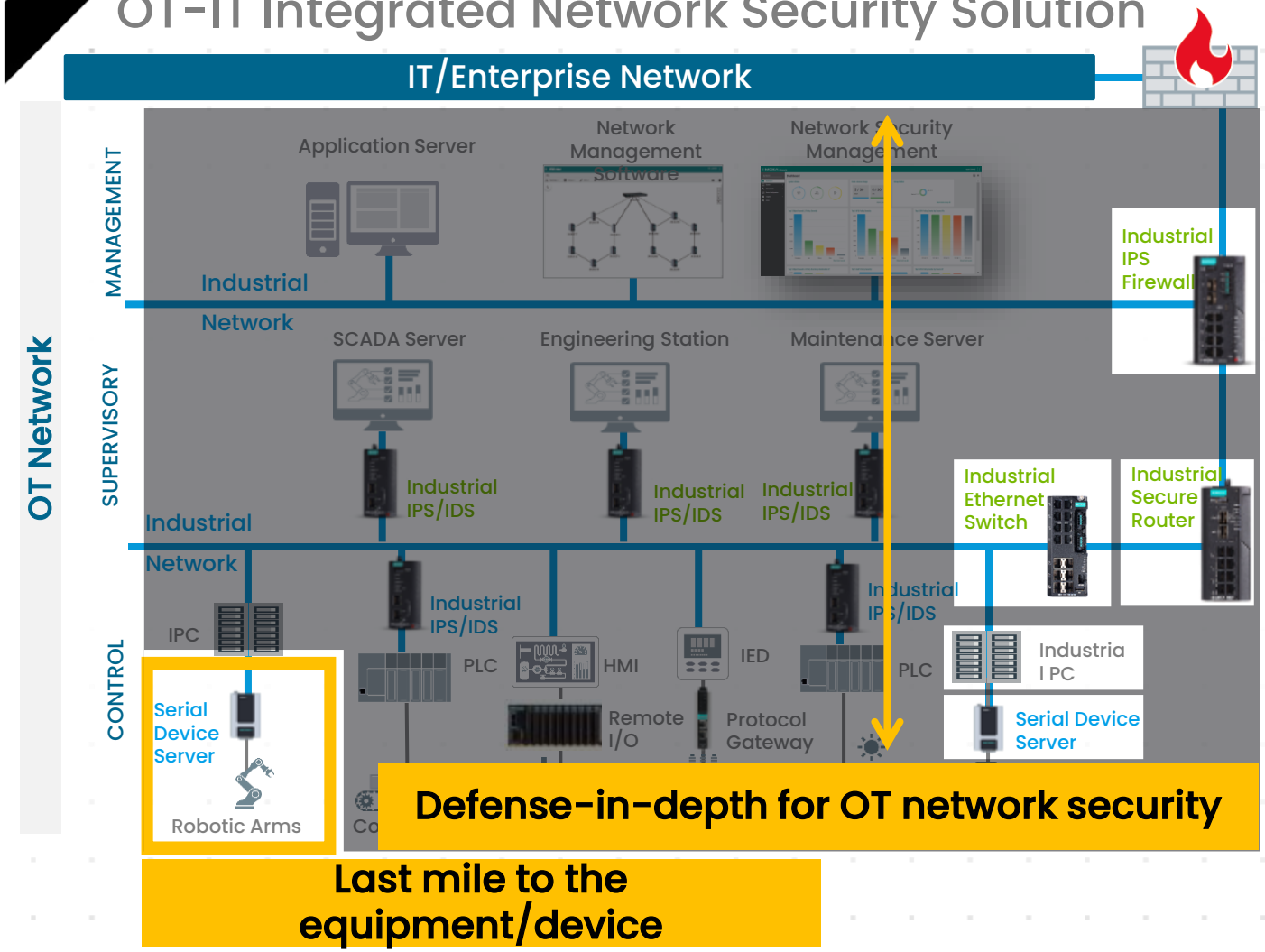
Elmark Automatyka

Nowa generacja komunikacji szeregowej – bezpieczne rozwiązania i monitoring w sieciach elektroenergetycznych

Dariusz Molenda

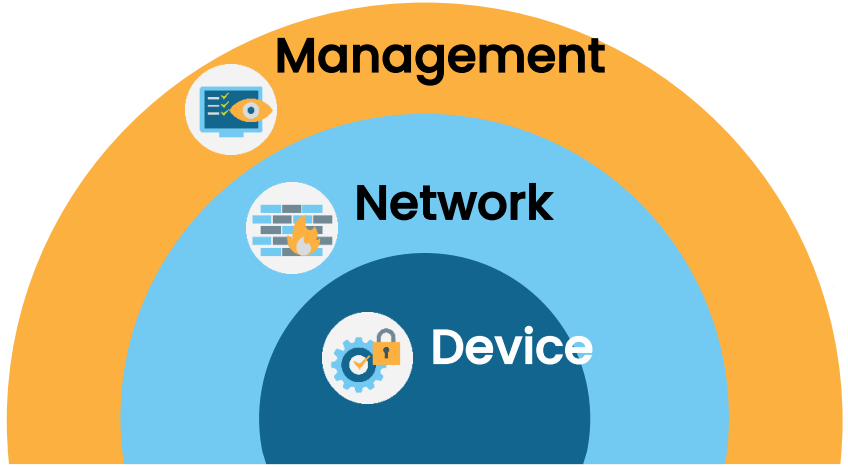
Dlaczego cyberbezpieczeństwa komunikacji szeregowej ma znaczenie?

