AXIS OS Hardening Guide

AXIS OS Portal (Portal poświęcony systemowi AXIS OS) | *AXIS OS Release Notes (Uwagi dotyczące wersji systemu AXIS OS)* |
AXIS OS Knowledge base (Baza wiedzy do systemu AXIS OS) |
AXIS OS Security Advisories (Ostrzeżenia dotyczących bezpieczeństwa AXIS OS)|
AXIS OS YouTube playlist (Lista odtwarzania na YouTube filmów dotyczących systemu AXIS OS)

AXIS OS Hardening Guide

Wprowadzenie

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 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.

Konfiguracja interfejsu WWW
W tym 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)

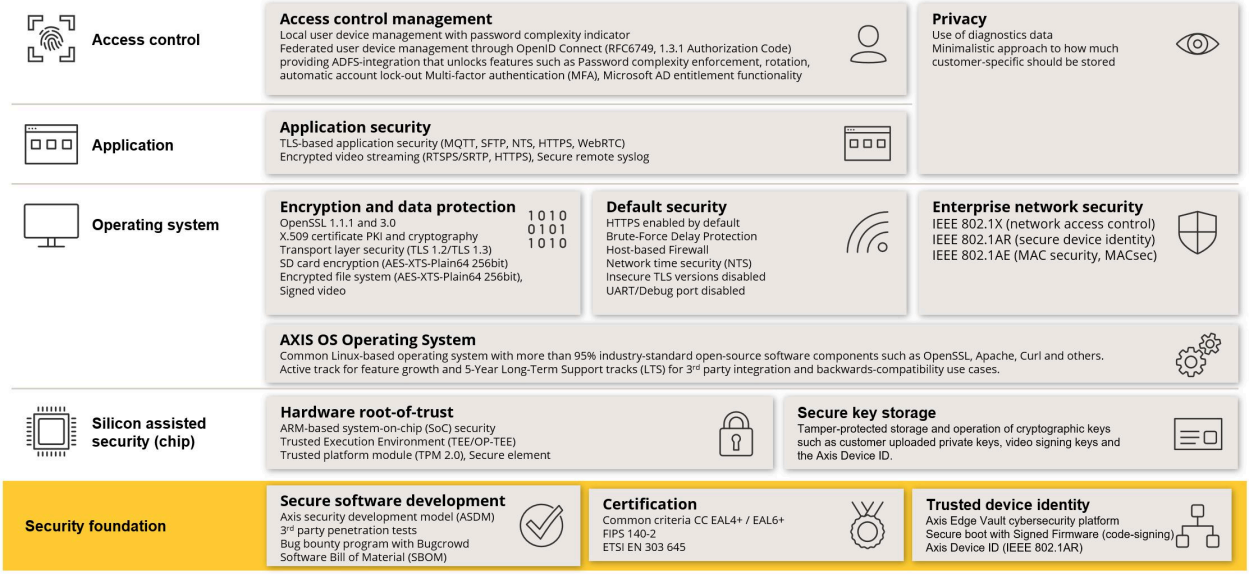
Zakres

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

Wprowadzenie

Architektura zabezpieczeń systemu AXIS OS

Schemat architektury zabezpieczeń systemu AXIS OS przedstawia jego możliwości w zakresie cyberbezpieczeństwa w poszczególnych warstwach. Diagram stanowi kompleksowy widok podstaw bezpieczeństwa, zawierający zabezpieczenia oparte na procesorze, zabezpieczenia systemu operacyjnego AXIS OS oraz warstwy aplikacji i kontroli dostępu.



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

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.

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.

Domyślne zabezpieczenia

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.

Domyślnie wyłączone

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy

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

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

Lokalny zasób pamięci

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy

Od wersji AXIS OS 12.0, opcja montowania noexec została dodana jako opcja domyślna dla zamontowanych udziałów sieciowych. Powoduje to wyłączenie bezpośredniego wykonywania plików binarnych z zamontowanego udziału sieciowego. Na kartach SD ta opcja była już dostępna we wcześniejszych wersjach AXIS OS.

Dostęp uwierzytelniany

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.

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 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.

Domyślne zabezpieczenia

Protokół	Port	Transport	Uwagi
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 w systemie 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 w systemie 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 komunikacji edge-to-edge można znaleźć w dokumencie Technologia edge-to-edge.*

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

Gdy tylko jest to możliwe, zalecamy wyłączanie 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.

Interfejs UART/debugowania

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy

Wszystkie urządzenia Axis są wyposażone w tak zwany fizyczny interfejs UART (Universal Asynchronous Receiver Transmitter), zwany czasem „portem debugowania" lub „konsolą szeregową". Fizyczny dostęp do interfejsu wymaga całkowitego rozmontowania urządzenia Axis. Interfejs UART/debugowania jest wykorzystywany wyłącznie na etapie opracowywania produktu i debugowania podczas wewnętrznych projektów inżynieryjnych realizowanych przez dział badań i rozwoju firmy Axis.

