AXIS Device Manager

Podręcznik użytkownika

Wprowadzenie

Cyberbezpieczeństwo nabiera coraz większego znaczenia w obszarze zabezpieczeń. Skuteczne cyberbezpieczeństwo wymaga zapewnienia wystarczającej siły obrony, aby odpowiednio chronić sieć IP na każdym poziomie, począwszy od wybranych produktów i partnerów, na wymaganiach stawianych przez użytkowników kończąc.

Niniejszy dokument opisuje, jak wykorzystać aplikację AXIS Device Manager, aby podnieść bezpieczeństwo systemu. Położono w nim nacisk na kluczowe aspekty i przedstawiono zalecenia.

Zarządzanie cyklem istnienia urządzeń

W Axis wiemy, jak ważne są zasady bezpieczeństwa w cyklu eksploatacji urządzenia. Zaangażowanie w cyberbezpieczeństwo gwarantuje, że nasze produkty i rozwiązania zapewniają silną ochronę przed potencjalnymi zagrożeniami.

Implementacja

Axis oferuje urządzenia zgodne z zasadami bezpieczeństwa w fazie projektowania z wbudowanymi funkcjami bezpieczeństwa takimi jak mechanizmy bezpiecznego uruchomienia, podpisany system operacyjny i szyfrowana pamięć masowa. Aplikacja AXIS Device Manager wspiera ponadto instalatorów i administratorów systemów w bezpiecznym konfigurowaniu i wdrażaniu urządzeń, zapewniając bezpieczną instalację od samego początku.

Aktywna usługa

W fazie operacyjnej Axis zapewnia regularne aktualizacje oprogramowania urządzeń i poprawki bezpieczeństwa celem ochrony przed lukami w zabezpieczeniach. Aplikacja AXIS Device Manager umożliwia również zdalne monitorowanie i zarządzanie, zapewniając szybkie rozwiązywanie problemów i minimalizację czasu przestoju. Ponadto nasze Zalecenia dotyczące zwiększenia funkcjonalności i bezpieczeństwa sieciowego zawierają instrukcje dotyczące konfiguracji urządzeń w celu spełnienia określonych wymagań bezpieczeństwa.

Wycofanie z eksploatacji

Gdy nadchodzi czas złomowania lub wymiany urządzenia, aplikacja AXIS Device Manager ułatwia jego bezpieczne wycofanie z eksploatacji poprzez wymazanie poufnych danych i przywrócenie ustawień fabrycznych. Jest to gwarancją, że żadne poufne informacje nie pozostaną na urządzeniu, a dane użytkownika są chronione i niedostępne dla osób niepowołanych.

AXIS Device Manager

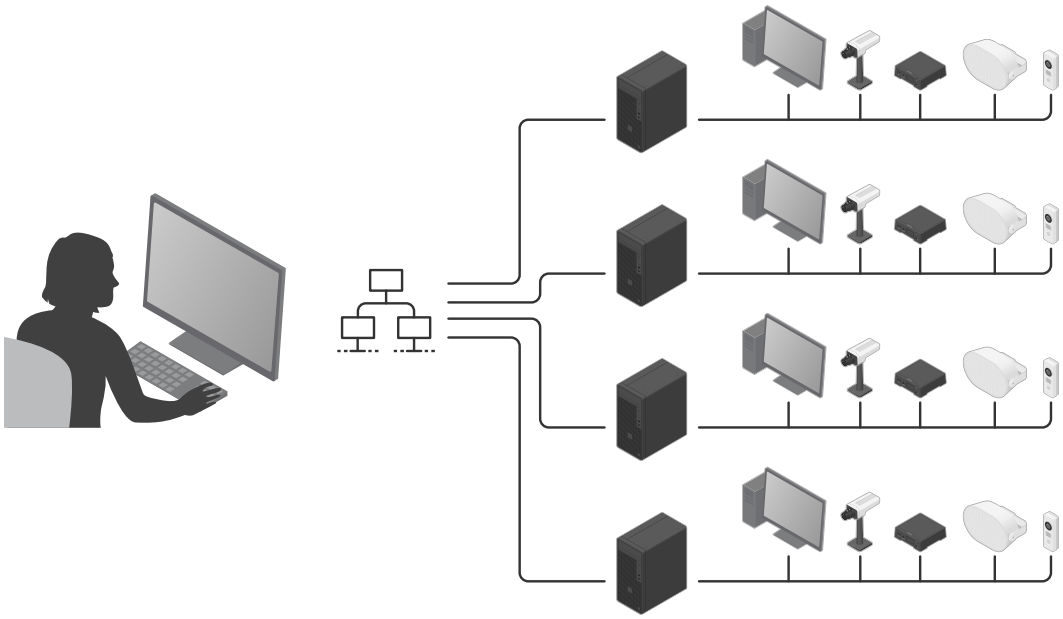
Aplikacja AXIS Device Manager to narzędzie lokalne zapewniające łatwy, przystępny cenowo i cyberbezpieczny sposób zarządzania wszystkimi głównymi zadaniami powiązanymi z instalacją, bezpieczeństwem i utrzymaniem (p. poniższa tabela). Narzędzie umożliwia zarządzanie kilkoma tysiącami urządzeń Axis w jednej lokalizacji lub kilkoma tysiącami urządzeń rozproszonych w wielu lokalizacjach. AXIS Device Manager zapewnia efektywne stosowanie środków cyberbezpieczeństwa na potrzeby ochrony urządzeń sieciowych i dostosowania ich do infrastruktury bezpieczeństwa.

