AXIS D8204–E PoE++ Switch

Podręcznik użytkownika

Spis treści

Informacje dotyczące tej instrukcji 3
Skróty 3
Informacje o rozwiązaniu 4
Od czego zacząć 5
Dostęp do produktu przez przeglądarkę 5
Poznaj stronę internetową swojego produktu 5
Zapoznaj się z wbudowaną pomocą swojego produktu 6
Przykłady konfiguracji 7
Konfiguracja sieci VLAN dostępu 7
Zastrzeganie adresu IP w oparciu o adres MAC 8
Tworzenie nadmiarowych łączy pomiędzy przełącznikami w celu zapewnienia nadmiarowości sieci 8
Włączanie lub wyłączanie PoE dla portu za pomocą interfejsu VAPIX 9
Konfiguracja MACsec 9
Statyczny klucz CAK 9
Dynamiczny klucz CAK 10
Podłączanie modułu SFP 1 Gb/s 12
Konserwacja systemu 13
Ponowne uruchamianie produktu 13
Przywracanie domyślnych ustawień fabrycznych 13
Aktualizowanie oprogramowania urządzenia 14
Powrót do alternatywnego obrazu oprogramowania 14
Specyfikacje 15
Przegląd produktów 15
Rozwiązywanie problemów 16
Cyberbezpieczeństwo 17
Zarządzanie podatnościami 17
Powiadomienia dotyczące zabezpieczeń 17
Bezpieczny cykl eksploatacji produktu 17

Informacje dotyczące tej instrukcji

Uwaga

Produkt jest przeznaczony do stosowania przez administratorów sieci, którzy są odpowiedzialni za obsługę i konserwację sprzętu sieciowego. Zakłada się podstawową znajomość pracy ogólnych funkcji przełącznika, zabezpieczeń, protokołu internetowego (IP) i prostego protokołu zarządzania siecią (SNMP).

Ta instrukcja obsługi zawiera informacje o:

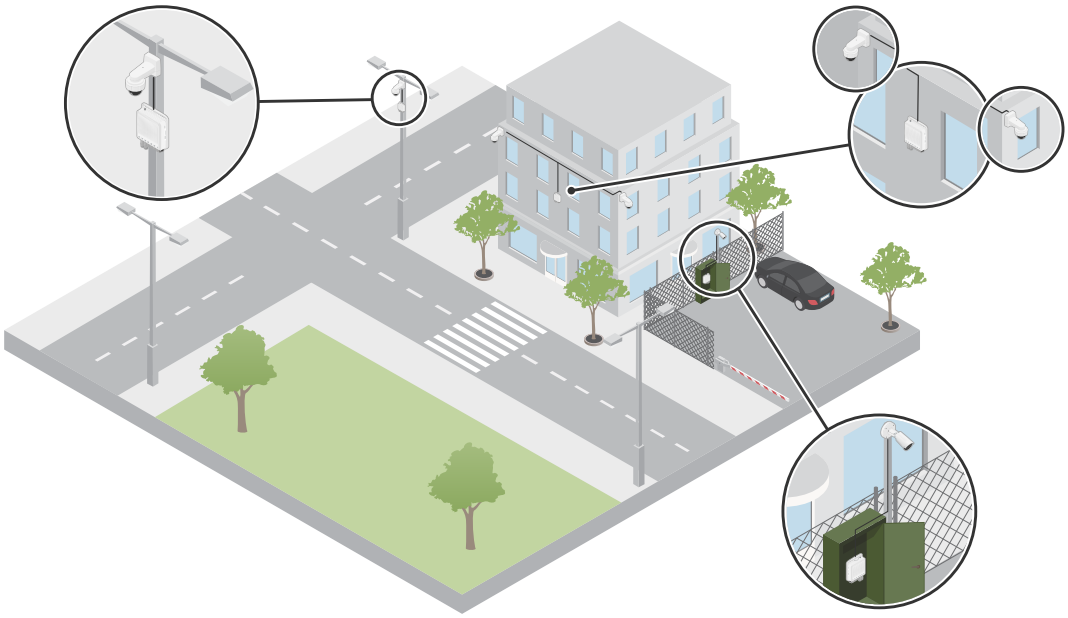
- dostępie do produktu
- konfigurowaniu wybranych przykładów ustawień
- przeprowadzaniu konserwacji produktu

Funkcje produktu i ich ustawienia są opisane bardziej szczegółowo w zależnej od kontekstu wbudowanej pomocy dotyczącej produktu.

Skróty

Skrót	Opis
MACsec	Media Access Control Security
802.1X	Kontrola dostępu do sieci
802.1AE	To samo co MACsec
CAK	Connectivity Association Key
CKN	Connectivity Key Name
DHCP	Protokół dynamicznego konfigurowania hostów (ang. Dynamic Host Configuration Protocol)
OpenSSL	Biblioteka oprogramowania open source
PoE	Zasilanie przez sieć Ethernet
PROMIEŃ	Remote Authentication Dial-in User Service (usługa telefonujących użytkowników zdalnego uwierzytelniania)
SFP	Interfejs światłowodowy, wtyczka mała (Small Form Factor)
SFP+	Rozszerzona wtyczka mała (Enhanced Small Form Factor Plug)
SNMP	Protokół zarządzania urządzeniami sieciowymi (ang. Simple Network Management Protocol)
SSL	Protokół SSL (ang. Secure Sockets Layer)
TLS	Transport Layer Security
VLAN	Virtual Local Area Network (wirtualna sieć lokalna)

Informacje o rozwiązaniu



Urządzenia brzegowe Axis są zainstalowane w środowisku lokalnym i połączone z przełącznikami Axis za pośrednictwem sieci Ethernet. Przełączniki są połączone światłowodem.