OT-IT Integrated Network Security Solution

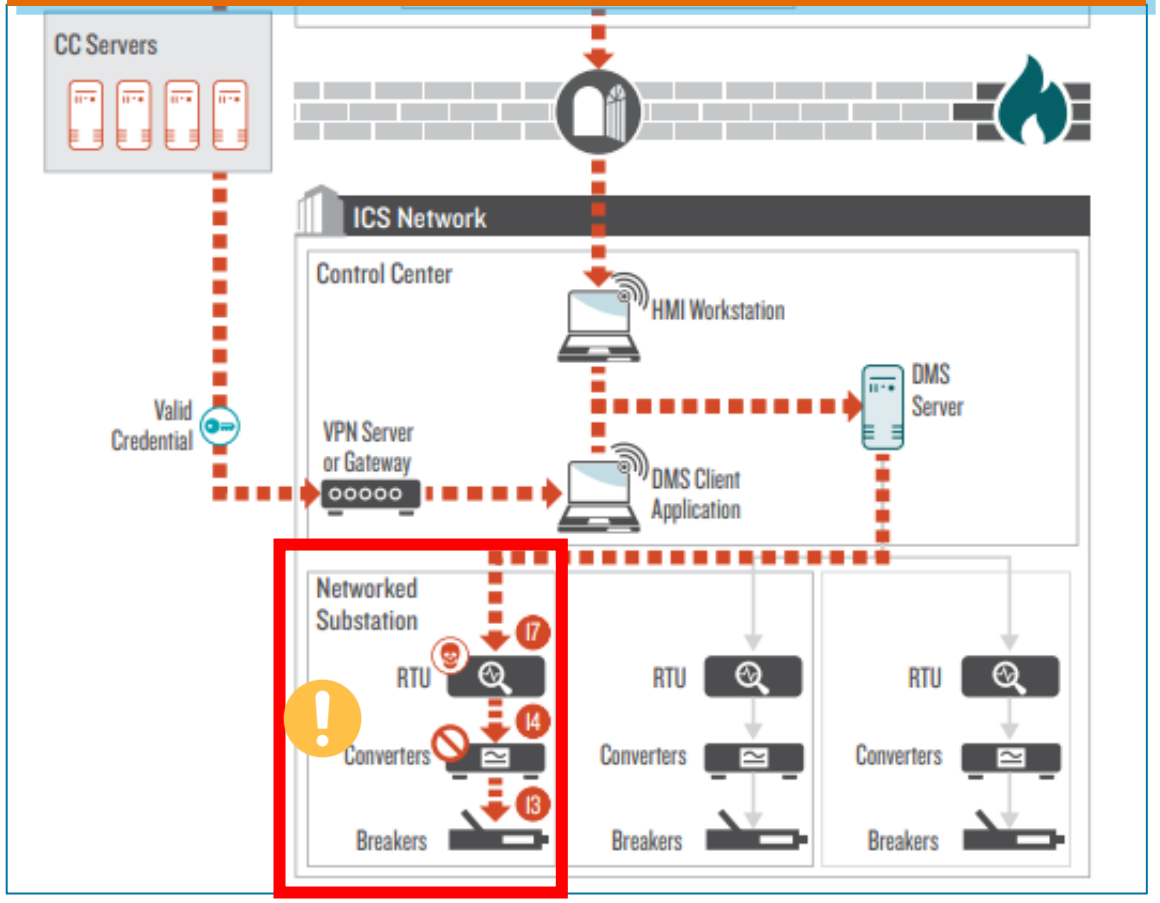


Holistic Security Strategy Aligned with IEC 62443

- Identify Network Status
- Protect Your Networks
- Select Secure Device



Atak na sieć energetyczną na Ukrainie w 2015 r.



Fakty

Konwerter Serial-to-Ethernet był stosowany w celu podłączenia wyłączników do RTU jako połączenie zapasowe.

W ramach 17-etapowego ataku, jeden z kroków polegał na wyłączeniu konwertera, aby uniemożliwić odzyskanie kontroli przez połączenie zapasowe.

Rezultat

Ponad 230 000 osób doświadczyło przerwy w dostawie prądu trwającej od jednej do sześciu godzin.

Wnioski

- Skuteczne cyberbezpieczeństwo wymaga **podejścia warstwowego (defense-in-depth)**.
- Podczas oceny zagrożeń należy **brać pod uwagę łączność brzegową (edge)** – np. urządzenia typu serwer portów szeregowych.

Fakty i zagrożenia

Brak wbudowanych zabezpieczeń w urządzenia

Brak widoczności incydentów

Dane przesyłane są „czytelnie”, bez szyfrowania

28 lat, a mimo to wciąż zaangażowani w łączność szeregową

NPort

Mgate

Nowa rzeczywistość

„Hej! Twoje urządzenie OT musi być zgodne z polityką bezpieczeństwa firmy bla bla bla…”

Musicie udowodnić, w jaki sposób Wasza firma chroni dane krytyczne przed zagrożeniami zgodnie z NIS2…

Bezpieczne połączenie szeregowe z siecią Ethernet kluczowe zagadnienia

Dostęp i integralność

Potencjalne zagrożenia:

- Niezamierzona błędna konfiguracja
- Wspólne domyślne hasło i brak poziomów uprawnień do urządzenia root
- Uruchamianie niezweryfikowanego oprogramowania

Bezpieczna komunikacja

Potencjalne zagrożenia:

- Wyciek danych procesowych w formie otwartego tekstu
- Niezabezpieczony interfejs zarządzania może umożliwić zmianę konfiguracji urządzenia
- Złośliwe działania w celu monitorowania lub przejęcia kontroli nad urządzeniem polowym

Rejestrowanie incydentów

Potencjalne zagrożenia:

- Brak widoczności raportów o incydentach i brak reakcji na zagrożenia
- Niedobór logów lub niewystarczające informacje o incydentach
- Konieczność zgodności z politykami audytu bezpieczeństwa (np. NIS2)

Polityka zarządzania

Potencjalne zagrożenia:

- Luki w produktach i bibliotekach open-source są stale wykorzystywane i odkrywane
- Ujawnienie danych logowania do urządzenia – konieczność okresowych aktualizacji

Jak zabezpieczyć?

Bezpieczne połączenie szeregowe z siecią Ethernet kluczowe zagadnienia

ELMARK Automatyka

Dostęp i integralność

Potencjalne zagrożenia:

- Niezamierzona błędna konfiguracja
- Wspólne domyślne hasło i brak poziomów uprawnień do urządzenia root
- Uruchamianie niezweryfikowanego oprogramowania

Jak zabezpieczyć?

- Secure Boot (bezpieczny rozruch) jest niezbędny dla zachowania integralności
- Uwierzytelnianie oparte na rolach użytkowników i kontrola dostępu do sieci
- Projektowanie pierwszego logowania tak, by wymuszać zmianę domyślnych loginów/hasła

Bezpieczna komunikacja

Potencjalne zagrożenia:

- Wyciek danych produkcyjnych w formie otwartego tekstu
- Niezabezpieczony interfejs zarządzania może umożliwić zmianę konfiguracji urządzenia
- Złośliwe działania w celu monitorowania lub przejęcia kontroli nad urządzeniem polowym

Jak zabezpieczyć?