Funkcje zarządzania urządzeniami, aplikacja AXIS Device Manager

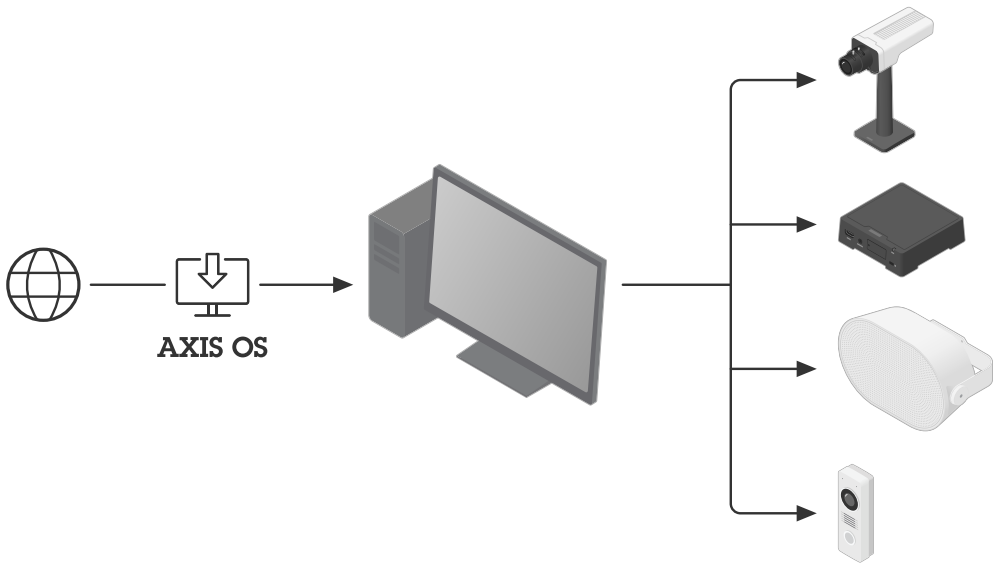
Instalacja	Konserwacja
Przypisywanie adresu IP	Status urządzeń
Eksportowanie listy urządzeń i śledzenie zasobów*	Zbieranie danych dotyczących urządzeń
Zarządzanie użytkownikami i hasłami*	Konfigurowanie urządzeń i kopiowanie konfiguracji do wielu urządzeń
Zarządzanie aplikacjami ACAP	Łączenie się z wieloma serwerami/systemami
Aktualizacja oprogramowania układowego AXIS OS w oparciu o ścieżki LTS lub aktywną*	Punkty przywracania

Zarządzanie certyfikatami HTTPS*	Przywracanie fabrycznych ustawień domyślnych
Zarządzanie certyfikatami IEEE 802.1*/**	Zastępowanie urządzeń
Tagowanie urządzeń	Odnawianie certyfikatów i zarządzanie nimi*
	Wzmacnianie zabezpieczeń przed cyberatakami*

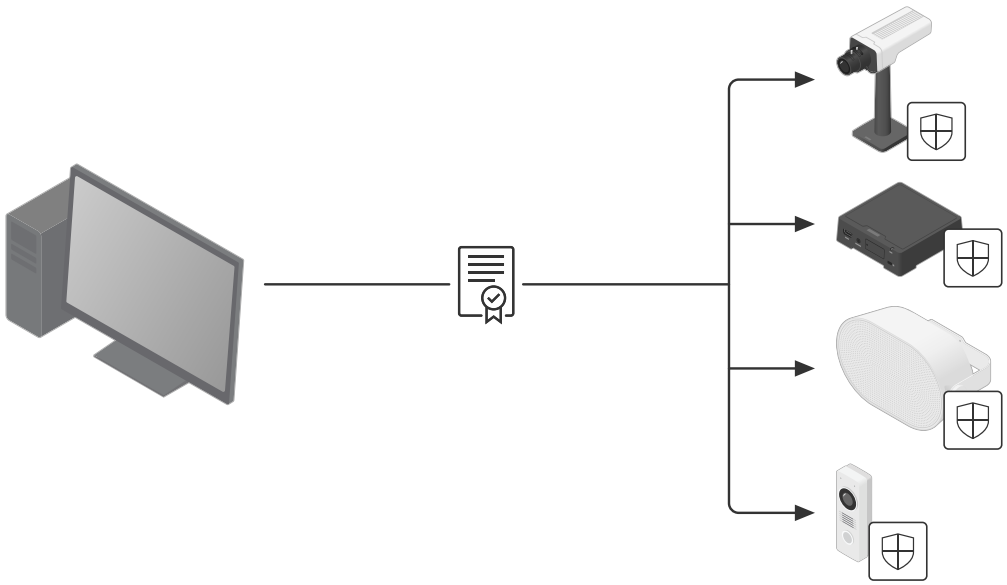
* Oznacza funkcję kontroli cyberbezpieczeństwa.
** Usługi certyfikatów Active Directory nie są obecnie obsługiwane. Zweryfikowano dla programu FreeRADIUS działającego w systemie Linux.



Zarządzanie wieloma lokalizacjami.



Uaktualnianie systemu AXIS OS.



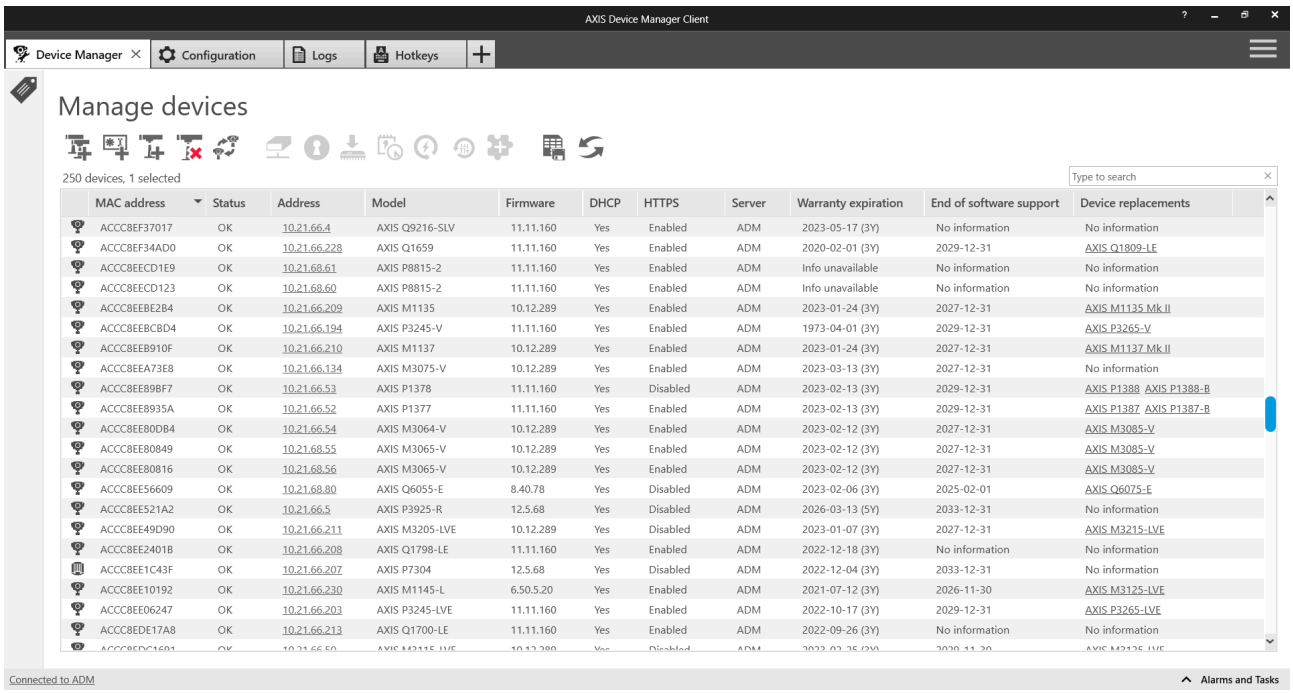
Zarządzanie certyfikatami.