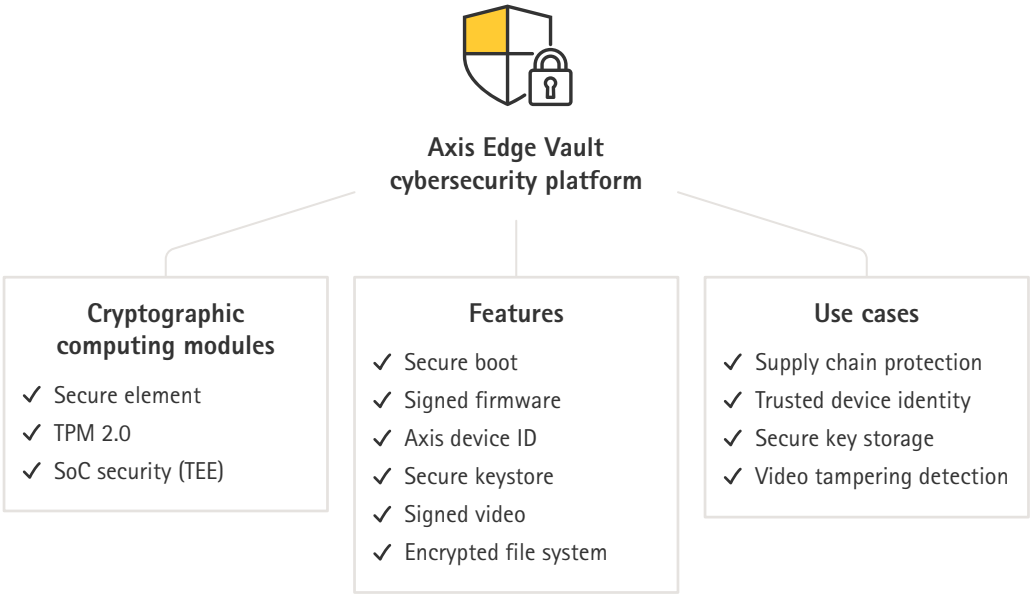
Interfejs UART/debugowania jest domyślnie włączony w urządzeniach Axis z systemem AXIS OS 10.10 lub starszym, ale wymaga uwierzytelnionego dostępu. Bez uwierzytelnienia żadne informacje poufne nie zostaną podane. W urządzeniach z systemem AXIS OS 10.11 lub nowszym interfejs UART/debugowania jest domyślnie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

Domyślne zabezpieczenia

Moduł Axis Edge

Axis Edge Vault zapewnia sprzętową platformę cyberbezpieczeństwa chroniącą urządzenia Axis. Jest ona oparta na silnej podstawie kryptograficznych modułów obliczeniowych (bezpiecznych elementów i modułów TPM) i zabezpieczeniu SoC (TEE i Secure Boot) w połączeniu z fachową wiedzą o bezpieczeństwie urządzeń brzegowych. Axis Edge Vault opiera się na wysokim poziomie zaufania zapewnianym przez bezpieczny rozruch i podpisane oprogramowanie układowe. Funkcje te tworzą nieprzerwany ciąg kryptograficznie zweryfikowanego oprogramowania w łańcuchu zaufania, na którym będą polegać wszystkie bezpieczne operacje.

Urządzenia Axis wyposażone w Axis Edge Vault minimalizują narażenie klienta na cyberzagrożenia, zapobiegając podsłuchiwaniu i złośliwemu wydobywaniu poufnych informacji. Axis Edge Vault zapewnia też, że urządzenie Axis jest w sieci klienta jednostką zaufaną i niezawodną.