Od czego zacząć

Dostęp do produktu przez przeglądarkę

Uwaga

- Zainstaluj, podłącz i włącz zasilanie urządzenia zgodnie z opisem podanym w podręczniku instalacji.
- Po wykonaniu czynności opisanych w tej sekcji przejdziesz na stronę internetową produktu, gdzie będzie można go skonfigurować i nim zarządzać.

1. Użyj narzędzia AXIS IP Utility lub AXIS Device Manager, aby znaleźć urządzenie w sieci. Więcej informacji na temat wykrywania urządzeń można znaleźć na stronie *axis.com/support*.
2. Wprowadź nazwę użytkownika i hasło podane na etykiecie produktu.
   Domyślna nazwa użytkownika to root.
3. Postępuj zgodnie z instrukcjami wyświetlanymi przez kreator instalacji, aby:

– zmienić hasło (zalecane ze względów bezpieczeństwa)

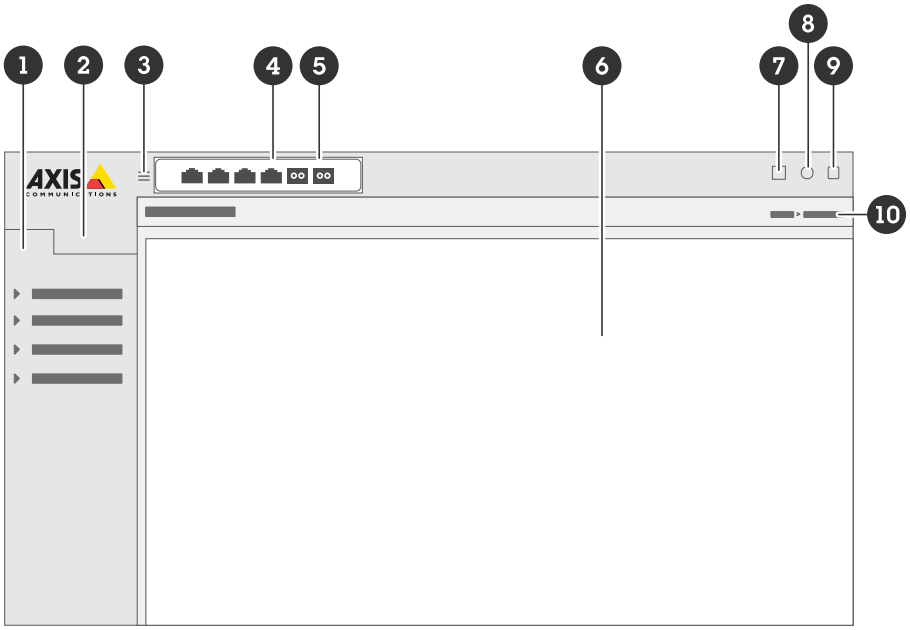
– ustawić adres IP za pośrednictwem usługi DHCP lub ręcznie

– ustawić datę i godzinę

– ustawić informacje o systemie

4. Kliknij przycisk **Save (Zapisz)**.
5. Zaloguj się ponownie przy użyciu nowego hasła.

Poznaj stronę internetową swojego produktu



1 Podstawowe funkcje
2 Zaawansowane funkcje
3 Przycisk przełączania — ukrywanie lub odsłanianie menu
4 Wskaźniki stanu portu RJ45
5 Wskaźniki stanu portu SFP
6 Obszar zawartości podstawowych/zaawansowanych funkcji
7 Przycisk Save (Zapisz) — zapisywanie ustawień w pliku konfiguracji rozruchu
8 Przycisk Pomoc — dostęp do wbudowanej pomocy zależnej od kontekstu
9 Przycisk Wyloguj
10 Ścieżka menu

Zapoznaj się z wbudowaną pomocą swojego produktu

Twój produkt ma wbudowaną pomoc zależną od kontekstu. Pomoc zawiera bardziej szczegółowe informacje na temat podstawowych i zaawansowanych funkcji produktu i ich ustawień. Aby uzyskać dostęp do zawartości pomocy dla danego widoku, kliknij przycisk