Spis urządzeń

Podstawowym aspektem w zapewnieniu bezpieczeństwa sieci korporacyjnej jest utrzymywanie pełnego spisu urządzeń znajdujących się w sieci IP. Podczas tworzenia i przeglądu ogólnych zasad bezpieczeństwa ważna jest wiedza i przejrzysta dokumentacja dotycząca każdego urządzenia - nie tylko zasobów o znaczeniu krytycznym, ponieważ każde przeoczone urządzenie może stać się swoistą furtką dla atakujących. Nie da się chronić urządzeń, które zostały przeoczone lub co do których brakuje pełnej wiedzy.

Spis urządzeń jest istotny dla zabezpieczania sieci korporacyjnej. Aplikacja AXIS Device Manager jest w stanie wesprzeć zabezpieczenia poprzez:

- zapewnienie łatwego dostępu do aktualnego, pełnego spisu urządzeń sieciowych przy pracy z dziennikami i reakcją na incydenty,
- zapewnienie pełnej listy urządzeń, które można sortować według całkowitej liczby, rodzaju, oznaczeń modeli itp.,
- podawanie stanu każdego urządzenia w sieci IP,
- pomoc w planowaniu z wyprzedzeniem ze wskazaniem harmonogramu zakończenia wsparcia dla oprogramowania urządzenia, a także podanie listy nowszych produktów, które mogą być stosowane jako zamienniki.



MAC address	Status	Address	Model	Firmware	DHCP	HTTPS	Server	Warranty expiration	End of software support	Device replacements
ACCC8EF37017	OK	10.21.66.4	AXIS Q9216-SLV	11.11.160	Yes	Enabled	ADM	2023-05-17 (3Y)	No information	No information
ACCC8EF34AD0	OK	10.21.66.228	AXIS Q1659	11.11.160	Yes	Enabled	ADM	2020-02-01 (3Y)	2029-12-31	AXIS Q1809-LE
ACCC8EECD1E9	OK	10.21.68.61	AXIS P8815-2	11.11.160	Yes	Enabled	ADM	Info unavailable	No information	No information
ACCC8EECD123	OK	10.21.68.60	AXIS P8815-2	11.11.160	Yes	Enabled	ADM	Info unavailable	No information	No information
ACCC8EEBE2B4	OK	10.21.66.209	AXIS M1135	10.12.289	Yes	Enabled	ADM	2023-01-24 (3Y)	2027-12-31	AXIS M1135 Mk II
ACCC8EEBCBD4	OK	10.21.66.194	AXIS P3245-V	11.11.160	Yes	Enabled	ADM	1973-04-01 (3Y)	2029-12-31	AXIS P3265-V
ACCC8EEB910F	OK	10.21.66.210	AXIS M1137	10.12.289	Yes	Enabled	ADM	2023-01-24 (3Y)	2027-12-31	AXIS M1137 Mk II
ACCC8EEA73E8	OK	10.21.66.134	AXIS M3075-V	10.12.289	Yes	Enabled	ADM	2023-03-13 (3Y)	2027-12-31	No information
ACCC8EE89BF7	OK	10.21.66.53	AXIS P1378	11.11.160	Yes	Disabled	ADM	2023-02-13 (3Y)	2029-12-31	AXIS P1388 AXIS P1388-B
ACCC8EE8935A	OK	10.21.66.52	AXIS P1377	11.11.160	Yes	Enabled	ADM	2023-02-13 (3Y)	2029-12-31	AXIS P1387 AXIS P1387-B
ACCC8EE80DB4	OK	10.21.66.54	AXIS M3064-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
ACCC8EE80849	OK	10.21.68.55	AXIS M3065-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
ACCC8EE80816	OK	10.21.68.56	AXIS M3065-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
ACCC8EE56609	OK	10.21.68.80	AXIS Q6055-E	8.40.78	Yes	Disabled	ADM	2023-02-06 (3Y)	2025-02-01	AXIS Q6075-E
ACCC8EE521A2	OK	10.21.66.5	AXIS P3925-R	12.5.68	Yes	Disabled	ADM	2026-03-13 (5Y)	2033-12-31	No information
ACCC8EE49D90	OK	10.21.66.211	AXIS M3205-LVE	10.12.289	Yes	Disabled	ADM	2023-01-07 (3Y)	2027-12-31	AXIS M3215-LVE
ACCC8EE2401B	OK	10.21.66.208	AXIS Q1798-LE	11.11.160	Yes	Enabled	ADM	2022-12-18 (3Y)	No information	No information
ACCC8EE1C43F	OK	10.21.66.207	AXIS P7304	12.5.68	Yes	Disabled	ADM	2022-12-04 (3Y)	2033-12-31	No information
ACCC8EE10192	OK	10.21.66.230	AXIS M1145-L	6.50.5.20	Yes	Enabled	ADM	2021-07-12 (3Y)	2026-11-30	AXIS M3125-LVE
ACCC8EE06247	OK	10.21.66.203	AXIS P3245-LVE	11.11.160	Yes	Enabled	ADM	2022-10-17 (3Y)	2029-12-31	AXIS P3265-LVE
ACCC8EDE17A8	OK	10.21.66.213	AXIS Q1700-LE	11.11.160	Yes	Enabled	ADM	2022-09-26 (3Y)	No information	No information

Aplikacja AXIS Device Manager zapewnia czytelny widok spisu urządzeń.

Aplikacja AXIS Device Manager zapewnia zautomatyzowane środki dostępu do spisu urządzeń sieciowych Axis w czasie rzeczywistym. Umożliwia automatyczną identyfikację, wyświetlanie list i sortowanie urządzeń. Pozwala także na użycie znaczników do grupowania i sortowania urządzeń na podstawie własnych kryteriów, co ułatwia przegląd i dokumentowanie wszystkich urządzeń Axis w sieci IP.