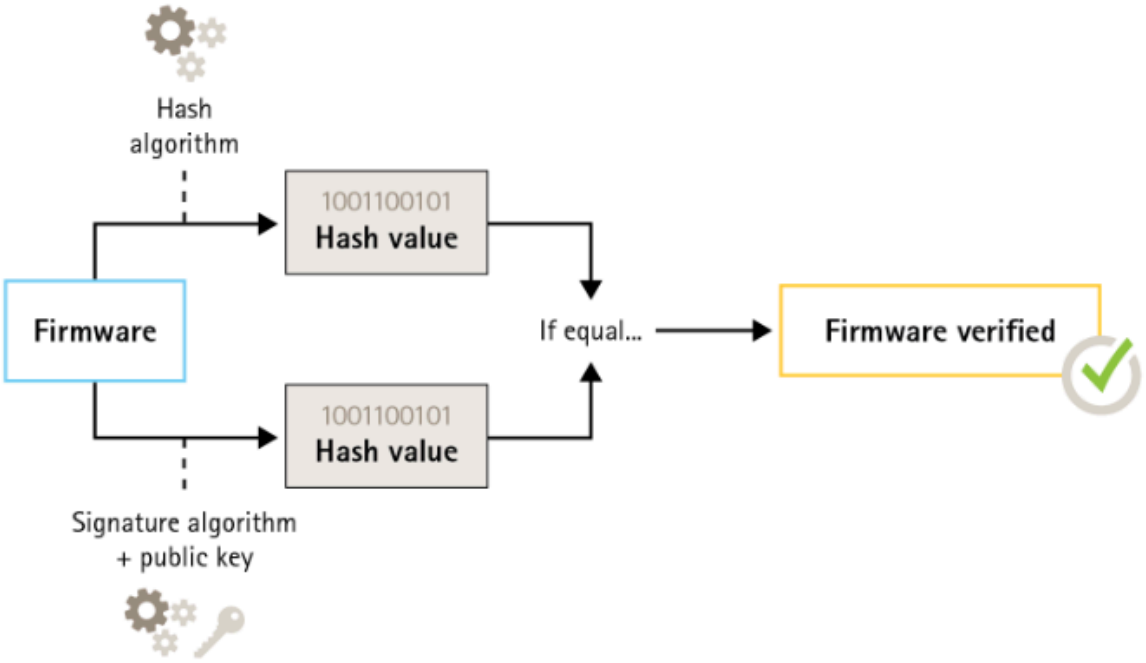


Podpisane oprogramowanie sprzętowe

CSC #2: Inwentaryzacja i kontrola zasobów oprogramowania

Od wersji 9.20.1 systemy AXIS OS są podpisane. Za każdym razem, gdy aktualizujesz wersję AXIS OS na urządzeniu, zostanie na nim sprawdzona integralność plików aktualizacji poprzez weryfikację podpisu kryptograficznego, a ewentualne sfałszowane pliki zostaną odrzucone. Dzięki temu hakerzy nie są w stanie nakłonić użytkownika do instalacji niebezpiecznych plików.

Domyślne zabezpieczenia

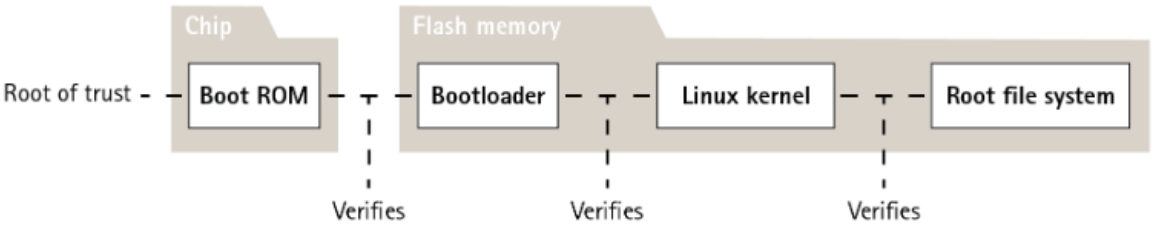


Więcej informacji znajduje się w oficjalnym dokumencie *Axis Edge Vault*.

Bezpieczne uruchamianie

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.



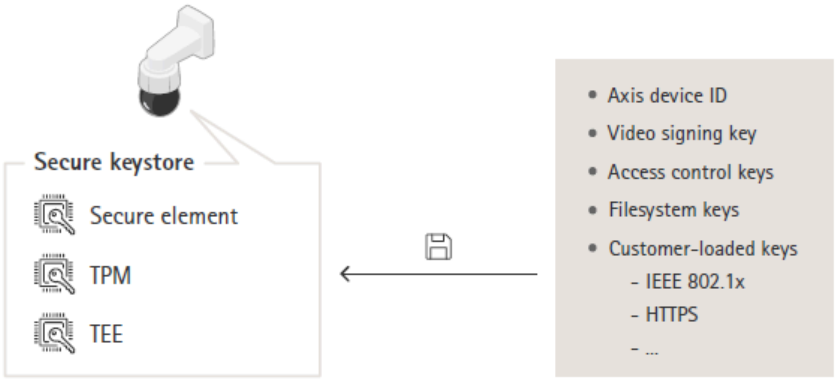
Więcej informacji znajduje się w oficjalnym dokumencie *Axis Edge Vault*.

Bezpieczny magazyn kluczy

CSC #6: Zarządzanie kontrolą dostępu

Bezpieczny magazyn kluczy zapewnia chronione przed manipulacją przechowywanie informacji kryptograficznych oparte na sprzęcie. 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).

Domyślne zabezpieczenia



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*.

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 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)

Domyślne nagłówki HTTP(S)

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 programowania aplikacji (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).

Domyślne zabezpieczenia

Uwierzytelnianie szyfrowane

CSC #3: Ochrona danych

Klienty 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)

Zapobiegnie atakom typu brute force

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy
CSC #13: Monitorowanie i ochrona sieci

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.

W systemie AXIS OS 11.5 i nowszych ochrona przed atakami brute-force jest domyślnie włączona. Szczegółowe przykłady konfiguracji i zalecenia można znaleźć w temacie *Brute force delay protection (Ochrona przed atakami brute force)* w AXIS OS Knowledge base (Bazie wiedzy o systemie AXIS OS).