- Zabezpieczony strumień danych szeregowych i interfejs zarządzania z uwierzytelnieniem i szyfrowaniem
- Zaawansowane, odporne metody szyfrowania

Rejestrowanie incydentów

Potencjalne zagrożenia:

- Brak widoczności raportów o incydentach i brak reakcji na zagrożenia
- Niedobór logów lub niewystarczające informacje o incydentach
- Konieczność zgodności z politykami audytu bezpieczeństwa (np. NIS2)

Jak zabezpieczyć?

- Syslog z dokładnymi typami zdarzeń, poziomami zagrożeń i czasem
- Obsługa centralnych Syslogów dla integracji z systemami SoC/SIEM
- Unikanie nadpisywania lokalnej pamięci

Polityka zarządzania

Potencjalne zagrożenia:

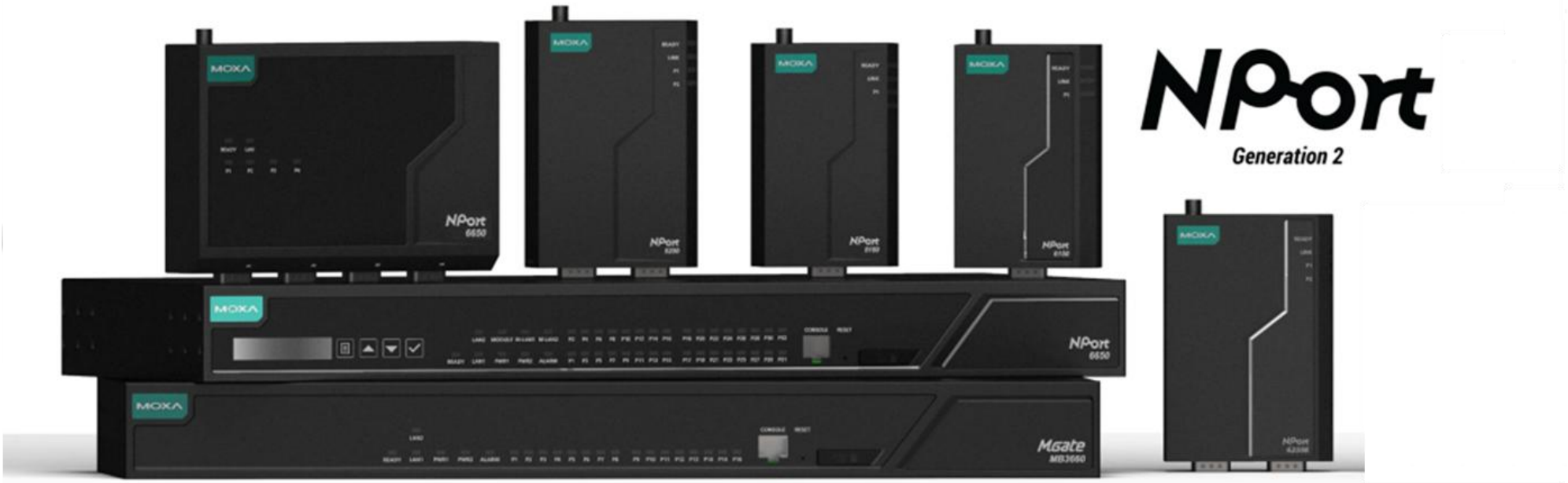
- Luki w produktach i bibliotekach open-source są stale wykorzystywane i odkrywane
- Ujawnienie danych logowania do urządzenia – konieczność okresowych aktualizacji

Jak zabezpieczyć?

- Ciągłe zaangażowanie w aktualizowanie i łatki bezpieczeństwa ma kluczowe znaczenie
- Polityka haseł, która wymusza ich okresowe aktualizacje

Serwery portów szeregowych nowej generacji

czyli NPort 6000-G2



Longevity | **Easy Integration** | **Cyber Security**

Nowe seria urządzeń NPort 6150-G2 / NPort 6250-G2

Model Selection	Serial Port	Secure Boot	SD Card for Serial Buffer	Operating Temperature
NPort 6150-G2	1	v	-	-10 to 60˚C
NPort 6150-G2-T	1	v	-	-40 to 75˚C
NPort 6250-G2	2	v	v	-10 to 60˚C
NPort 6250-G2-T	2	v	v	-40 to 75˚C

*plan certyfikacji koniec 2025 razem z wprowadzeniem modeli 4-32 portowych

1. Opracowano zgodnie z procesem bezpiecznego projektowania

- Zespół certyfikowany zgodnie z normą IEC 62443-4-1
- Cykl życia produktu/projektowanie zgodnie z normami IEC 62443/CRA
- Zgodność z normą IEC 62443-4-2 Secure Level 2 (certyfikacja w planie*)

2. Zarządzenie cyberbezpieczeństwem

- Sprzętowa funkcja Secure Boot pozwala uruchamiać tylko zaufany firmware i konfigurację
- Uwierzytelnianie użytkowników przy użyciu kontroli dostępu opartej na rolach
- Proces pierwszego logowania bez domyślnej nazwy użytkownika i hasła
- Syslog do audytu incydentów

3. Bezpieczna komunikacja

- Zabezpieczony strumień danych szeregowych i interfejs zarządzania z szyfrowaniem i dodatkowym uwierzytelnianiem
- Obsługa najnowocześniejszej metody szyfrowania do RSA 4096 (lub ECC 521= RSA 15360)

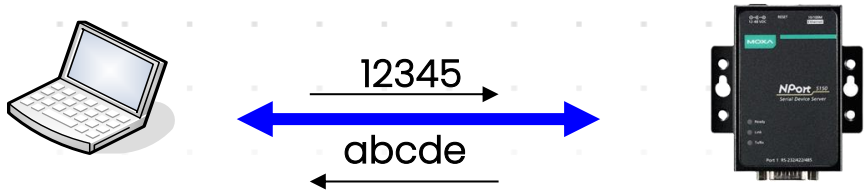
4. Integracja w ramach systemu przedsiębiorstwa