Zasady dotyczące kont i haseł

Uwierzytelnianie i kontrola uprawnień jest szczególnie istotnym elementem ochrony zasobów sieciowych. Zastosowanie zasad pomaga zmniejszyć ryzyko przypadkowego lub celowego nadużycia. Kluczowe jest egzekwowanie stosowania silnych haseł, choć zmniejszenie ryzyka złamania haseł jest równie ważne. Hasła do urządzeń często rozchodzą się w organizacji, a użytkownik traci kontrolę nad tym, kto ma do nich dostęp. Aplikacja AXIS Device Manager wspomaga łatwe zarządzanie wieloma kontami i hasłami do urządzeń Axis.

Dlaczego warto mieć więcej niż jedno konto użytkownika w urządzeniach:

- Kontrola poziomów uprawnień dla różnych rodzajów użytkowników (maszyn i ludzi).
- Zmniejszenie ryzyka złamania hasła głównego.
- Możliwość zresetowania poświadczenia dla jednego rodzaju użytkownika bez wpływu na innych.

Uprawnienia w aplikacji AXIS Device Manager

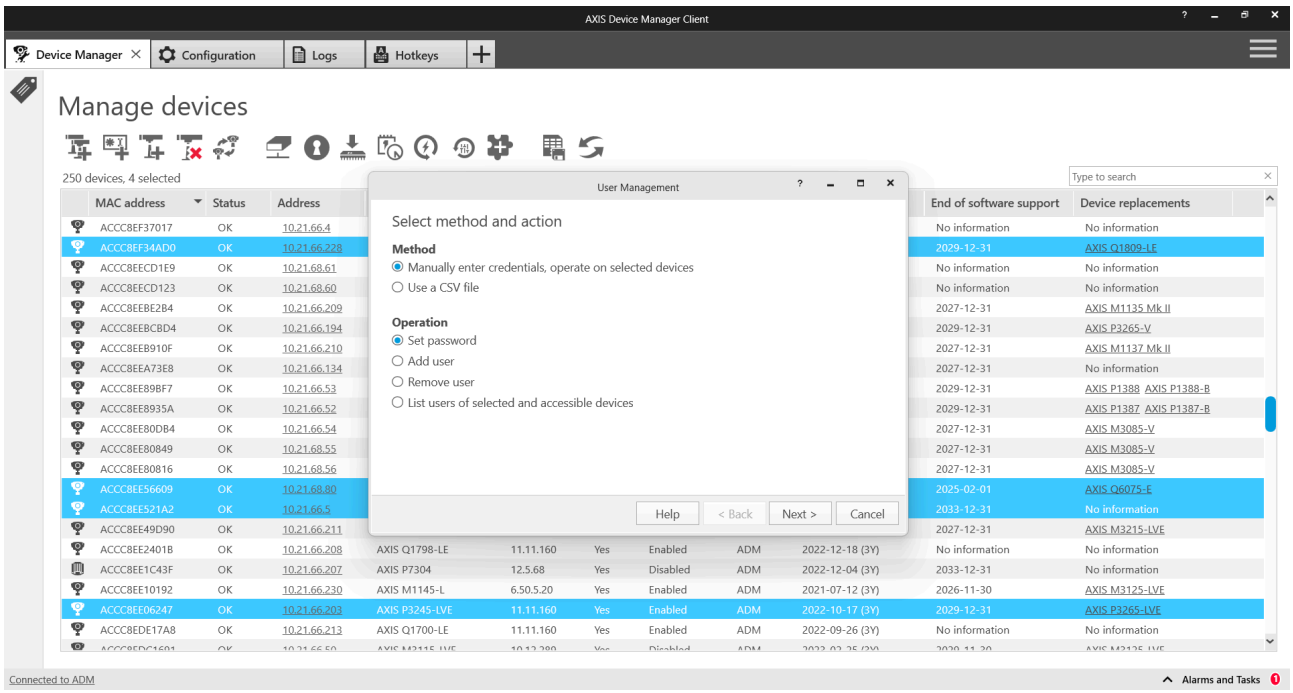
Urządzenia Axis obsługują kilka kont, z których każde ma jeden z trzech poziomów uprawnień:

- **Dozorcy**: Użytkownicy ci mają dostęp do obrazu i sterowania PTZ.
- **Operatorzy**: Użytkownicy z uprawnieniami operatora mogą optymalizować ustawienia kamer i profile strumieni wizyjnych.
- **Administratorzy**: Administratorzy mają możliwość zarządzania kontami, zmiany ustawień sieciowych i sterowania szeregiem usług w urządzeniu.

Każda rola mająca dostęp do kamery powinna obejmować własne konto. Przykładowo można skonfigurować rolę „Personel pomieszczenia nadzoru" z poziomem uprawnień „operator", podczas gdy rola „Patrol interwencyjny" może wymagać tylko poziomu uprawnień „dozorca".

Zalecane czynności

- Przed dodaniem kamer do systemu VMS dodaj kamery do aplikacji AXIS Device Manager.
- W aplikacji AXIS Device Manager wybierz wszystkie kamery i utwórz nowe konto użytkownika o nazwie „vms" lub podobnej, a następnie ustaw silne hasło. Uprawnienia muszą być zgodne z wymaganiami w systemie VMS – może to być operator lub administrator (należy sprawdzić u producenta).
- Dodaj urządzenia do systemu VMS z wykorzystaniem utworzonego konta i hasła.
- Wracając do aplikacji AXIS Device Manager – wybierz ponownie wszystkie urządzenia i zresetuj (zmień) hasło konta „root" na nowe, silne hasło. Hasło do konta „root" powinno być znane tylko ograniczonej liczbie osób (korzystającej z aplikacji AXIS Device Manager).
- Jeżeli ktoś musi użyć przeglądarki sieciowej na potrzeby uzyskania dostępu do urządzenia w celach utrzymania lub rozwiązywania problemów, **nie** wolno podawać mu hasła root. Zamiennie użyj aplikacji AXIS Device Manager, aby utworzyć nowe (tymczasowe) konto dla wybranych urządzeń z uprawnieniami administratora lub operatora. Po zakończeniu pracy za pomocą aplikacji AXIS Device Manager usuń konto tymczasowe.
- Aplikacja AXIS Device Manager obsługuje lokalnych administratorów oraz użytkowników i grupy domenowe. Można wykorzystać lokalnego administratora, o ile dostęp do klienta AXIS Device Manager będzie możliwy tylko z tego samego urządzenia, na którym znajduje się serwer AXIS Device Manager. Zaleca się korzystanie z użytkowników domenowych, jeżeli osoba utrzymująca system będzie korzystać ze zdalnych klientów.