Domyślne zabezpieczenia

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Nd.
≥ 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)

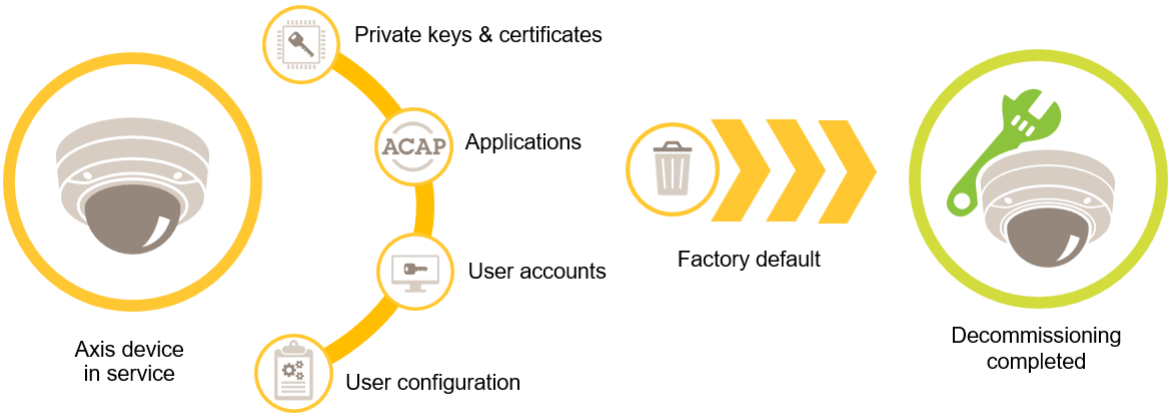
Wycofanie z użytku

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 powszechniej 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.

Należy pamiętać, że polecenie przywrócenia ustawień fabrycznych nie spowoduje natychmiastowego usunięcia danych. Urządzenie uruchomi się ponownie, a usunięcie danych nastąpi w trakcie uruchamiania systemu. Nie wystarczy zatem wydać polecenia przywrócenia ustawień fabrycznych. Urządzenie musi również mieć możliwość ponownego uruchomienia się i ukończenia tego procesu przed wyłączeniem zasilania, aby usuwanie danych zostało zakończone.



Domyślne zabezpieczenia

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 wykorzystuje niestandardowe certyfikaty, które umożliwiają użytkownikom przesyłanie (między innymi) systemu AXIS OS.*
*** Nagrania i obrazy przechowywane w zasobie lokalnym (karta SD, udział sieciowy) muszą zostać osobno usunięte przez użytkownika. Więcej informacji można znaleźć w temacie Formatting Axis SD cards (Formatowanie kart SD Axis)* w AXIS OS Knowledge base (Bazie wiedzy o systemie AXIS OS).*
**** Wszystkie konfiguracje wykonane przez użytkownika, od tworzenia kont po konfiguracje sieci, O3C, zdarzeń, obrazów, PTZ i systemu.*
***** Na urządzeniu zachowywane są wszelkie wstępnie zainstalowane aplikacje, ale wszystkie konfiguracje wprowadzone przez użytkownika są usuwane*
****** Dane produkcyjne (kalibracja, certyfikaty produkcyjne 802.1AR) i statystyki żywotności obejmują informacje niewrażliwe i niezwiązane z użytkownikiem.*

Podstawowe zabezpieczenia

Podstawowe zabezpieczenia to minimalny zalecany poziom ochrony urządzeń Axis. Podstawowe zabezpieczenia można ustawić na krawędzi systemu (tj. na urządzeniach końcowych). Można konfigurować je bezpośrednio w urządzeniu Axis niezależnie od zewnętrznej infrastruktury sieciowej, systemów zarządzania materiałem wizyjnym 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: .

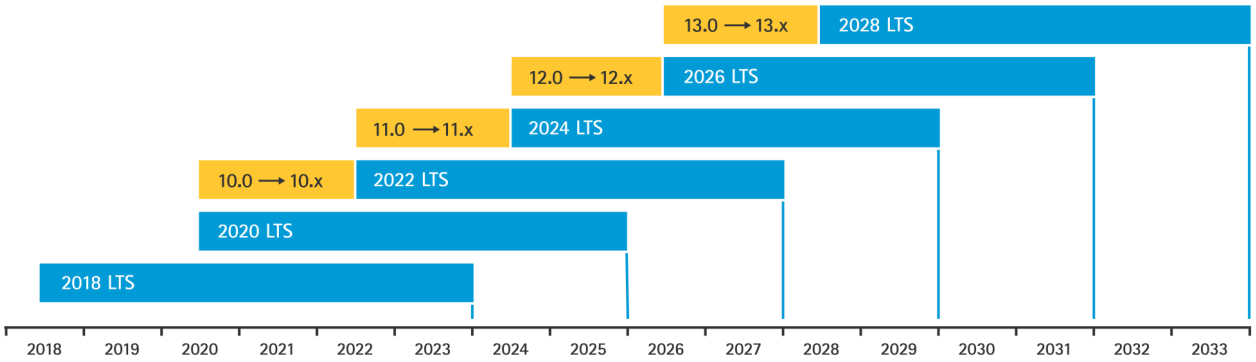
Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Maintenance > Default (Konfiguracja > Opcje systemowe > Konserwacja > Domyślne ustawienia)
≥ 7.10	Settings > System > Maintenance > Default (Ustawienia > System > Konserwacja > Domyślne ustawienia)
≥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