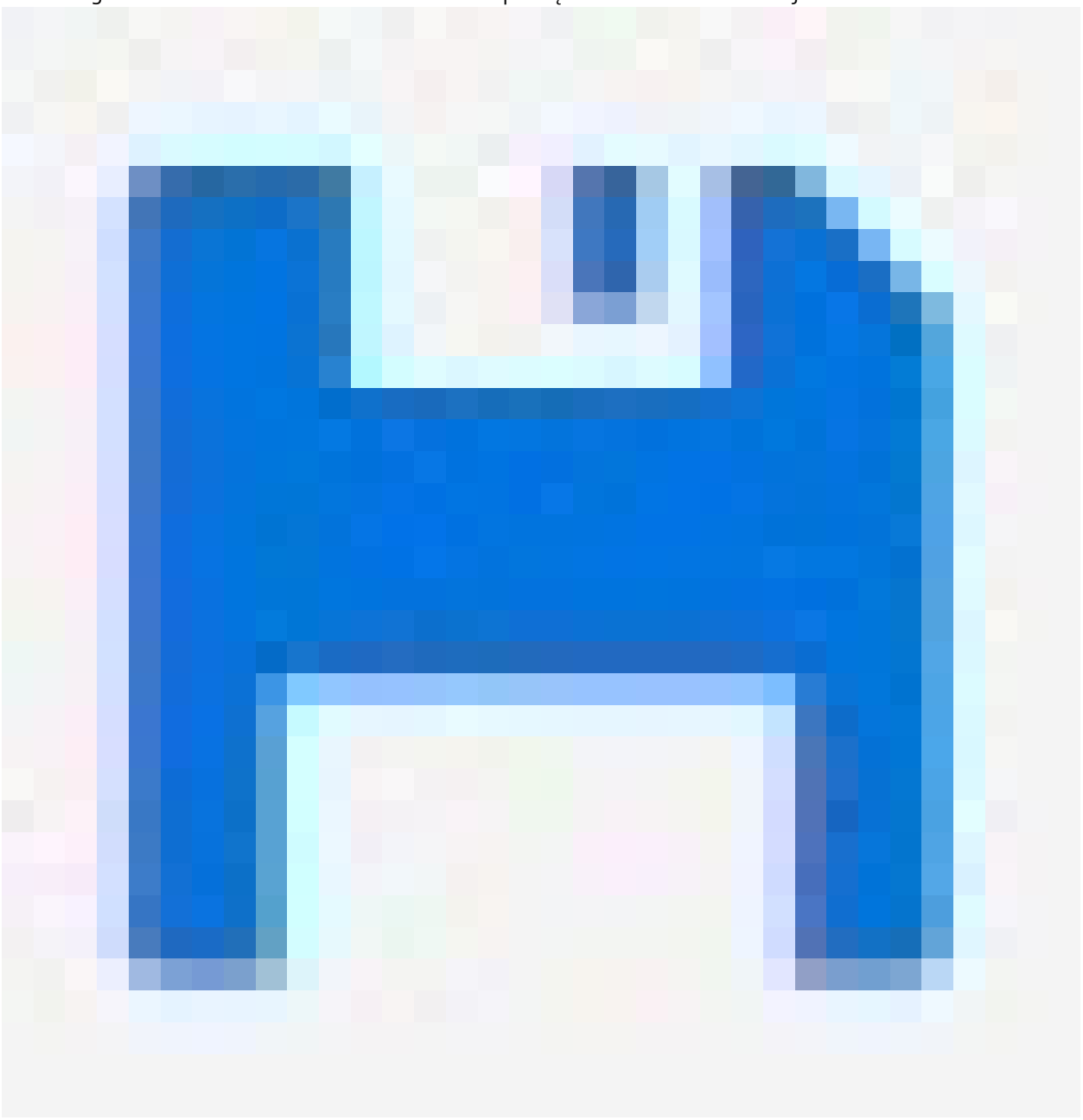


. Niektóre treści pomocy obejmują również klikalne terminy i akronimy, które są bardziej szczegółowo wyjaśnione we wbudowanym słowniku.

Przykłady konfiguracji

Uwaga

Po skonfigurowaniu lub zaktualizowaniu ustawień przełącznika koniecznie kliknij



, aby zapisać aktualizacje w pliku konfiguracji rozruchu.

Plik konfiguracji rozruchu jest zachowywany po ponownym uruchomieniu przełącznika, ale nie po przywróceniu jego domyślnych ustawień fabrycznych.

Konfiguracja sieci VLAN dostępu

Sieci VLAN są zazwyczaj używane w dużych sieciach do tworzenia wielu domen rozgłoszeniowych, ale można je również wykorzystywać do oddzielania ruchu w sieci. Na przykład ruch wideo może być częścią jednej sieci VLAN, a inny ruch w sieci może być częścią innego.

1. Przejdź do **Advanced** > **VLANs** > **Configuration** (Zaawansowane > Sieci VLAN > Konfiguracja).
2. W sekcji **Global VLAN Configuration (Globalna konfiguracja VLAN)** w polu **Allowed Access VLANs (Dozwolone dostępowe sieci VLAN)** wprowadź identyfikatory VLAN ID do utworzenia. Na przykład po

wprowadzeniu: 1, 10–13, 200, 300 zostaną utworzone następujące identyfikatory VLAN ID: 1, 10, 11, 12, 13, 200 i 300.

3. Aby przypisać dany port do utworzonego identyfikatora VLAN ID w sekcji **Port VLAN Configuration (Konfiguracja VLAN portu)**, wprowadź ten identyfikator w polu **Port VLAN (VLAN portu)**.
4. Kliknij przycisk **Save (Zapisz)**.

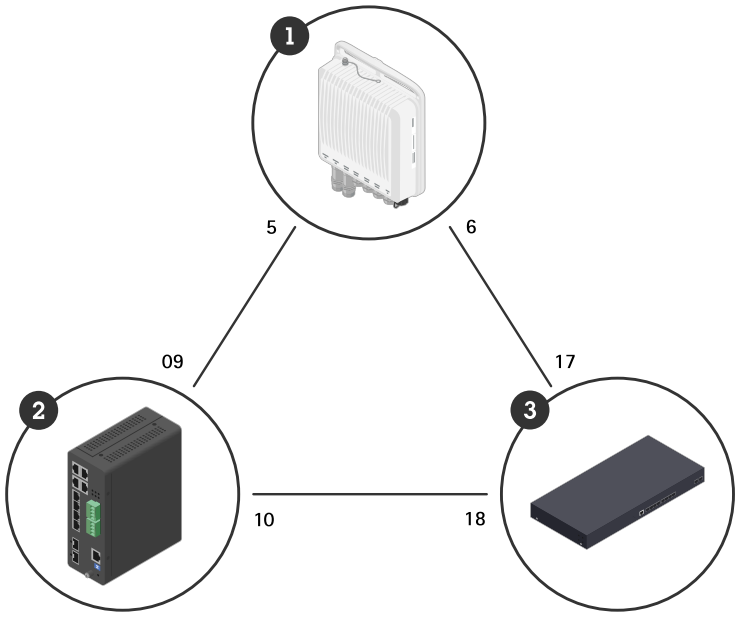
Zastrzeganie adresu IP w oparciu o adres MAC