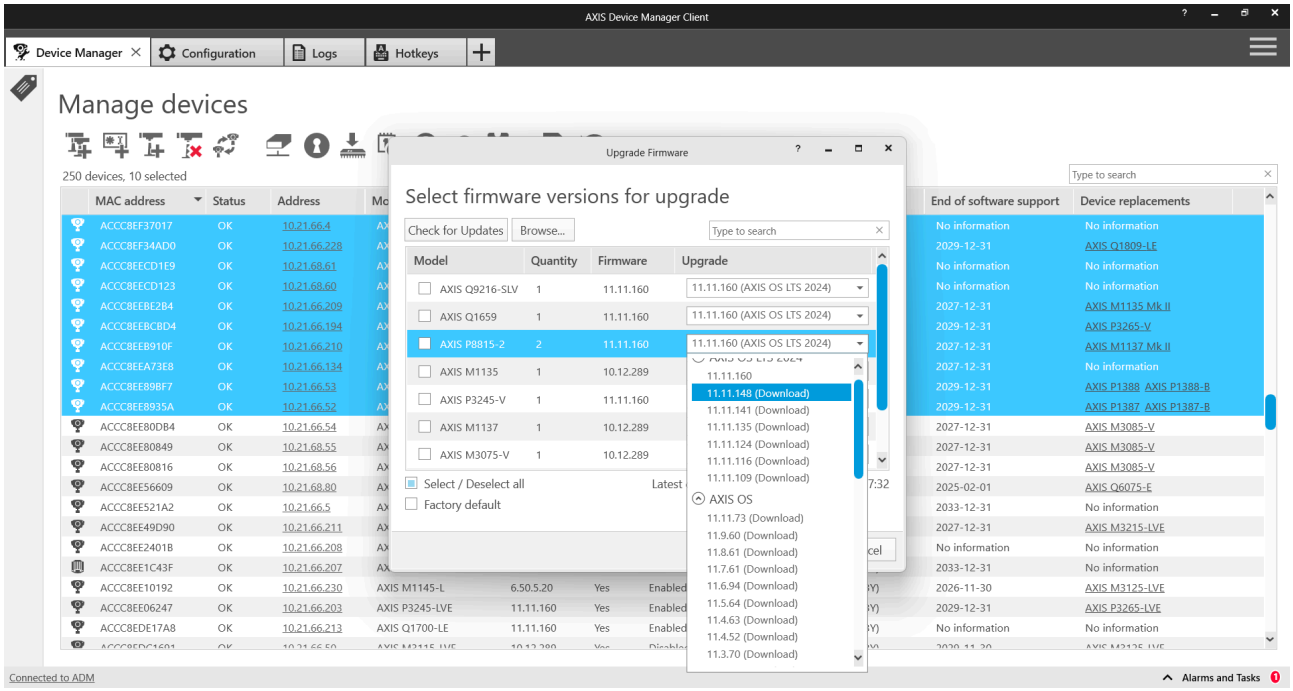
Zmiana ról i haseł użytkowników w aplikacji AXIS Device Manager.

Aktualizacje oprogramowania AXIS OS

Zaktualizowane wersje oprogramowania układowego AXIS OS zawierają poprawki znanych luk bezpieczeństwa. Ważne, aby zawsze korzystać z najnowszego oprogramowania, ponieważ atakujący mogą próbować wykorzystać znane luki bezpieczeństwa. Co równie ważne, szybkie wdrożenie nowej wersji oprogramowania układowego AXIS OS zwiększa możliwości operacyjne i eliminuje wąskie gardła związane z ręcznym wydawaniem aktualizacji nowych wersji. Aplikacja AXIS Device Manager łączy się ze stroną www.axis.com i pobiera najnowsze obowiązujące wersje oprogramowania AXIS OS lub usług. Jeżeli użytkownik nie chce pobrać aktualizacji bezpośrednio do własnej sieci z internetu, może zapisać aktualizacje w pamięci USB, a następnie przesłać je do klienta AXIS Device Manager. Narzędzie informuje również, czy dostępne są nowe wersje oprogramowania AXIS OS i umożliwia szybkie ich wczytanie do urządzeń Axis.

Dlaczego zawsze należy stosować najnowsze wersje oprogramowania AXIS OS:

- Sieć IP i urządzenia są chronione poprzez najnowsze poprawki znanych luk, zwłaszcza krytycznych.
- Urządzenia są aktualizowane pod kątem najnowszych ulepszeń parametrów działania, a także poprawek błędów i usterek.
- Otrzymują natychmiastowy dostęp do najnowszych funkcji i ulepszeń funkcjonalności.



Aktualizacja oprogramowania AXIS OS za pomocą aplikacji AXIS Device Manager została uproszczona poprzez powiadomienia na ekranie i intuicyjne okna dialogowe.

Dodatkowe zabezpieczenia

Stosowanie dobrych praktyk dotyczących użytkowników i haseł, a także korzystanie z aktualnych wersji oprogramowania układowego AXIS OS ogranicza typowe zagrożenia dotyczące urządzeń. Przewodnik *Zalecenia dotyczące zwiększenia funkcjonalności i bezpieczeństwa systemu AXIS* opisuje dodatkowe środki mające na celu zmniejszenie ryzyka stosowane w organizacjach dużych i o krytycznym znaczeniu. Obejmuje to wyłączenie usług, które mogą nie być używane i włączenie usług, które mogą pomóc w wykrywaniu i monitorowaniu wskazania ataku lub naruszenia. Aplikacja AXIS Device Manager upraszcza proces wdrażania niektórych z tych zasad. Axis udostępnia szablon konfiguracji na potrzeby podstawowych zalecanych ustawień.

Jak zabezpieczać urządzenia zgodnie z Zaleceniami dotyczącymi zwiększenia funkcjonalności i bezpieczeństwa Axis:

- Zapoznaj się z przewodnikiem *Zalecenia dotyczące zwiększenia funkcjonalności i bezpieczeństwa systemu AXIS* i pobierz plik szablonu znajdujący się na końcu dokumentu.
- Edytuj plik konfiguracyjny, aby wybrać odpowiednie elementy.
- Wybierz urządzenia w spisie AXIS Device Manager.
- Kliknij prawym przyciskiem myszy i wybierz kolejno opcje „Configure Devices > Configure...” (Konfiguruj urządzenia > Konfiguruj).
- Kliknij „Configuration File” (Plik konfiguracyjny) i wybierz pobrany plik.
- W razie potrzeby zmień ustawienia.