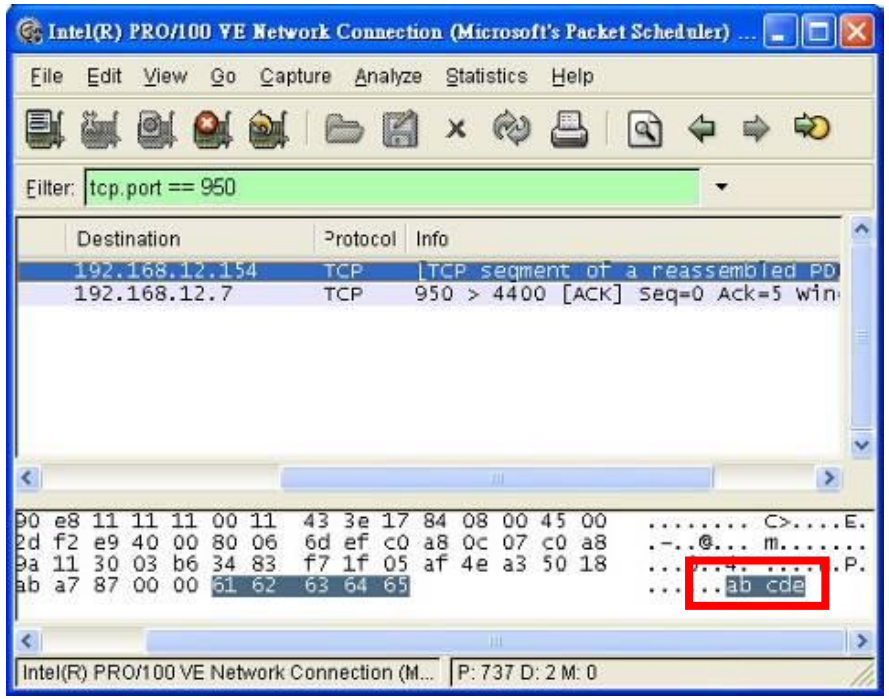
- Obsługa zdalnego syslog (RFC3164) dla SIEM
- Obsługa zdalnego serwera uwierzytelniania dla serwera RADIUS/TACACS+

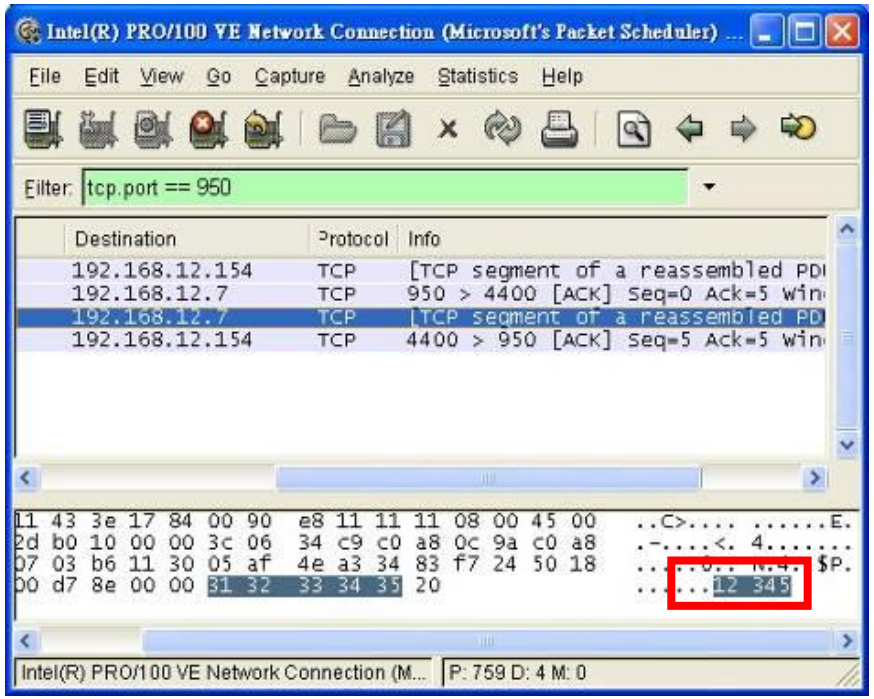
5. Ciągłość obsługi

- Ciągłe zaangażowanie w usuwanie i łatanie luk w zabezpieczeniach.