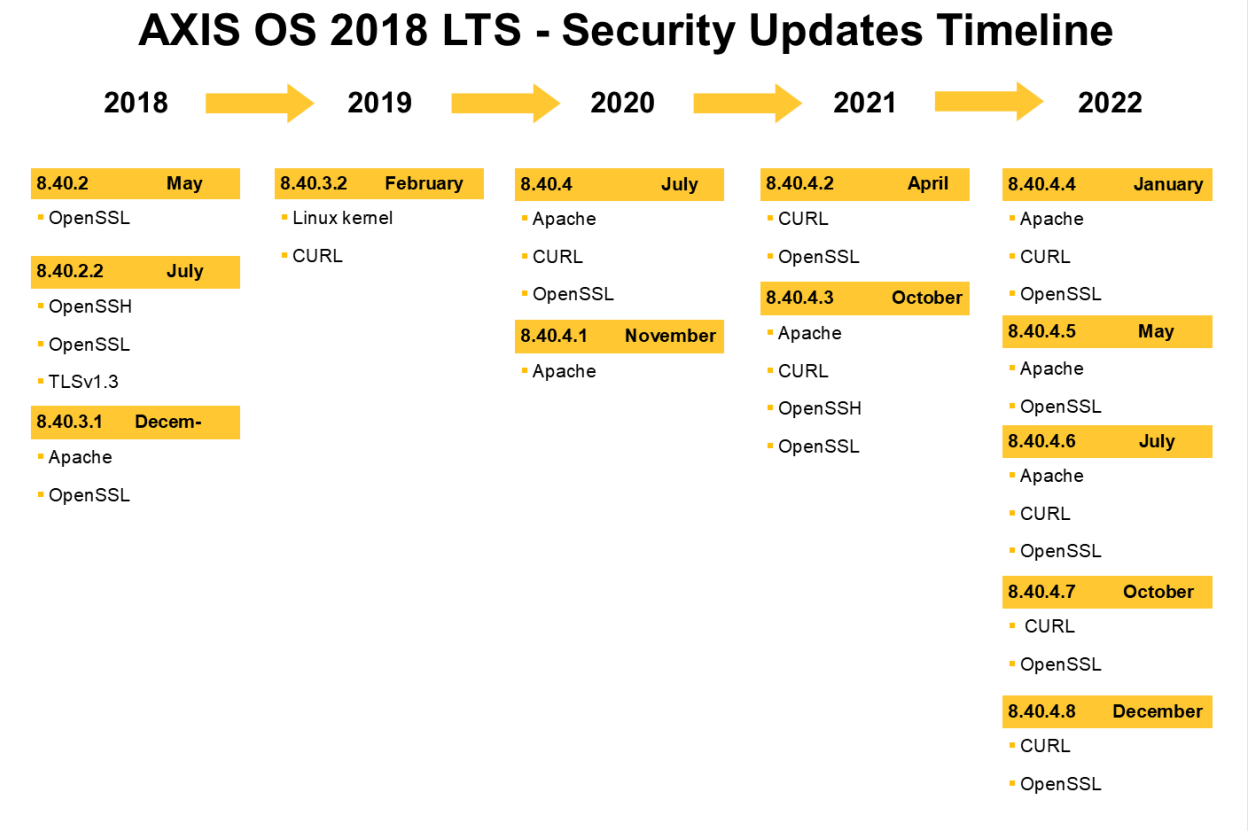
Axis zapewnia dwa tryby obsługi systemu AXIS OS: aktywny i długoterminowy (LTS). Oba te tryby uwzględniają najnowsze poprawki o znaczeniu krytycznym, lecz LTS nie zawiera nowych funkcji. Jest to podyktowane troską o maksymalne wyeliminowanie ryzyka niezgodności. Więcej informacji można znaleźć w temacie *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).

Konfiguracja hasła konta root urządzenia

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy
CSC #5: Zarządzanie kontami

Podstawowe zabezpieczenia

Konto root urządzenia jest jego głównym kontem administracyjnym. Aby używać konta root, trzeba skonfigurować hasło do urządzenia. Należy używać silnego hasła i korzystać z konta root tylko do zadań administracyjnych. Nie należy używać konta root do wykonywania codziennej pracy.

Używanie tego samego hasła do logowania się na różnych urządzeniach Axis ułatwia zarządzanie, ale jednocześnie zwiększa ryzyko włamań i wycieku danych. Używanie niepowtarzalnych haseł na każdym urządzeniu Axis zapewnia większy poziom bezpieczeństwa, lecz utrudnia zarządzanie urządzeniami. Zalecamy regularnie zmienianie haseł do urządzeń.