Usługa Urzędu Certyfikacji

Urząd Certyfikacji (UC) to usługa wydająca certyfikaty cyfrowe serwerom, klientom lub użytkownikom. Może on być publiczny lub prywatny. Publiczne Urzędy Certyfikacji takie jak Comodo i Symantec (wcześniej Verisign) są zwykle stosowane w usługach publicznych, takich jak publiczne strony internetowe i poczta e-mail.

Prywatny UC (zazwyczaj Active Directory / usługa certyfikacji) wydaje certyfikaty dla wewnętrznych / prywatnych usług sieciowych. W sieciowym systemie zarządzania obrazem certyfikaty służą głównie do szyfrowania w sieci HTTPS i kontroli dostępu sieciowego IEEE 802.1x. Aplikacja AXIS Device Manager zawiera usługę UC dla urządzeń Axis i działa jako prywatny główny UC lub jako prywatny pośredni UC, jako część infrastruktury klucza publicznego (PKI) klasy enterprise.

Certyfikaty z podpisem UC są stosowane zarówno dla certyfikatów IEEE 802.1x (klient), jak i HTTPS (serwer).

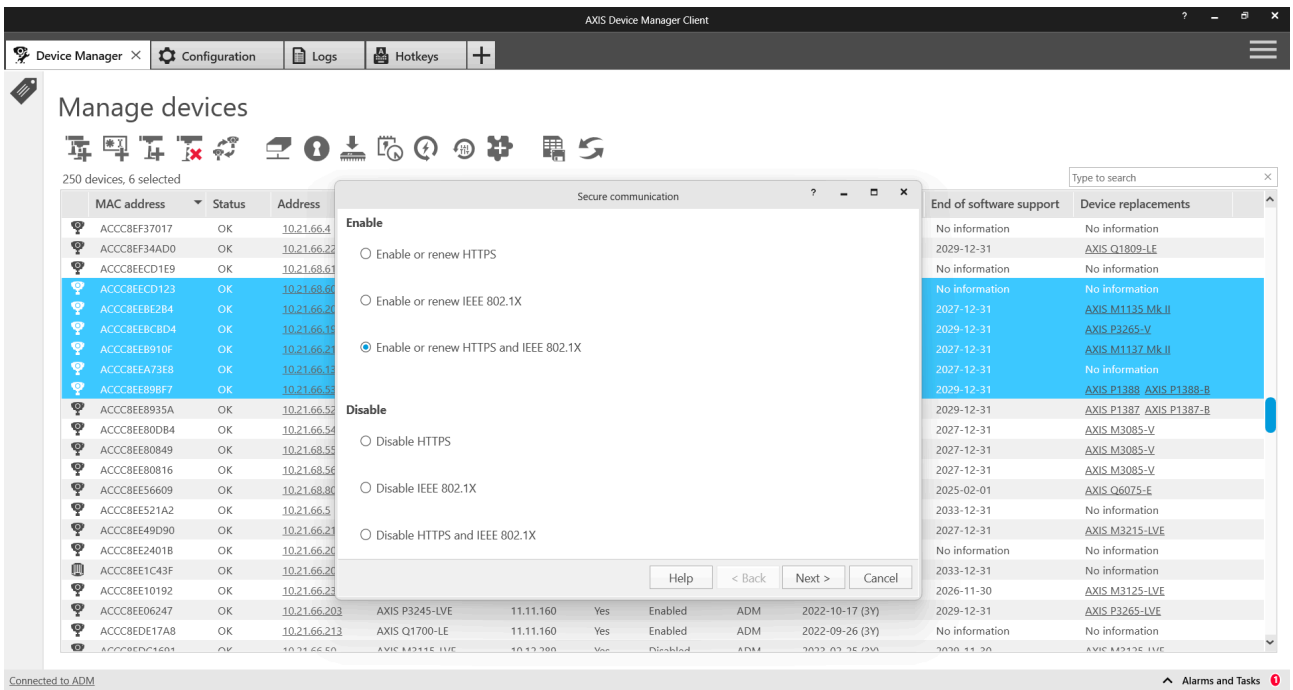
HTTPS

HTTPS to bezpieczna wersja protokołu HTTP, w której komunikacja między klientem a serwerem jest szyfrowana. Certyfikaty samopodpisane są wystarczające do uzyskania szyfrowanego połączenia. Pod względem poziomu szyfrowania między certyfikatami samopodpisanymi a certyfikatami z podpisem UC nie ma różnicy. Jedyna różnica polega na tym, że samopodpisane certyfikaty nie chronią przed spoofingiem sieciowym, w którym atakujący komputer próbuje podszyć się pod legalny serwer. Certyfikaty z podpisem UC dodają czynnik zaufania dla klientów celem uwierzytelnienia, że mają dostęp do zaufanego urządzenia. Należy przy tym pamiętać, że klient wizyjny (VMS) musi obsługiwać żądanie obrazu przez HTTPS (RTP przez RTSP przez HTTPS) w celu szyfrowania obrazu.

IEEE 802.1X

Standard określany często jako 802.1X uniemożliwia nieautoryzowanym urządzeniom sieciowym dostęp do sieci lokalnej. Urządzenie musi się uwierzytelnić, aby uzyskać dostęp do sieci IP (i jej zasobów). Możliwe jest stosowanie różnych metod uwierzytelniania: adres MAC (filtrowanie MAC), nazwa użytkownika / hasło lub certyfikat klienta. Wyboru dokonuje właściciel systemu, oceniwszy zagrożenia, ryzyka i koszty.

Posługiwanie się infrastrukturą 802.1X jest inwestycją. Wymaga zarządzalnych przełączników sieciowych i dodatkowych serwerów, zazwyczaj RADIUS (Remote Authentication Dial-In User Service). Korzystanie z certyfikatów klienta wymaga UC (prywatnego lub publicznego), który wydaje certyfikaty klienta. Infrastruktura najczęściej wymaga personelu na potrzeby utrzymania i nadzoru.



Konfiguracja certyfikatu w aplikacji AXIS Device Manager.

Zarządzanie cyklem życia certyfikatu

Zarządzanie cyklem życia certyfikatu to sposób na relatywnie niedrogą obsługę wszystkich procesów i zadań związanych z wydawaniem, instalacją, inspekcją, rozwiązywaniem problemów i odnawianiem certyfikatów. Aplikacja AXIS Device Manager zapewnia efektywne zarządzanie certyfikatami, umożliwiając administratorom:

- wydawanie certyfikatów podpisanych przez Urząd Certyfikacji (UC), gdy żaden inny urząd certyfikacji nie jest dostępny,
- łatwe zarządzanie certyfikatami IEEE 802.1X,
- łatwe zarządzanie certyfikatami HTTPS,
- monitorowanie dat wygaśnięcia certyfikatów,
- łatwe odnawianie certyfikatów przed ich wygaśnięciem.