Szyfrowanie transmisji w warstwie Ethernet

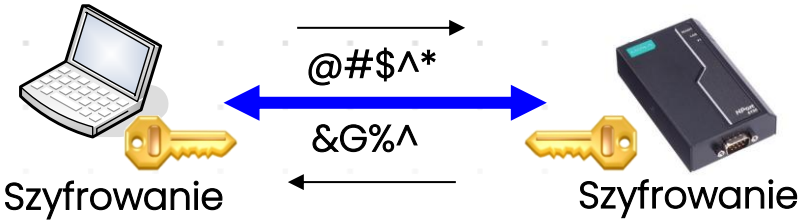


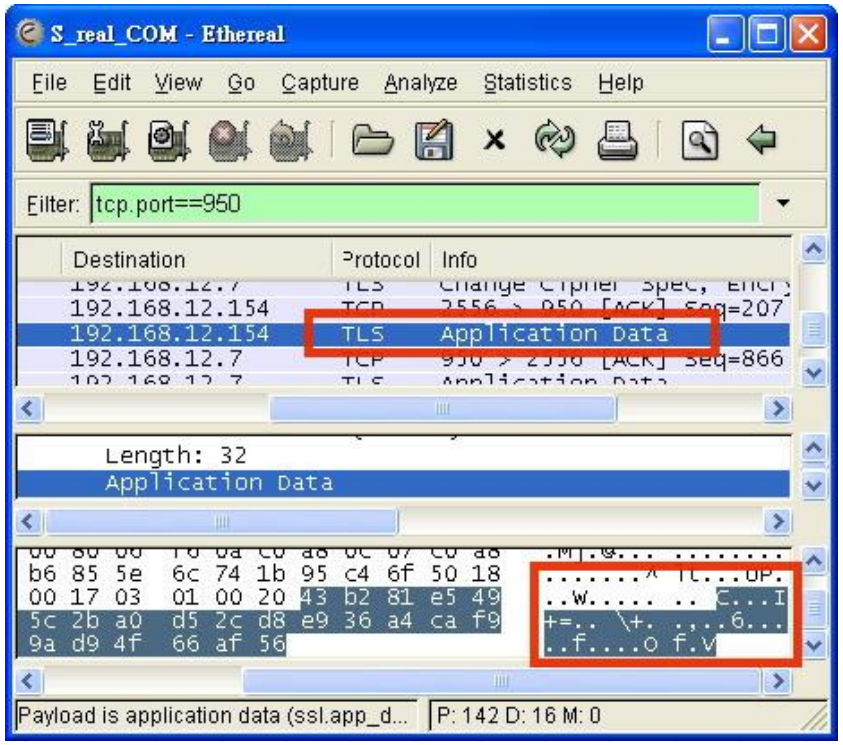


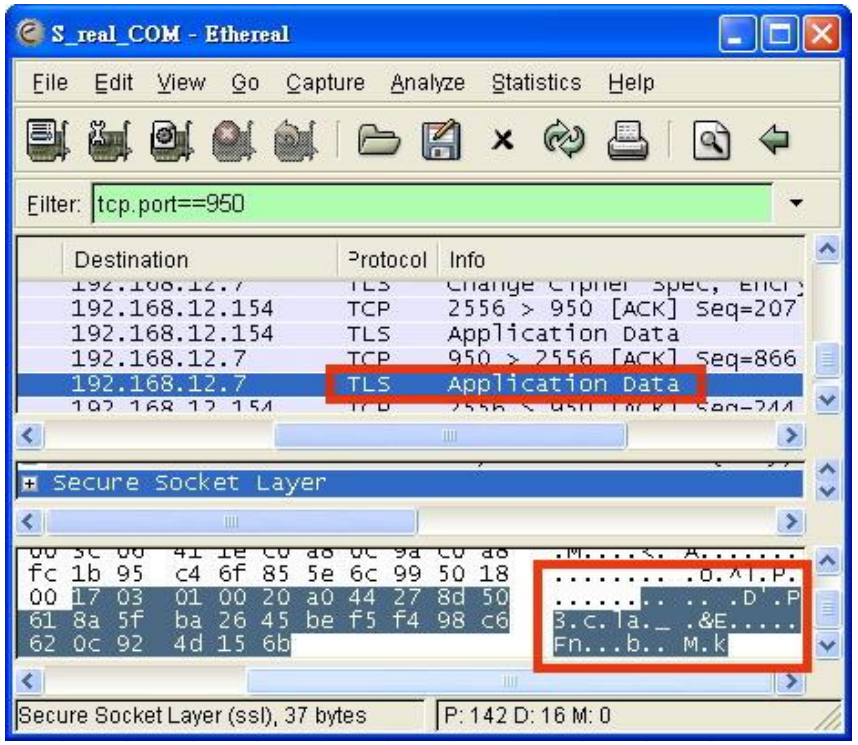


W normalnym trybie NPort 5000 nie szyfruje transmisji. Dane mogą być podsłuchane np. Wiresharkiem.

Szyfrowanie transmisji w warstwie Ethernet







Szyfrowanie transmisji – bezpieczniejsze algorytmy, uwierzytelnianie za pomocą certyfikatu SSL (*.pem)

Nowa konsola www

MOXA | NPort 6250-G2 | Administrator admin

- Dashboard
- System Settings
- Network Settings
- Serial Port Settings
- Security
- Account Management
- Maintenance
- Diagnostics

Home > Dashboard

Dashboard

Device Information

Model Name	NPort 6250-G2
Device Name	NPort-6250-G2_3215
Description	--
Serial Number	TBDGB1043215
MAC Address	00:90:E8:C9:8C:DA
Firmware Version	v1.0.0 Build 24092704

System Operations

Time

System Time	2025-02-07T13:21:20
Uptime	0 day 01h:45m:14s

System State

CPU Usage	26%
Memory Usage	11%
Power Input1	✓ Power on
SD Card	○ Undetected

Network Operations

Device Address

IPv4 Address	192.168.127.254
IPv6 Address	::

Running State

LAN1 ✓ 100MB FD

System Log

Top 5 critical events within the past 30 days — VIEW MORE >

Severity	Category	Event Name	Timestamp
Error	Security	Authentication fail	2025-02-07 12:46:22
Error	Security	Authentication fail	2025-02-07 12:46:21
Warning	Security	Account lockout	2025-02-07 12:46:20
Error	Security	Authentication fail	2025-02-07 12:46:20
Error	Security	Authentication fail	2025-02-07 12:46:19

