https</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.viewer=https</code>
Włączanie tylko TLS 1.2 i TLS 1.3	<code>https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS1=no</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS11=no</code>

Przeznaczenie	Wywołanie interfejsu programowania aplikacji (API) VAPIX
<i>Konfiguracja bezpiecznego szyfrowania TLS 1.2</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.Ciphers=ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384</code>
<i>Włączanie zabezpieczenia przed atakami typu brute-force***</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.ActivatePasswordThrottling=on</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSBlockingPeriod=10</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageCount=20</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageInterval=1</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteCount=20</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteInterval=1</code>
<i>Wyłączanie środowiska edytora skryptów</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&System.EditCgi=no</code>
<i>Włączanie udoskonalonego rejestrowania dostępu użytkowników</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&System.AccessLog=On</code>
<i>Włączanie zabezpieczenia przed atakami powtórzeniowymi na ONVIF</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&WebService.UsernameToken.ReplayAttackProtection=yes</code>
<i>Wyłączanie dostępu do interfejsu WWW urządzenia</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&System.WebInterfaceDisabled=yes</code>
<i>Wyłączanie nagłówka serwera HTTP/OpenSSL</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&System.HTTPServerTokens=no</code>
<i>Wyłączanie dostępu anonimowych użytkowników i PTZ</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&root.Network.RTSP.ProtViewer=password</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&root.System.BoaProtViewer=password</code>

Przeznaczenie	Wywołanie interfejsu programowania aplikacji (API) VAPIX
	<code>https://ip-address/axis-cgi/param.cgi?action=update&root.PTZ.BoaProtPTZOperator=password</code>
<i>Zapobieganie instalacji uprawnień roota wymagających aplikacji ACAP</i>	<code>http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowRoot&value=false</code>
<i>Zapobieganie instalacji niepodpisanych aplikacji ACAP</i>	<code>http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowUnsigned&value=false</code>

* Zastąpić „X” rzeczywistym numerem portu w sekcji „port=X”. Przykłady: „port=1” powoduje wyłączenie portu 1, a „port=2” wyłączenie portu 2.

** Zastąpić „1” rzeczywistym numerem portu w sekcji „eth1.1”. Przykłady: „eth1.1” powoduje wyłączenie portu 1, a „eth1.2” wyłączenie portu 2.

*** Po 20 nieudanych próbach logowania w ciągu jednej sekundy adres IP klienta blokuje się na 10 s. Każde kolejne nieudane żądanie w ciągu 30 sekund spowoduje wydłużenie okresu blokowania DoS o kolejne 10 sekund.

Podstawowe zabezpieczenia ustawiane za pomocą AXIS Device Manager (Extend)

AXIS Device Manager i AXIS Device Manager Extend umożliwiają zabezpieczanie urządzeń Axis zgodnie z tematami omówionymi na stronie . Należy użyć tego *pliku konfiguracyjnego* zawierającego tę samą konfigurację, którą można znaleźć na stronie .

Niektóre ustawienia konfiguracji mogą nie być już dostępne w wersji systemu AXIS OS urządzenia. Jest to spowodowane wycofaniem części funkcji w celu poprawy bezpieczeństwa. AXIS Device Manager i AXIS Device Manager Extend automatycznie usuną te ustawienia z konfiguracji zabezpieczeń.

Uwaga

Po przesłaniu tego pliku konfiguracji urządzenie Axis zostanie skonfigurowane pod kątem używania tylko protokołu HTTPS, a interfejs WWW zostanie wyłączony. Plik konfiguracji można zmieniać pod kątem własnych potrzeb, np. poprzez usuwanie lub dodawanie parametrów.

Powiadomienia dotyczące zabezpieczeń

Zachęcamy do subskrypcji *usługi Axis security notification service*. Dzięki niej można otrzymywać informacje o nowo wykrytych lukach zabezpieczeń w produktach Axis, rozwiązaniach problemów i usługach, a także porady z zakresu dbania o bezpieczeństwo urządzeń Axis.