Zalecamy wdrażanie reguł wymagających tworzenie odpowiednio długich i skomplikowanych haseł. Warto korzystać ze wskazówek podanych w dokumencie *NIST password recommendations (Zalecenia NIST dotyczące haseł)*. W urządzeniach Axis można ustawiać hasła mające maks. 64 znaki. Hasła **krótsze niż 8 znaków** są uznawane za słabe.

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)

Tworzenie dedykowanych kont

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy
CSC #5: Zarządzanie kontami

Domyślne konto root posiada wszystkie uprawnienia i powinno być zarezerwowane dla zadań administracyjnych. Do codziennej pracy zalecamy utworzenie klienckiego konta użytkownika z ograniczonymi uprawnieniami. Zmniejsza to ryzyko naruszenia bezpieczeństwa hasła administratora urządzenia.

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)

Ograniczanie dostępu do interfejsu WWW

CSC #5: Zarządzanie kontami

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. Więcej informacji: .

Wyłączanie dostępu do interfejsu WWW

CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy

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	Nd.
≥ 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)

Konfiguracja ustawień sieciowych

CSC #12: Zarządzanie infrastrukturą sieciową

Konfiguracja IP urządzenia zależy od konfiguracji sieci, takiej jak IPv4/IPv6, statyczny lub dynamiczny (DHCP) adres sieciowy, maska podsieci i domyślny router. Przy dodawaniu nowych rodzajów komponentów warto zawsze przejrzeć topologię sieci.

Ponadto zalecamy korzystanie z konfiguracji statycznych adresów IP na urządzeniach Axis, aby zapewnić zasięg sieci i rozdzielić zależność od serwerów w sieci (takich jak serwery DHCP), które mogą być celem ataków.

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)

Konfigurowanie ustawień daty i godziny

CSC #8: Zarządzanie dziennikami audytów

Ze względów bezpieczeństwa ważne jest ustawienie prawidłowej daty i godziny. Pozwala to na przykład zapewnić prawidłowe oznaczenie dzienników systemowych sygnaturami czasowymi oraz weryfikację i stosowanie certyfikatów cyfrowych podczas uruchamiania. Usługi oparte na certyfikatach cyfrowych, takie jak HTTPS, IEEE i 802.1x, mogą nie działać prawidłowo bez odpowiedniej synchronizacji czasu.

Zalecamy zsynchronizowanie zegara urządzenia Axis z serwerami Network Time Protocol (NTP, niezaszyfrowane) lub najlepiej z serwerami Network Time Security (NTS, zaszyfrowane). W wersji 11.1 systemu AXIS OS została dodana obsługa szyfrowanego i bezpiecznego wariantu Network Time Protocol (NTP) — Network Time Security (NTS). Zalecamy skonfigurowanie kilku serwerów czasu, aby zwiększyć dokładność synchronizacji czasu i umożliwić obsługę scenariusza przełączania awaryjnego, w którym jeden ze skonfigurowanych serwerów czasu może być niedostępny.

Korzystanie z publicznych serwerów NTP lub NTS może być alternatywą dla osób prywatnych i małych organizacji, które nie mogą samodzielnie obsługiwać instancji lokalnych serwerów czasu. 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
Jeśli urządzenie Axis obsługuje i wykorzystuje karty SD do przechowywania nagrań wideo, zalecamy 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)
Jeśli używasz sieciowego zasobu dyskowego (NAS) jako urządzenia nagrywającego, zalecamy przechowywanie go w zamkniętym obszarze z ograniczonym dostępem 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)

Szyfrowanie eksportu nagrań

CSC #3: Ochrona danych

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	Nd.
≥ 7.10	Nd.
≥ 10.9	Nagrania

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	Nd.
≥ 7.10	Nd.
≥ 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*)
	Nd.
≥ 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)
≥ 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.

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	Nd.
≥ 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	Nd.
≥ 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)

Audio

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 wyłącznie 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	Nd.
≥ 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 jest niezabezpieczonym protokołem komunikacyjnym, który służy wyłącznie do debugowania i rozwiązywania problemów. Dostęp przez FTP został wycofany wraz z wersją AXIS OS 11.1 i w nowszych wersjach systemu nie jest już dostępny. 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 z systemem AXIS OS 5.50 i nowszymi. Zalecamy wyłączenie dostępu przez 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. Telnet jest obsługiwany w urządzeniach Axis z systemem w wersjach wcześniejszych niż AXIS OS 5.50. Zalecamy wyłączenie dostępu Telnet.

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 5.50	Szczegółowe instrukcje można znaleźć w temacie *Device access (Dostęp do urządzeń)* w AXIS OS Knowledge base (Bazie wiedzy o systemie AXIS OS).
< 7.10	Nd.
≥ 7.10	Nd.
≥ 10.9	Nd.

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	Nd.
≥ 10.9	Nd.

Filtr adresów IP

CSC #1: Inwentaryzacja i kontrolowanie zasobów firmy
CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy
CSC #13: Monitorowanie i ochrona sieci

Filtrowanie adresów IP zapobiega dostępowi nieautoryzowanych klientów do urządzenia Axis. Zalecamy skonfigurowanie w urządzeniu obsługi adresów IP autoryzowanych hostów sieciowych lub odrzucanie adresów IP nieautoryzowanych hostów sieciowych.