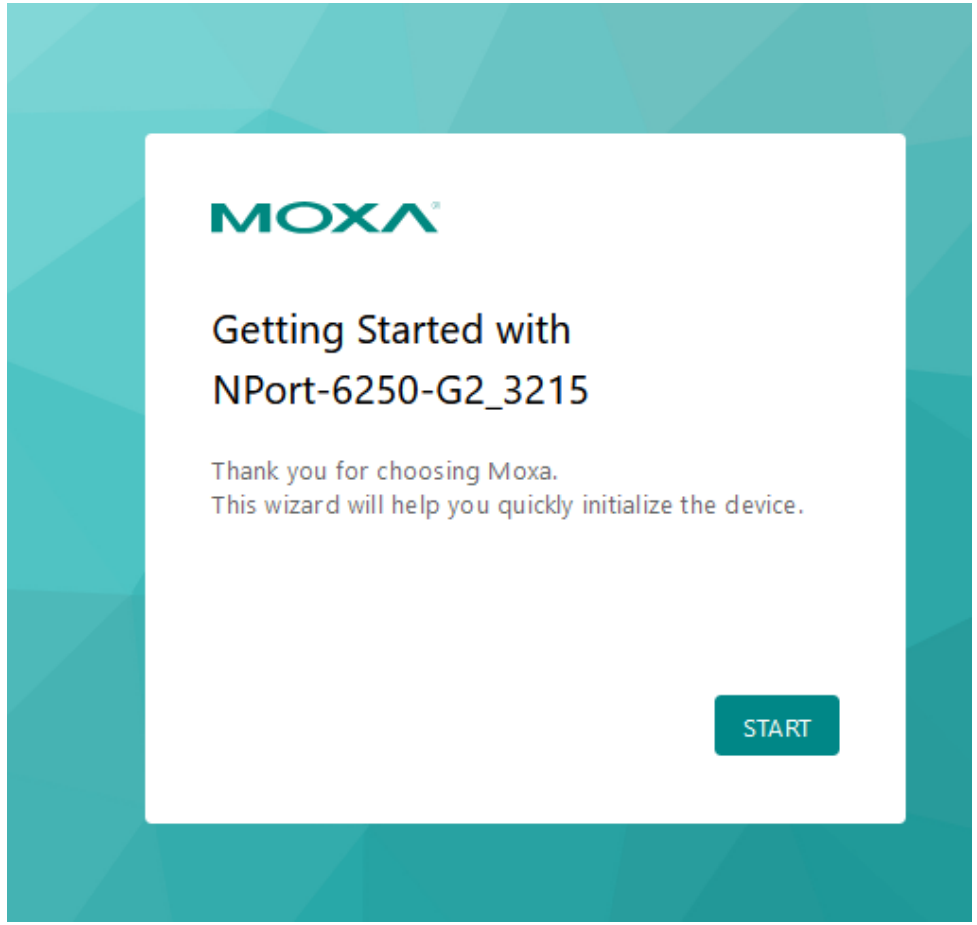
Operation Mode State

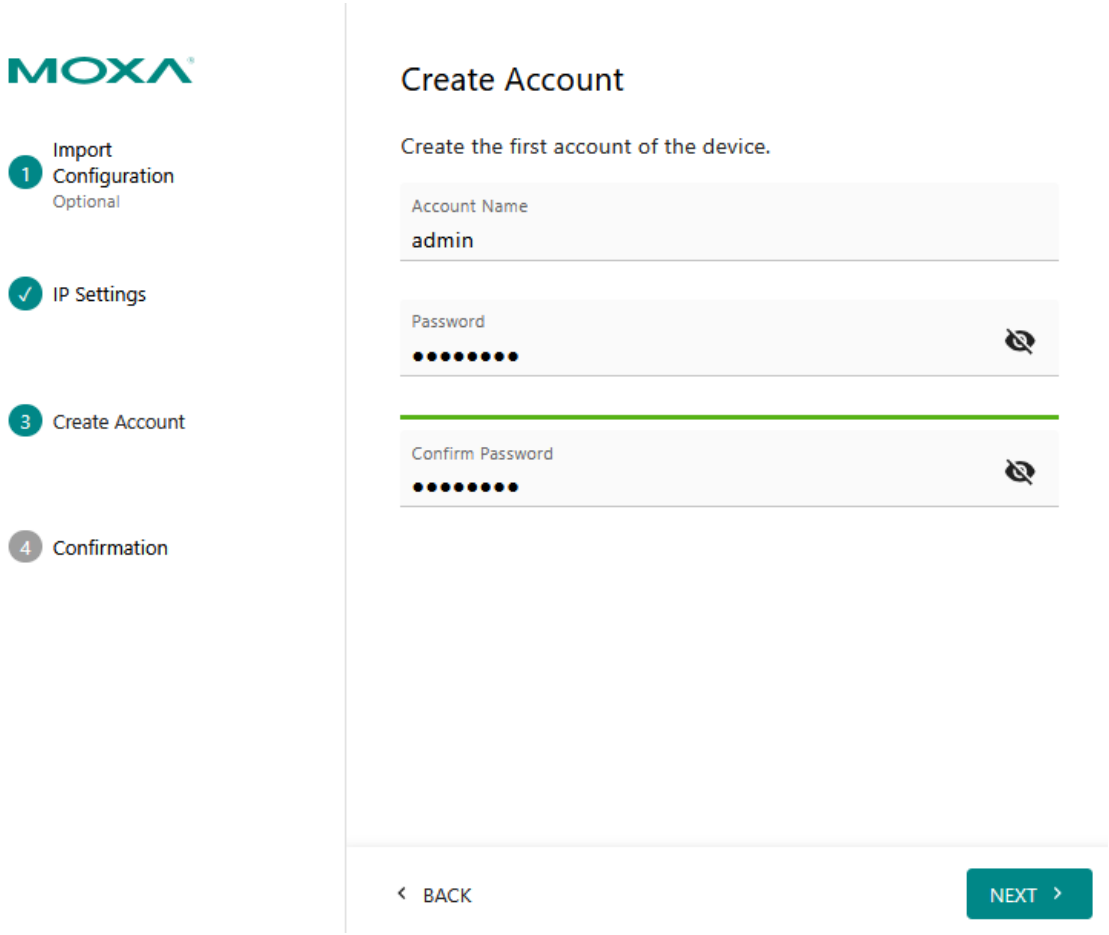
VIEW MORE >

Port	Operation Mode	Connection Status	Serial Parameters	Serial Errors (count)
1	Real COM	Disconnected	RS-232, 19200, None, 8, 1	0
2	Real COM	Disconnected	RS-232, 0, None, 8, 1	0

Pierwsze uruchomienie

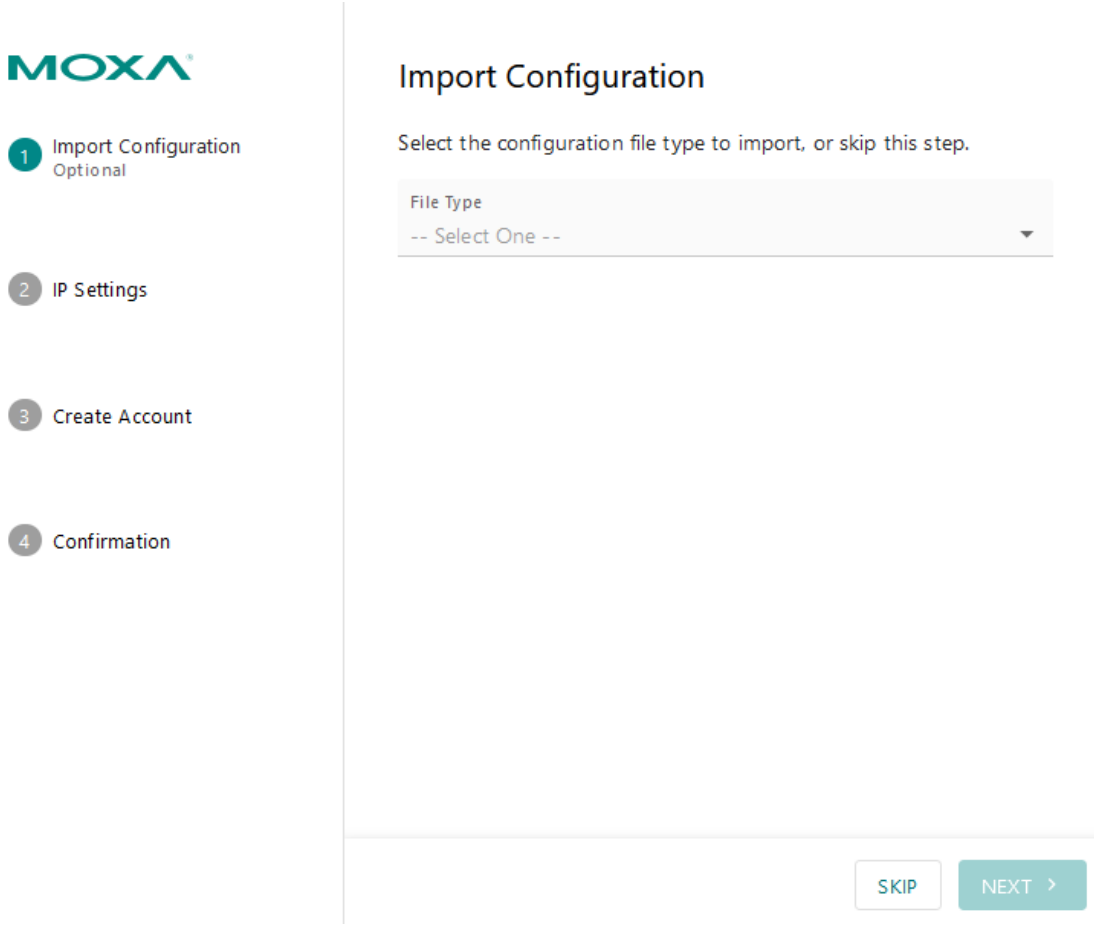
- Wizard który pozwala na przeprowadzenie konfiguracji krok po kroku