1. Przejdź do obszaru **Advanced** > **DHCP** > **Server Configuration** > **Pool** (Zaawansowane > DHCP > Serwer > Konfiguracja > Pula).
2. Kliknij polecenie **Add New Pool (Dodaj nową pulę)**.
3. Wprowadź nazwę puli i kliknij **Save (Zapisz)**. Nazwa nie może zawierać spacji.
4. Aby uzyskać dostęp do ustawień puli, kliknij dodaną nazwę.
5. Z menu rozwijanego **Type (Typ)** wybierz **Host**.
6. Wprowadź inne wymagane ustawienia, na przykład adres **IP**, **Subnet Mask (Maskę podsieci)** i **Default Router (Router domyślny)**.
7. W menu rozwijanym **Client Identifier (Identyfikator klienta)** wybierz opcję **MAC**.
8. W polu **Hardware Address (Adres sprzętowy)** wprowadź adres MAC urządzenia.
9. Kliknij przycisk **Save (Zapisz)**.

Tworzenie nadmiarowych łączy pomiędzy przełącznikami w celu zapewnienia nadmiarowości sieci

Jeżeli wymagana jest nadmiarowość sieci, można utworzyć dodatkowe łącza pomiędzy przełącznikami za pomocą konfiguracji drzewa rozpinającego.

Przykład:
W tym przykładzie przełączniki AXIS D8204-E (1), AXIS D8208-R (2) i AXIS T8516 (3) są połączone łączem nadmiarowym, bez dodatkowych sieci VLAN. Jeżeli dowolne łącza uplink między przełącznikami nie powinny działać, zostanie uaktywnione łącze nadmiarowe zapewniające łączność sieciową.



Device name (Nazwa urządzenia):	Nazwa modelu	Porty CIST
Przełącznik - 01	AXIS D8204-E	5, 6

Przełącznik - 02	AXIS D8208-R	9, 10
Przełącznik - 03	AXIS T8516	17, 18

Aby utworzyć nadmiarowe łącze na stronie internetowej przełącznika:

1. Przejdź do **Advanced** > **Spanning Tree** > **Configuration** > **Bridge Settings**(Zaawansowane > Drzewo rozpinające > Konfiguracja > Ustawienia mostka).
2. W opcji **Basic Settings (Ustawienia podstawowe)** w menu rozwijanym **Protocol Version (Wersja protokołu)** wybierz **RSTP** i kliknij przycisk **Save (Zapisz)**.
3. Przejdź do **Advanced** > **Spanning Tree** > **Configuration** > **CIST Port** (Zaawansowane > Drzewo rozpinające > Konfiguracja > Port CIST).
4. W opcji **CIST Normal Port Configuration (Normalna konfiguracja portu CIST)** upewnij się, że wybrana jest wartość **STP Enabled (STP włączone)** dla portów przełącznika w następujący sposób:

- Przełącznik — 01: porty 5 i 6
- Przełącznik — 02: porty 9 i 10
- Przełącznik — 03: porty 17 i 18

5. Kliknij przycisk **Save (Zapisz)**.

Uwaga

Aby upewnić się, że określony port jest używany jako główne łącze komunikacyjne, wprowadź **Path Cost (Koszt ścieżki)** tego portu w opcji **CIST Normal Port Configuration (Normalna Konfiguracja portu CIST)**. Jeżeli nie określono tego parametru, przełącznik wybiera port automatycznie. Aby na przykład użyć portu 17 jako głównego łącza komunikacyjnego, wprowadź wartość **Path Cost (Koszt ścieżki)** 10 do portu 6 i wartość **Path Cost (Koszt ścieżki)** 50 do portu 18.

Włączanie lub wyłączanie PoE dla portu za pomocą interfejsu VAPIX

Za pomocą następujących poleceń dostępnych w interfejsie VAPIX można włączyć lub wyłączyć funkcję PoE dla określonego portu:

- Włączanie PoE:
  `http://[IP address of the switch]/axis-cgi/nvr/poe/setportmode.cgi?port=[number of the port on the switch]&enabled=yes&schemaversion=1`
- Wyłączanie PoE:
  `http://[IP address of the switch]/axis-cgi/nvr/poe/setportmode.cgi?port=[number of the port on the switch]&enabled=no&schemaversion=1`

Konfiguracja MACsec

Konfiguracja MACsec ustanawia bezpieczne połączenie między dwoma urządzeniami obsługującymi standard MACsec, aby zapewnić poufność, uwierzytelnienie oraz ochronę komunikacji między urządzeniami przed atakami typu replay.

Statyczny klucz CAK

Klucz CAK (Connectivity Association Key) to klucz kryptograficzny zapewniający bezpieczną komunikację między urządzeniami. Musi składać się z 32 znaków szesnastkowych w przypadku klucza 128-bitowego lub 64 znaków szesnastkowych w przypadku klucza 256-bitowego.

Nazwa CKN (Connectivity Key Name) identyfikuje klucz w celu nawiązania bezpiecznego połączenia MACsec między urządzeniami i zezwala na udział w bezpiecznej komunikacji wyłącznie autoryzowanym urządzeniom. Nazwa CKN musi składać się z od 2 do 64 znaków szesnastkowych, a liczba znaków musi być parzysta. Nazwa CKN określa, którego klucza CAK należy użyć, a w celu nawiązania komunikacji MACsec zarówno klucz CAK, jak i nazwa CKN muszą być zgodne na obu końcach łącza.