Zalecenia dotyczące prywatnych głównych i prywatnych pośrednich urzędów certyfikacji (UC)

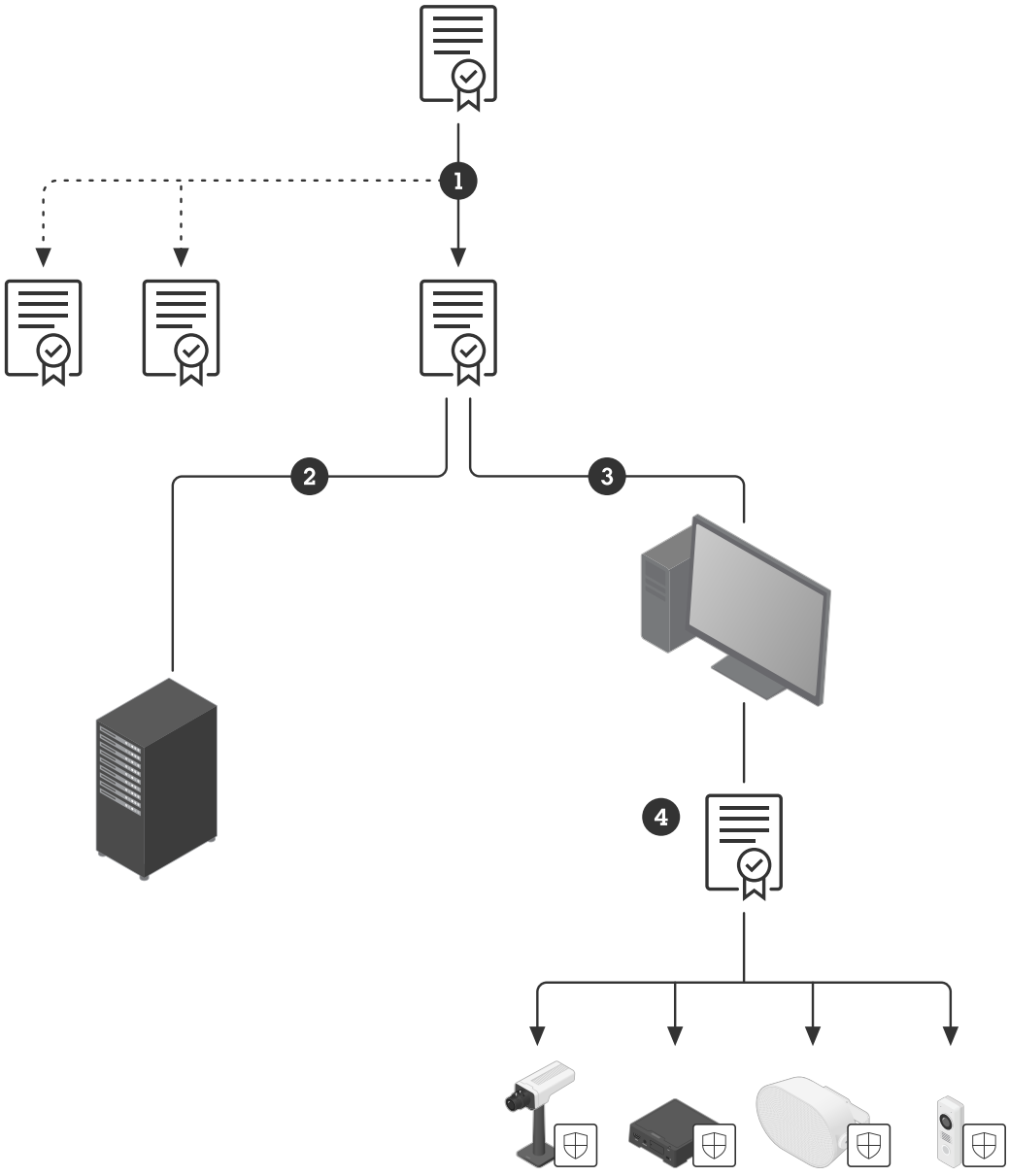
Nie zaleca się wystawiania urządzeń Axis jako publicznych, ogólnodostępnych serwerów, w związku z czym korzystanie z publicznego UC na potrzeby prywatnych zasobów jest nieopłacalne.

W przypadku protokołu HTTPS serwer VMS jest jedynym klientem, który musi potwierdzić, że ma dostęp do zaufanej kamery. Klienty-operatorzy nie będą mieć bezpośredniego dostępu do kamer, ponieważ obraz na żywo i nagrania dostarczane są przez serwer VMS. W tej sytuacji włączenie certyfikatów serwera kamer do istniejącej infrastruktury klucza publicznego klasy enterprise ma ograniczoną wartość.

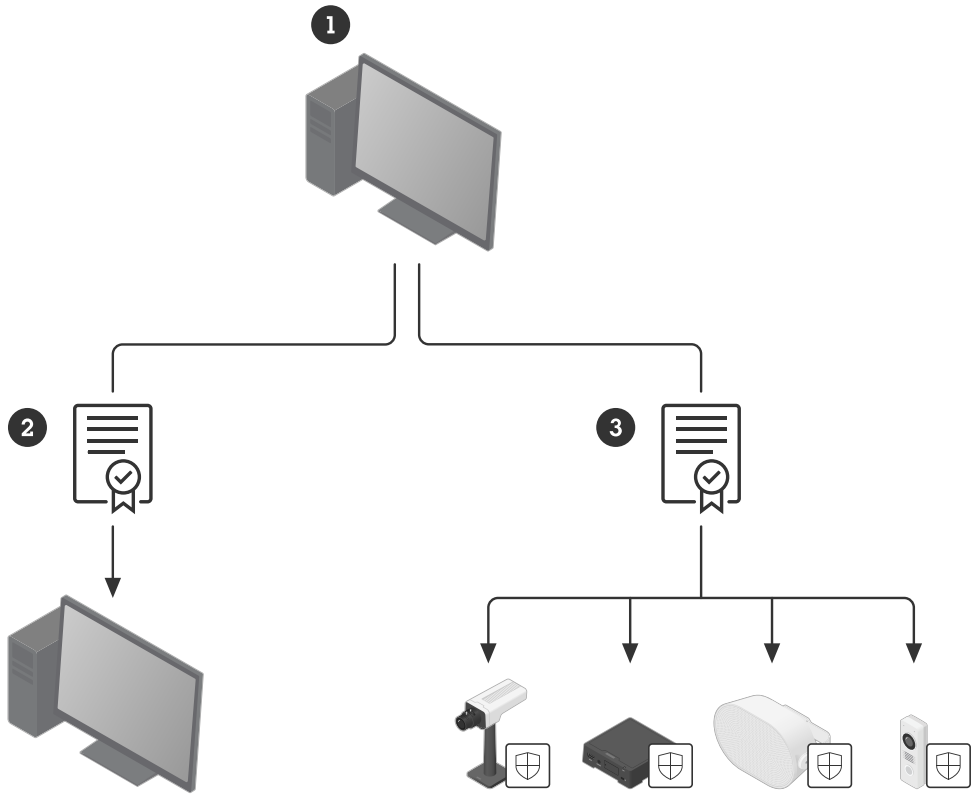
Wykorzystanie aplikacji AXIS Device Manager jako prywatnego UC jest najbardziej opłacalnym rozwiązaniem. Po wygenerowaniu certyfikatu głównego UC należy zainstalować certyfikat AXIS Device Manager w magazynie certyfikatów serwera VMS. Jeżeli inne klienty mają bezpośredni dostęp do kamer (na potrzeby utrzymania lub rozwiązywania problemów), należy zainstalować certyfikat główny UC AXIS Device Manager również na tych klientach.