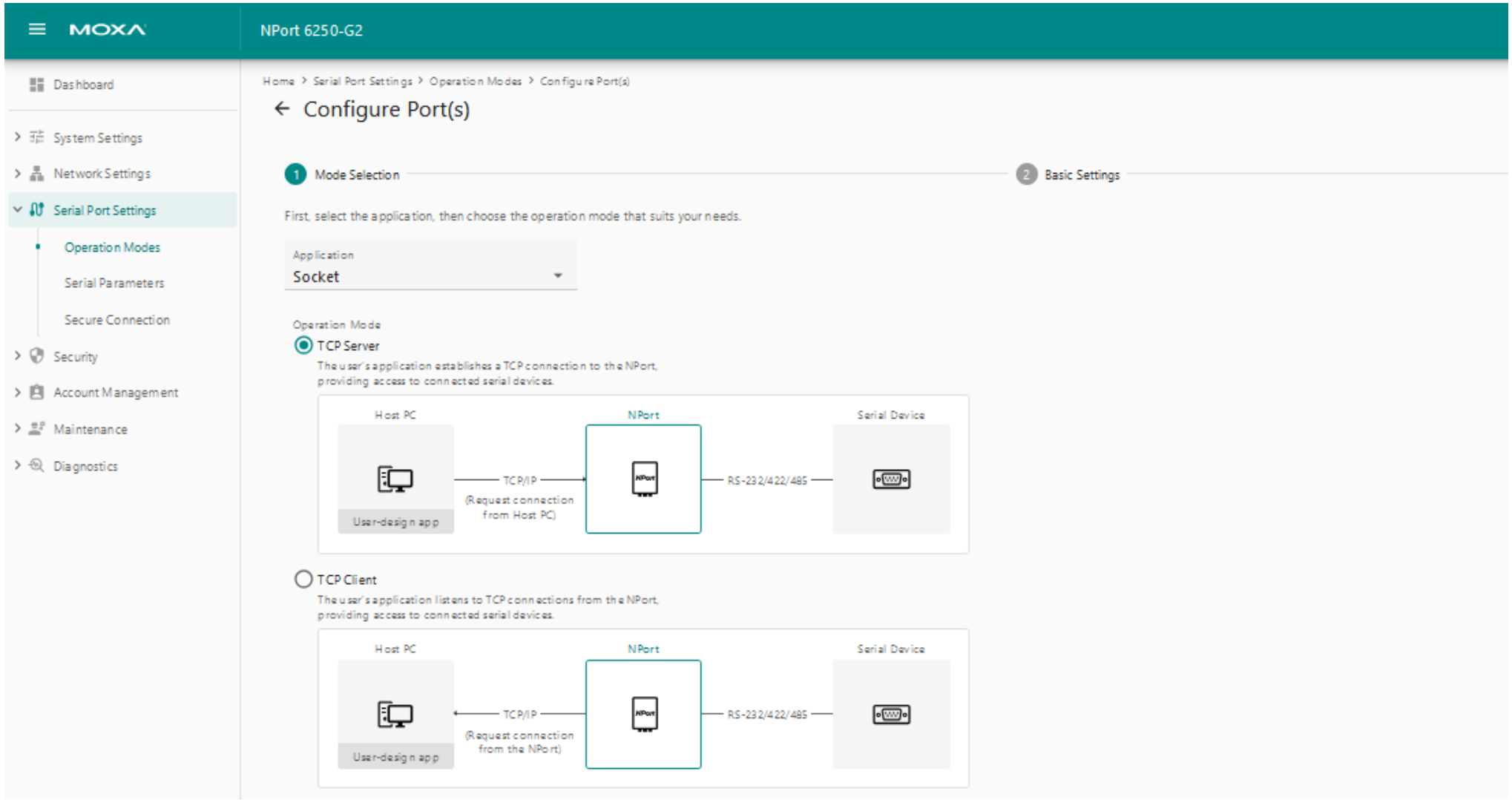


Pierwsze uruchomienie

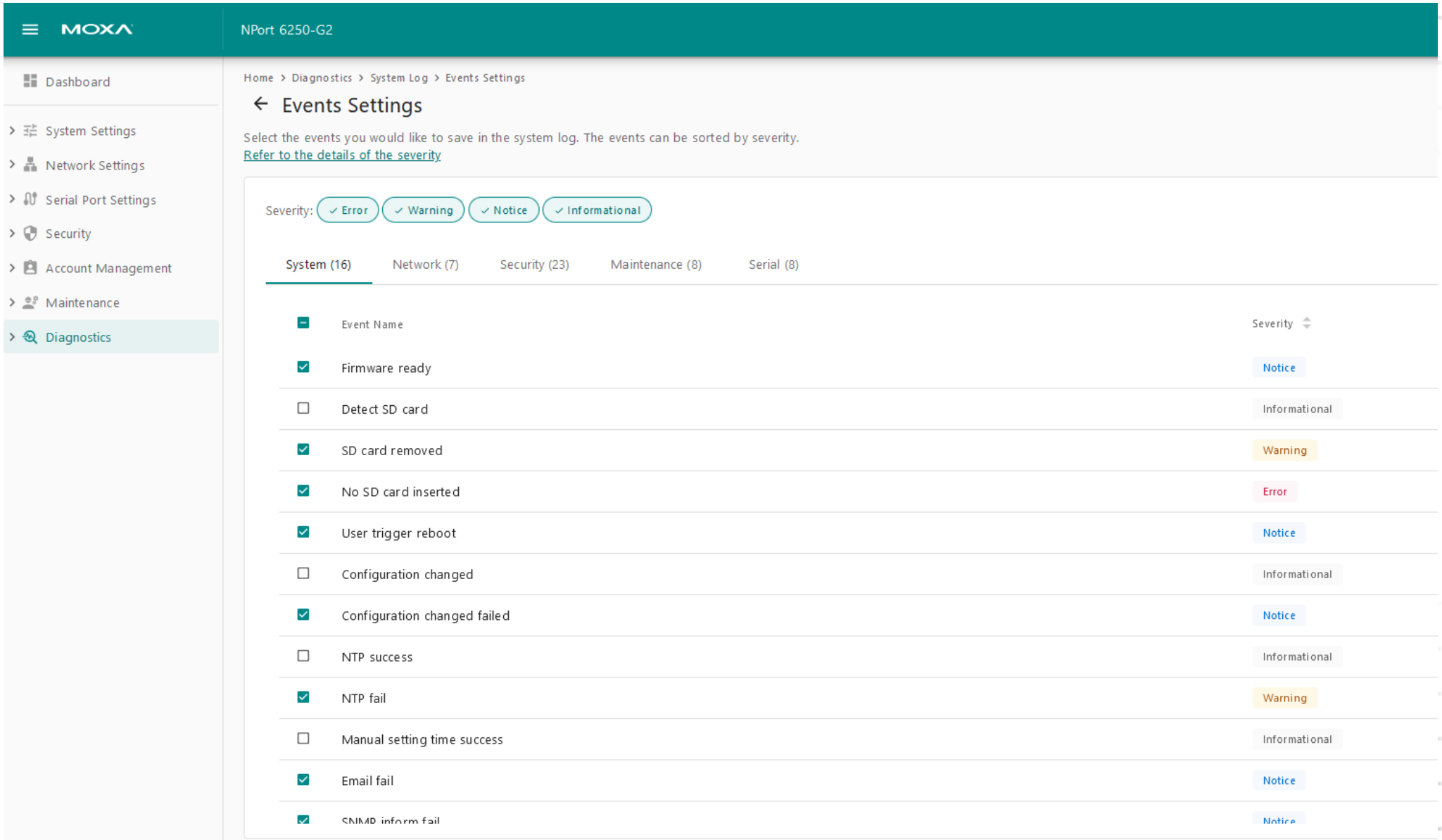
- Możliwość importu konfiguracji z serii