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

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

** W systemie AXIS OS 11.9 lub nowszym filtr adresu IP został zastąpiony nową hostowaną zaporą sieciową.*

Hostowana zapora sieciowa

CSC #1: Inwentaryzacja i kontrolowanie zasobów firmy
CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy
CSC #13: Monitorowanie i ochrona sieci

Użytkownicy mogą używać zapory do tworzenia reguł regulujących ruch przychodzący do urządzeń na podstawie adresów IP lub numerów portów TCP/UDP. Można w ten sposób zablokować nieautoryzowanym klientom dostęp do urządzenia Axis lub jego określonych 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 > Zapora sieciowa

HTTPS

CSC #3: Ochrona danych

W urządzeniach Axis z systemem AXIS OS 7.20 lub nowszym protokoły HTTP i HTTPS są domyślnie włączone. W przypadku protokołu HTTP dostęp jest nieszyfrowany i niezabezpieczony, natomiast protokół HTTPS szyfruje ruch między 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-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
```

Wersja systemu operacyjnego AXIS OS	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 kontrolowanie zasobów firmy
CSC #8: Zarządzanie dziennikami audytów

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 kontrolowanie 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 wyzwalać alarmy, co pozwala urządzeniom Axis wysyłać powiadomienia lub alarmy do wybranych klientów.

Więcej informacji o ofercie akcesoriów antsabotażowych można znaleźć w tematach:

- *AXIS TA8501 Physical Tampering Switch*

- *AXIS Dome Intrusion Switch C*
- *AXIS Door Switch 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.

Ograniczanie ekspozycji 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. Małym organizacjom i osobom prywatnym, które nie korzystają z VMS lub potrzebują zdalnego dostępu do materiałów wideo, zalecamy korzystanie z AXIS Companion.

System AXIS Companion używa oprogramowania klienckiego Windows/iOS/Android, jest bezpłatny i zapewnia łatwy dostęp do materiałów wideo bez narażania urządzenia Axis na zagrożenia obecne w Internecie. Więcej informacji o AXIS Companion można znaleźć na stronie *axis.com/companion*.

Uwaga

Klientów używających systemu VMS zachęcamy do skonsultowania się z jego dostawcą w celu uzyskania porad dotyczących najlepszych rozwiązań w zakresie zdalnego dostępu do materiałów wideo.

Ograniczenie ekspozycji w sieci

CSC #12: Zarządzanie infrastrukturą sieciową

Często stosowaną metodą ograniczania zagrożeń dla sieci jest fizyczna i wirtualna izolacja urządzeń sieciowych oraz powiązanych infrastruktury i aplikacji. Do przykładów takich aplikacji i infrastruktury należą oprogramowanie do zarządzania materiałem wizyjnym (VMS), sieciowe rejestratory wideo (NVR) oraz inne rodzaje sprzętu używane w systemach dozorowych.

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

Aby zapewnić podstawowy poziom zabezpieczeń, należy chronić sieć lokalną i jej infrastrukturę (router, przełączniki) przed nieautoryzowanym dostępem, dodając wielowarstwowe mechanizmy bezpieczeństwa sieci. Przykładami takich mechanizmów mogą być segmentacja VLAN, ograniczone możliwości routingu, wirtualna sieć prywatna (VPN) do obsługi połączeń między sieciami lub w systemie WAN, zapory sieciowe warstwy 2/3 i listy kontroli dostępu (ACL).

W celu wzmocnienia podstawowych zabezpieczeń zalecamy zastosowanie bardziej zaawansowanych technik kontroli sieci, takich jak głęboka inspekcja pakietów i detekcja włamań. Taka taktyka pozwoli zapewnić spójną i kompleksową ochronę przed zagrożeniami w sieci. Rozszerzone zabezpieczenie sieci wymaga dedykowanego oprogramowania i/lub urządzeń sprzętowych.

Skanowanie luk w zabezpieczeniach sieci

CSC #1: Inwentaryzacja i kontrolowanie 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 przejrzenie 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.

Rozszerzone zabezpieczenia

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 centrum certyfikacji ze zweryfikowanym łańcuchem zaufania pomaga usunąć z przeglądarki ostrzeżenia o certyfikacie podczas łączenia się za pomocą protokołu HTTPS. Certyfikat podpisany przez CA zapewnia również autentyczność urządzenia Axis podczas wdrażania rozwiązania kontroli dostępu do sieci (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.

Kontrola dostępu do sieci IEEE 802.1X

CSC #6: Zarządzanie kontrolą dostępu
CSC #13: Monitorowanie i ochrona sieci

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 kontrolowanie zasobów firmy
CSC #13: Monitorowanie i ochrona sieci

Urządzenia Axis z Axis Edge Vault obsługują standard sieciowy IEEE 802.1AR. Umożliwia to zautomatyzowane i bezpieczne wdrażanie urządzeń Axis w sieci za pomocą identyfikatora urządzenia Axis, unikalnego certyfikatu zainstalowanego w urządzeniu w fazie 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.