Klucz CAK i nazwę CKN można utworzyć ręcznie lub wygenerować za pomocą narzędzia OpenSSL.

Generowanie klucza CAK i nazwy CKN za pomocą OpenSSL

1. Otwórz wiersz polecenia na komputerze z zainstalowanym oprogramowaniem OpenSSL.
2. Aby wygenerować klucz CAK:
   - Wpisz `openssl rand -hex 16`.
   - Naciśnij klawisz Enter.
3. Aby wygenerować nazwę CKN:
   - Wpisz `openssl rand -hex 8`.
   - Naciśnij klawisz Enter.
4. Zapisz klucz CAK i nazwę CKN. Będą potrzebne później.

Konfiguracja urządzenia z systemem AXIS OS

1. W interfejsie WWW urządzenia przejdź do **System** > **Security** > **Network access control and encryption** (System > Zabezpieczenia > Kontrola dostępu do sieci i szyfrowanie).
2. W polu **Authentication method (Metoda uwierzytelniania)** wybierz **IEEE 802.1AE MACsec (Static CAK/Pre-Shared Key)**.
3. W polu **Key agreement connectivity association key name (Nazwa klucza CAK uzgadniania kluczy)** wpisz nazwę CKN.
4. W polu **Key agreement connectivity association key (Klucz CAK uzgadniania kluczy)** wpisz klucz CAK.
5. Kliknij przycisk **Save (Zapisz)**.

Konfiguracja przełącznika

1. W interfejsie WWW przełącznika przejdź do **Advanced** > **Security** > **MACsec** > **Configuration** > **Policies** (Zaawansowane > Zabezpieczenia > MACsec > Konfiguracja > Zasady).
2. Kliknij przycisk **Add Policy (Dodaj zasadę)**.
3. Wprowadź nazwę zasady.
4. Zaznacz opcję **Enable (Włącz)** i wprowadź wygenerowany klucz CAK oraz nazwę CKN.
5. Kliknij przycisk **Save (Zapisz)**.
6. Przejdź do **Advanced** > **Security** > **MACsec** > **Configuration** > **Interfaces** (Zaawansowane > Zabezpieczenia > MACsec > Konfiguracja > Interfejsy).
   - Dla **Interface (Interfejs)** połączonego z urządzeniem wybierz nową zasadę z listy rozwijanej.
   - Kliknij przycisk **Save (Zapisz)**.

Weryfikacja połączenia

1. W interfejsie WWW przełącznika przejdź do **System** > **Security** > **MACsec** > **Status** > **Status** (System > Zabezpieczenia > MACsec > Stan > Stan).
2. Sprawdź, czy w polu **State (Stan)** widnieje zielony wskaźnik stanu.

Dynamiczny klucz CAK

CAK jest generowany w ramach procesu uwierzytelniania i zarządzania kluczami z wykorzystaniem standardu IEEE 802.1X oraz serwera uwierzytelniającego. Dzięki temu można dynamicznie generować klucze i nimi zarządzać, bez konieczności ręcznego konfigurowania kluczy długoterminowych.

Uwaga

- Upewnij się, że serwer RADIUS jest skonfigurowany i dostępny w sieci.
- Zainstaluj *certyfikat CA identyfikatora urządzenia Axis* na serwerze RADIUS.

Konfiguracja podłączonego urządzenia

1. W interfejsie WWW urządzenia przejdź do **System** > **Security** > **Network access control and encryption** (System > Zabezpieczenia > Kontrola dostępu do sieci i szyfrowanie).
2. W polu **Authentication method (Metoda uwierzytelniania)** wybierz **IEEE 802.1X EAP-TLS / IEEE 802.1AE MACsec (Dynamic CAK) (IEEE 802.1X EAP-TLS / IEEE 802.1AE MACsec (dynamiczny CAK))**.
3. W polu **Client certificate (Certyfikat klienta)** wybierz certyfikat identyfikatora urządzenia Axis, któremu ufa serwer RADIUS. Serwer uwierzytelniania używa certyfikatu do weryfikacji tożsamości klienta.
4. W przypadku pola **CA certificates (Certyfikaty CA)**, gdy nie wybrano żadnego certyfikatu, urządzenie uwierzytelnia się niezależnie od tego, z jaką siecią jest połączone.
5. W polu **EAP Identity (Tożsamość EAP)** wpisz tożsamość użytkownika powiązaną z certyfikatem klienta. Wartość EAP Identity (Tożsamość EAP) musi być zgodna z wartością w polu Common Name (CN) (Nazwa zwyczajowa (CN)) w wybranym certyfikacie klienta.
6. Na liście **EAPOL Version (Wersja EAPOL)** wybierz wersję używaną przez przełącznik sieciowy.
7. Włącz opcję **Use IEEE 802.1X (Użyj IEEE 802.1X)**, aby używać protokołu IEEE 802.1X.
8. Kliknij przycisk **Save (Zapisz)**.