W przypadku certyfikatu 802.1X kamera wymaga certyfikatu klienta celem uwierzytelnienia na serwerze RADIUS. Zaleca się, aby administrator infrastruktury klucza publicznego klasy enterprise / UC wygenerował certyfikat pośredni UC i wyeksportował go jako certyfikat PKCS#12 (P12), który można zainstalować w aplikacji AXIS Device Manager.

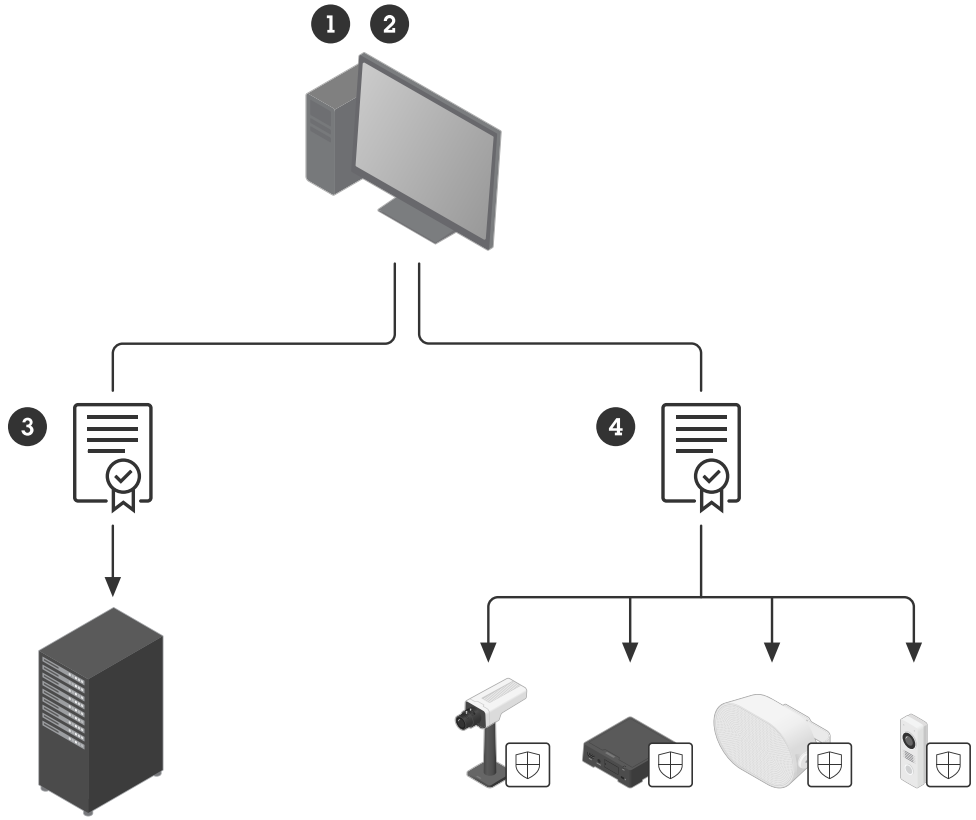
Aby uzyskać pomoc w ustawieniu serwera FreeRADIUS, przejdź do sekcji *Technical papers (Dokumentacja techniczna)* dla aplikacji AXIS Device Manager.



Zarządzanie certyfikatami HTTPS obejmuje: 1) wygenerowanie pośredniego lub głównego certyfikatu UC w aplikacji AXIS Device Manager; 2) wyeksportowanie certyfikatu UC do VMS; 3) przesłanie certyfikatów serwera do urządzeń.



Korzystanie z prywatnego UC. Zarządzanie certyfikatami IEEE 802.1X obejmuje: 1) wygenerowanie pośredniego UC i certyfikatu klienta; 2) instalację certyfikatu UC na serwerze Radius; 3) importowanie certyfikatu UC w aplikacji AXIS Device Manager; 4) przesłanie certyfikatów UC oraz klienta do urządzeń.



Korzystanie z aplikacji AXIS Device Manager jako UC. Aby zarządzać certyfikatami IEEE 802.1X, należy: 1) wygenerować certyfikat główny UC w aplikacji AXIS Device Manager; 2) zaimportować certyfikat UC uwierzytelniania do aplikacji AXIS Device Manager; 3) zainstalować certyfikat UC na serwerze Radius; 4) przesłać certyfikaty UC uwierzytelniania i klienta do urządzeń.

Podsumowanie

Zarządzanie bezpieczeństwem i kontrola bezpieczeństwa to istotne składowe właściwego podejścia do cyberbezpieczeństwa. Każde jest ciągłym procesem wymagającym utrzymania czytelnego stanu i wykonania odpowiednich działań w celu minimalizacji skutków potencjalnych zagrożeń mogących wpłynąć na działanie sieci IP. Aplikacja AXIS Device Manager zapewnia narzędzia zarówno do zarządzania urządzeniami, jak i do zwiększenia bezpieczeństwa sieci IP. Aby uzyskać więcej informacji lub pomoc techniczną, należy kontaktować się z lokalnym przedstawicielem Axis lub odwiedzić stronę *www.axis.com*.

T10231485_pl

2025-09 (M4.2)