Monitorowanie SNMP

CSC #8: Zarządzanie dziennikami audytów

Urządzenia Axis obsługują następujące protokoły SNMP:

- **SNMP v1**: nie należy go używać; jest obsługiwany wyłącznie w celu zapewnienia zgodności wstecznej.
- **SNMP v2c**: nadaje się do użytku w zabezpieczonych segmentach sieci.
- **SNMP v3**: zalecany do monitorowania.

Urządzenia Axis obsługują również monitorowanie MIB-II i Axis Video MIB. Aby pobrać MIB Video MIB, zobacz *AXIS Video MIB* w AXIS OS Knowledge base (Bazie wiedzy o systemie AXIS OS).

Więcej informacji o konfigurowaniu SNMP w systemie AXIS OS można znaleźć w temacie *SNMP (Simple Network Management Protocol)* w AXIS OS Knowledge base (Bazie wiedzy o systemie AXIS OS).

Wersja systemu operacyjnego AXIS	Ścieżka konfiguracji interfejsu WWW
< 7.10	Setup > System Options > Network > SNMP (Konfiguracja > Opcje systemowe > Sieć > SNMP)
≥ 7.10	Settings > System > SNMP (Ustawienia > System > SNMP)
≥ 10.9	System > Network > SNMP (System > Sieć > SNMP)

Zdalny dziennik systemowy

CSC #8: Zarządzanie dziennikami audytów

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 *Syslog (Dziennik systemu)* 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

Urządzenia z systemem AXIS OS 7.40 lub nowszym obsługują bezpieczne strumieniowanie wideo za pomocą protokołu RTP, znanego też pod nazwą SRTP/RTSPS. SRTP/RTSPS wykorzystuje metodę bezpiecznego, kompleksowego szyfrowania, dzięki czemu strumień wideo z urządzenia Axis jest odbierany tylko przez autoryzowanych klientów. 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)

Podpisane wideo

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	Nd.
≥ 7.10	Nd.
≥ 10.9	System > Plain config > Image > SignedVideo (System > Zwykła konfiguracja > Obraz > Podpisane wideo)

Skrócony przewodnik

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

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: .

Używanie jednego hasła
CSC #4: Bezpieczna konfiguracja zasobów i oprogramowania firmy
CSC #5: Zarządzanie kontami

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 kontami.

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

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: . 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: .

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.

Skrócony przewodnik

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

Skrócony przewodnik

Przeznaczenie	Wywołanie interfejsu programowania aplikacji (API) VAPIX
Konfiguracja bezpiecznego szyfrowania TLS 1.2	`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`

*Włączanie zabezpieczenia przed atakami typu brute-force***	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.ActivatePasswordThrottling=on`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSBlockingPeriod=10`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageCount=20`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageInterval=1`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteCount=20`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteInterval=1`

Wyłączanie środowiska edytora skryptów	`https://ip-address/axis-cgi/param.cgi?action=update&System.EditCgi=no`
Włączanie udoskonalonego rejestrowania dostępu użytkowników	`https://ip-address/axis-cgi/param.cgi?action=update&System.AccessLog=On`
Włączanie zabezpieczenia przed atakami powtórzeniowymi na ONVIF	`https://ip-address/axis-cgi/param.cgi?action=update&WebService.UsernameToken.ReplayAttackProtection=yes`
Wyłączanie dostępu do interfejsu WWW urządzenia	`https://ip-address/axis-cgi/param.cgi?action=update&System.WebInterfaceDisabled=yes`
Wyłączanie nagłówka serwera HTTP/OpenSSL	`https://ip-address/axis-cgi/param.cgi?action=update&System.HTTPServerTokens=no`

Wyłączanie dostępu anonimowych użytkowników i PTZ	`https://ip-address/axis-cgi/param.cgi?action=update&root.Network.RTSP.ProtViewer=password`
	`https://ip-address/axis-cgi/param.cgi?action=update&root.System.BoaProtViewer=password`
	`https://ip-address/axis-cgi/param.cgi?action=update&root.PTZ.BoaProtPTZOperator=password`

Przeznaczenie	Wywołanie interfejsu programowania aplikacji (API) VAPIX
Zapobieganie instalacji uprawnień roota wymagających aplikacji ACAP	`http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowRoot&value=false`
Zapobieganie instalacji niepodpisanych aplikacji ACAP	`http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowUnsigned&value=false`

** W „port=X" zastąp wartość „X" rzeczywistym numerem portu. Przykłady: „port=1" wyłączy port 1, a „port=2" wyłączy port 2.*
*** W „eth1.1" zastąp „1" rzeczywistym numerem portu. Przykłady: „eth1.1" wyłączy port 1, a „eth1.2" wyłączy port 2.*
**** Po 20 nieudanych próbach logowania w ciągu jednej sekundy adres IP klienta jest blokowany na 10 sekund. 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.

AXIS OS Hardening Guide

Wer. M48.2
Data: Wrzesień 2024
Numer części