Konfiguracja protokołu 802.1X na przełączniku

1. W interfejsie WWW przełącznika przejdź do **Advanced** > **Security** > **Radius** > **Configuration** (Zaawansowane > Zabezpieczenia > Radius > Konfiguracja).
2. Kliknij **Add new server (Dodaj nowy serwer)** i wprowadź nazwę hosta oraz hasło.
3. Kliknij przycisk **Save (Zapisz)**.
4. Przejdź do **Advanced** > **Spanning Tree** > **Configuration** > **CIST Ports** (Zaawansowane > Drzewo rozpinające > Konfiguracja > Porty CIST).
5. Odznacz pole wyboru **STP Enabled (STP włączone)** dla portu połączonego z urządzeniem.
6. Kliknij przycisk **Save (Zapisz)**.
7. Przejdź do **Advanced** > **Security** > **802.1X** > **Configuration** (Zaawansowane > Zabezpieczenia > 802.1X > Konfiguracja).
8. Na liście **Mode (Tryb)** wybierz **Enabled (Włączone)**.
9. Dla odpowiedniego portu ustaw opcję **Admin state (Stan administratora)** na wartość **Port-based 802.1X (802.1X oparte na portach)**.
10. Kliknij przycisk **Save (Zapisz)**.

Weryfikacja połączenia 802.1X

1. W interfejsie WWW urządzenia przejdź do **System** > **Security (Zabezpieczenia)**.
2. Sprawdź, czy pole **802.1X Authorized (Autoryzowano 802.1X)** ma zielony wskaźnik stanu.

Konfiguracja MACsec na przełączniku

1. W interfejsie WWW przełącznika przejdź do **Advanced** > **Security** > **MACsec** > **Configuration** > **Policies** (Zaawansowane > Zabezpieczenia > MACsec > Konfiguracja > Zasady).
2. Kliknij **Add policy (Dodaj zasadę)** i wpisz nazwę zasady.
3. Kliknij przycisk **Save (Zapisz)**.
4. Przejdź do **Advanced** > **Security** > **MACsec** > **Configuration** > **Interfaces** (Zaawansowane > Zabezpieczenia > MACsec > Konfiguracja > Interfejsy).
5. Dla interfejsu połączonego z urządzeniem wybierz nowo utworzoną zasadę z listy.
6. Kliknij przycisk **Save (Zapisz)**.

Weryfikacja połączenia MACsec

1. Przejdź do **System** > **Security** > **MACsec** > **Status** > **Status** (System > Zabezpieczenia > MACsec > Stan > Stan).

2. Sprawdź, czy w polu **State (Stan)** widnieje zielony wskaźnik stanu.

Uwaga

Jeśli stan połączenia pozostaje oczekujący, uruchom ponownie urządzenie.

Podłączanie modułu SFP 1 Gb/s

1. Przejdź do obszaru **Advanced (Zaawansowane)** > **Ports (Porty)** > **Configuration (Konfiguracja)**.
2. Dla portu, do którego podłączono moduł (5 lub 6), w ustawieniu **Configured (Skonfigurowano)** zaznacz wartość **1 Gbps FDX (1 Gb/s FDX)**.

Uwaga

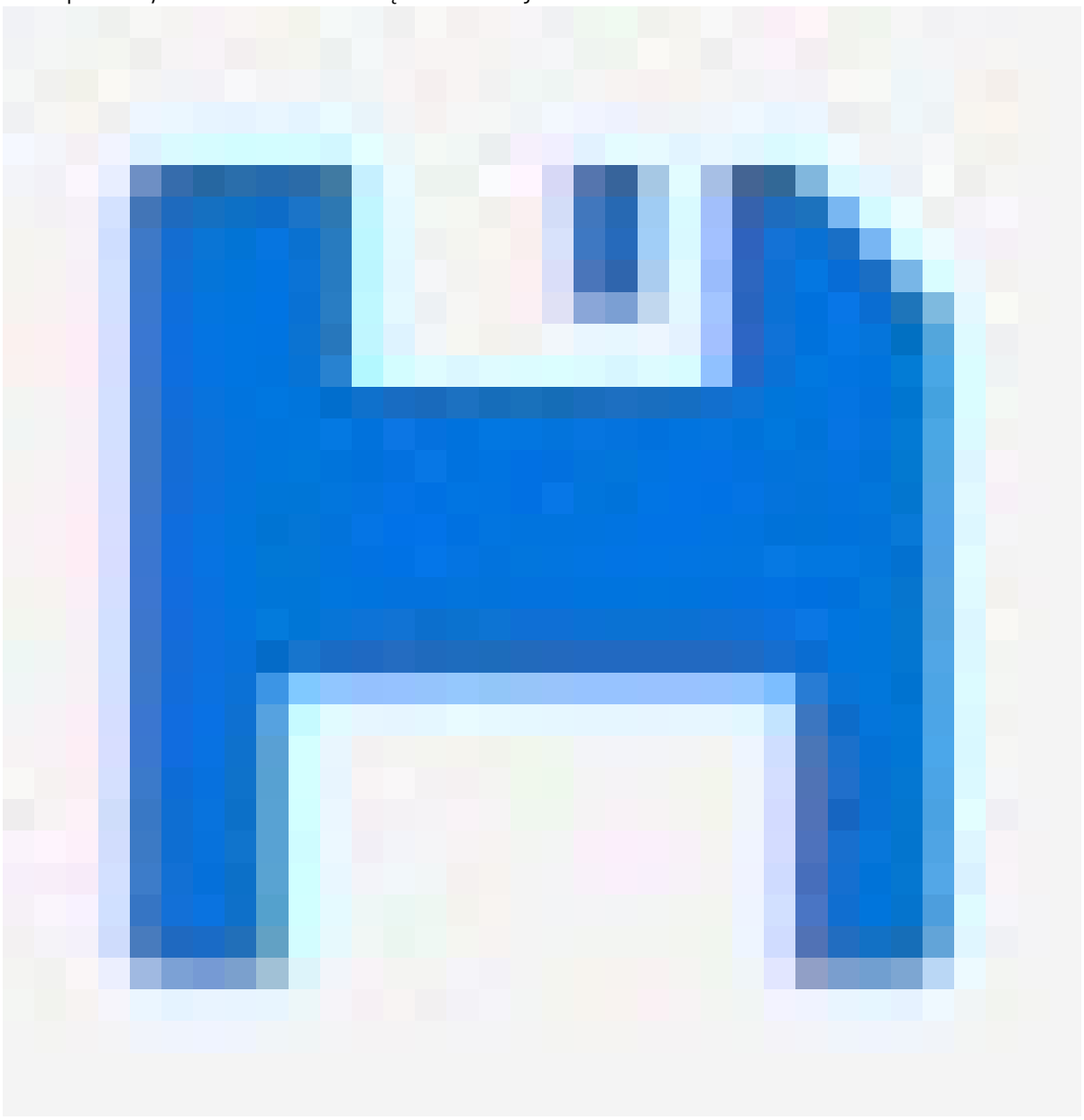
Jeżeli w ustawieniu portu zaznaczono wartość **Auto (Automatycznie)**, będą działały oba protokoły — SFP i SFP+.

Konserwacja systemu

Ponowne uruchamianie produktu

Uwaga

- Ponowne uruchomienie ma wpływ na ruch przepływający przez urządzenie.
- Przed ponownym uruchomieniem urządzenia kliknij



, aby zapisać ustawienia w pliku konfiguracji rozruchu.

1. Przejdź do **Advanced** > **Maintenance** > **Restart Device** (Zaawansowane > Konserwacja > Uruchom ponownie urządzenie).
2. Kliknij **Tak**. Po ponownym uruchomieniu produkt uruchomi się normalnie.

Przywracanie domyślnych ustawień fabrycznych

Ważne

Ewentualna zapisana konfiguracja zostanie przywrócona do domyślnych ustawień fabrycznych.

1. Przejdź do **Advanced** > **Maintenance** > **Factory Defaults** (Zaawansowane > Konserwacja > Ustawienia fabryczne).

2. Kliknij **Tak**.

W przypadku utraty hasła wykonaj następujące czynności, aby przywrócić ustawienia fabryczne:

1. Odłącz wszystko od przełącznika, w tym zasilanie.
2. Podłącz kabel RJ45 między portami 1 i 2.
3. Podłącz kabel zasilający i włącz zasilanie przełącznika.
4. Po 5 minutach odłącz kabel RJ45. Kabel zasilający powinien pozostać podłączony.
5. Podłącz jednostkę do komputera – adres IP powinien powrócić do wartości domyślnej, czyli 192.168.0.254.
6. Przejdź do **Advanced** > **Maintenance** > **Factory Defaults** (Zaawansowane > Konserwacja > Ustawienia fabryczne).
7. Kliknij **Tak**.

Aktualizowanie oprogramowania urządzenia

Ważne

Aktualizacja oprogramowania trwa do 10 minut. W tym czasie nie uruchamiaj ponownie ani nie wyłączaj urządzenia.

Uwaga

Aktualizacja ma wpływ na ruch przepływający przez urządzenie.

1. Przejdź do **Advanced** > **Maintenance**> **Device Software** > **Software Upgrade** (Zaawansowane > Konserwacja > Oprogramowanie urządzenia > Uaktualnienie oprogramowania).
2. Aby wybrać plik oprogramowania z określonej lokalizacji, kliknij **Select file... (Wybierz plik...)**.
3. Kliknij **Aktualizuj**.

Po uaktualnieniu oprogramowania produkt uruchomi się ponownie w normalny sposób.

Powrót do alternatywnego obrazu oprogramowania

Zamiast aktywnego (podstawowego) obrazu oprogramowania w produkcie można użyć alternatywnego (zapasowego) obrazu oprogramowania. Tabele informacji dotyczące obu obrazów są wyświetlane w obszarze **Advanced (Zaawansowane) > Maintenance (Konserwacja) > Device Software (Oprogramowanie urządzenia) > Software Selection (Wybór oprogramowania)**.

Uwaga

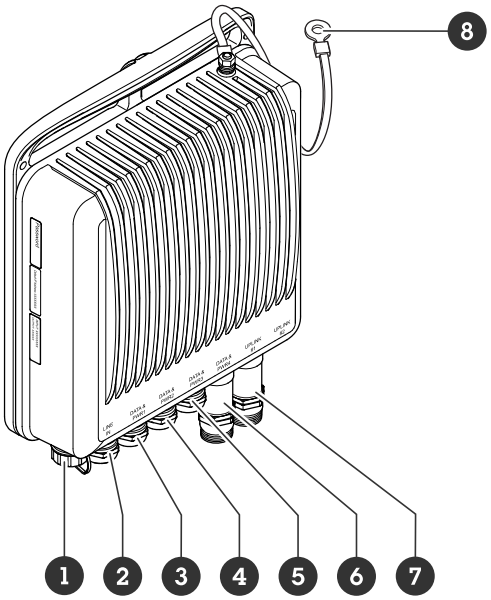
- Jeśli aktywny obraz jest już ustawiony jako obraz alternatywny, wyświetlana jest tylko tabela **Active Image (Aktywny obraz)**, a przycisk **Activate Alternate Image (Aktywuj obraz alternatywny)** jest wyłączony.
- Jeśli obraz alternatywny jest już ustawiony jako obraz aktywny (ręcznie lub na skutek uszkodzenia obrazu podstawowego), a do produktu zostanie przesłany nowy obraz oprogramowania, ten nowy obraz zostanie automatycznie ustawiony jako obraz aktywny.
- W przypadku starszych wersji oprogramowania informacje o wersji oprogramowania i dacie mogą być puste. To normalne.

Aby ustawić obraz alternatywny jako aktywny:

1. Przejdź do obszaru **Advanced (Zaawansowane) > Maintenance (Konserwacja) > Device Software (Oprogramowanie urządzenia) > Software Selection (Wybór oprogramowania)**.
2. Kliknij pozycję **Activate Alternate Image (Aktywuj obraz alternatywny)**.

Specyfikacje

Przegląd produktów



1 Port złącza zasilania
2 – 5. Port RJ45 PoE
6 – 7. gniazdem SFP
8 Przewód uziemienia

Rozwiązywanie problemów

Problemy z dostępem do urządzenia

Nie można się zalogować podczas dostępu do urządzenia z poziomu przeglądarki

Gdy protokół HTTPS jest włączony, upewnij się, że podczas próby zalogowania się używasz prawidłowego protokołu (HTTP lub HTTPS). Może zajść konieczność ręcznego wpisania `http` lub `https` w polu adresu przeglądarki.

Jeśli hasło do konta root zostało utracone, należy zresetować urządzenie do domyślnych ustawień fabrycznych. Instrukcje p. *Przywracanie domyślnych ustawień fabrycznych, on page 13*.

Serwer DHCP zmienił adres IP

Adresy IP otrzymane z serwera DHCP są dynamiczne i mogą się zmieniać. Jeśli adres IP został zmieniony, użyj narzędzia AXIS IP Utility lub AXIS Device Manager, aby zlokalizować urządzenie w sieci. Znajdź urządzenie przy użyciu nazwy modelu lub numeru seryjnego bądź nazwy DNS (jeśli skonfigurowano tę nazwę).

Jeśli potrzebujesz dodatkowej pomocy, odwiedź stronę *axis.com/support* lub zapoznaj się z dokumentem *Axis Network Switches Configuration Guide (Podręcznik konfiguracji przełączników sieciowych Axis)*.

Cyberbezpieczeństwo

Bezpieczeństwo cybernetyczne jest składnikiem udanego cyklu eksploatacji produktu dzięki minimalizacji narażeń. Szczegółowe informacje i dokumentacja na temat naszego podejścia do bezpieczeństwa cybernetycznego znajdują się na stronie *axis.com/about-axis/cybersecurity*. Przestrzegaj poniższych wytycznych dotyczących bezpieczeństwa cybernetycznego, aby otrzymywać powiadomienia od Axis dotyczące bezpieczeństwa produktów oraz skonfigurować produkt w sposób zapewniający bezpieczny cykl eksploatacji oraz wycofanie z użytku.

Na stronie *Axis Trust Center* znajdują się informacje o sposobach, w jakie Axis zapewnia zgodność z wymogami bezpieczeństwa, transparentność, ochronę danych oraz ochronę prywatności.

Zarządzanie podatnościami

Axis ma status *Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA)*. Aby zminimalizować ryzyko narażenia na zagrożenia, postępujemy zgodnie z branżowymi normami w zakresie wykrywania i usuwania luk w zabezpieczeniach naszych urządzeń, oprogramowania i usług. Informacje na temat naszej polityki zarządzania lukami w zabezpieczeniach oraz instrukcje dotyczące zgłaszania luk znajdują się na stronie *axis.com/vulnerability-management*.

Powiadomienia dotyczące zabezpieczeń

Subskrybuj powiadomienia o zagrożeniach bezpieczeństwa w produktach Axis na stronie *axis.com/security-notification-service*. Będziemy informować Cię o lukach w zabezpieczeniach, udzielać odnośnych wskazówek oraz powiadamiać o innych kwestiach związanych z bezpieczeństwem użytkowanego produktu Axis.

Bezpieczny cykl eksploatacji produktu

Axis minimalizuje ryzyko w całym cyklu eksploatacji swoich produktów dzięki bezpiecznemu zarządzaniu cyklem eksploatacji. Skorzystaj z naszych przewodników dotyczących zwiększenia bezpieczeństwa dostępnych na stronie *help.axis.com*, aby bezpieczniej konfigurować i obsługiwać produkty Axis oraz uzyskać informacje na poniższe tematy:

Bezpieczne pierwsze użycie – Produkty Axis są skonfigurowane fabrycznie z wysokim poziomem domyślnej ochrony, co oznacza bezpieczną pierwszą konfigurację oraz szyfrowaną komunikację od samego początku użytkowania.

Przeznaczenie i typowe błędy w konfiguracji – Nasze przewodniki zawierają informacje o przeznaczeniu produktów Axis, w tym o typowych błędach użytkowania związanych z bezpieczeństwem oraz błędach przy konfiguracji, których należy unikać.

Zarządzanie lukami w zabezpieczeniach i transparentność łańcucha dostaw – Wraz z każdą wersją oprogramowania na stronie *axis.com* publikowany jest wykaz komponentów oprogramowania (SBOM – Software Bill of Material) w celu poinformowania o lukach w zabezpieczeniach (podatnościach na zagrożenie) oraz zwiększenia transparentności łańcucha dostaw.

Wycofanie z eksploatacji i bezpieczne usuwanie danych – Aby bezpiecznie wycofać produkt po zakończeniu cyklu eksploatacji, przywróć jego ustawienia fabryczne. Spowoduje to usunięcie konfiguracji, zapisanych danych oraz informacji poufnych.

T10231182_pl

2026-11 (M1.17)

© 2025 – 2026 Axis Communications AB