NPort 6000 (1. generacja)



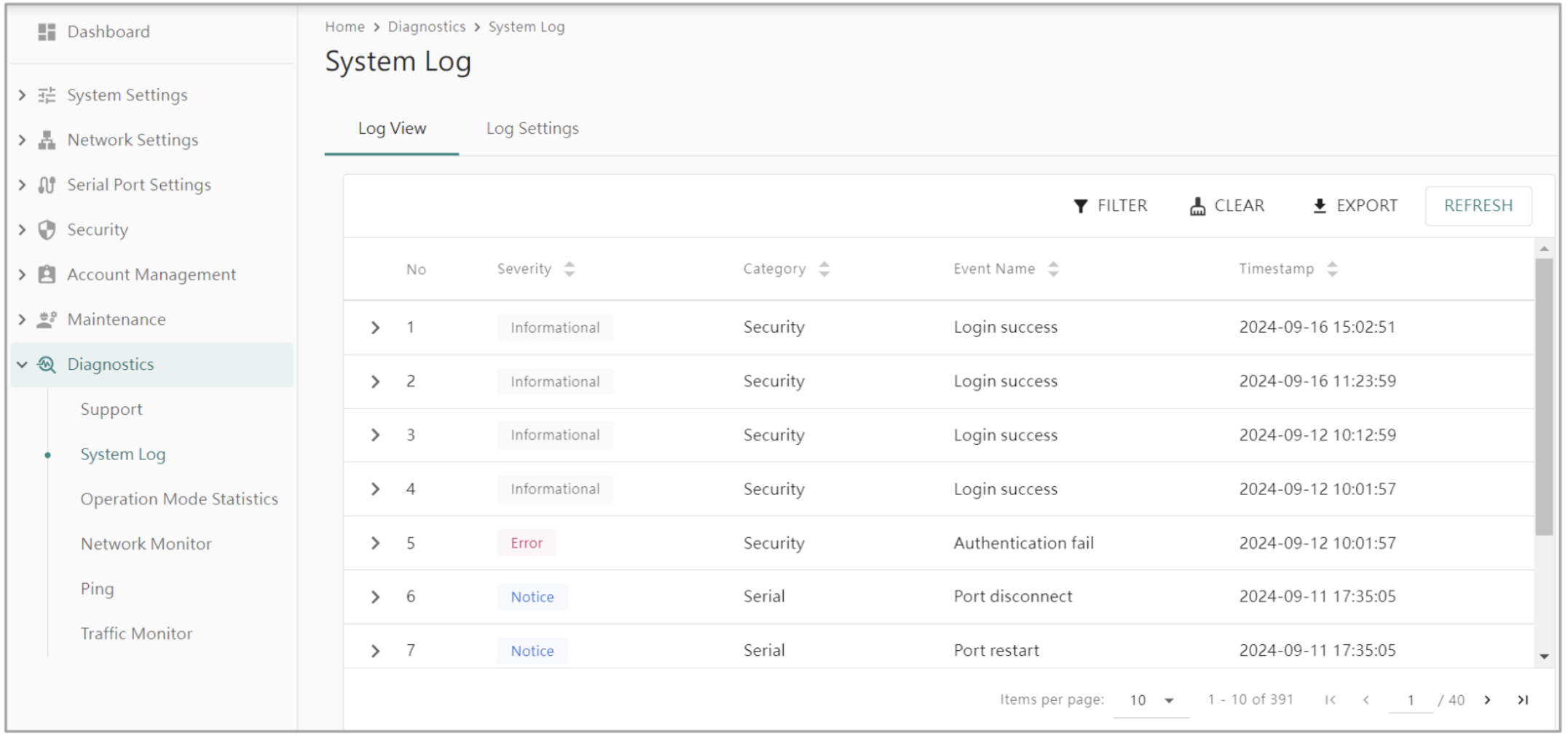
Intuicyjna konfiguracja trybów pracy: wybór trybu



Szczegółowe logi



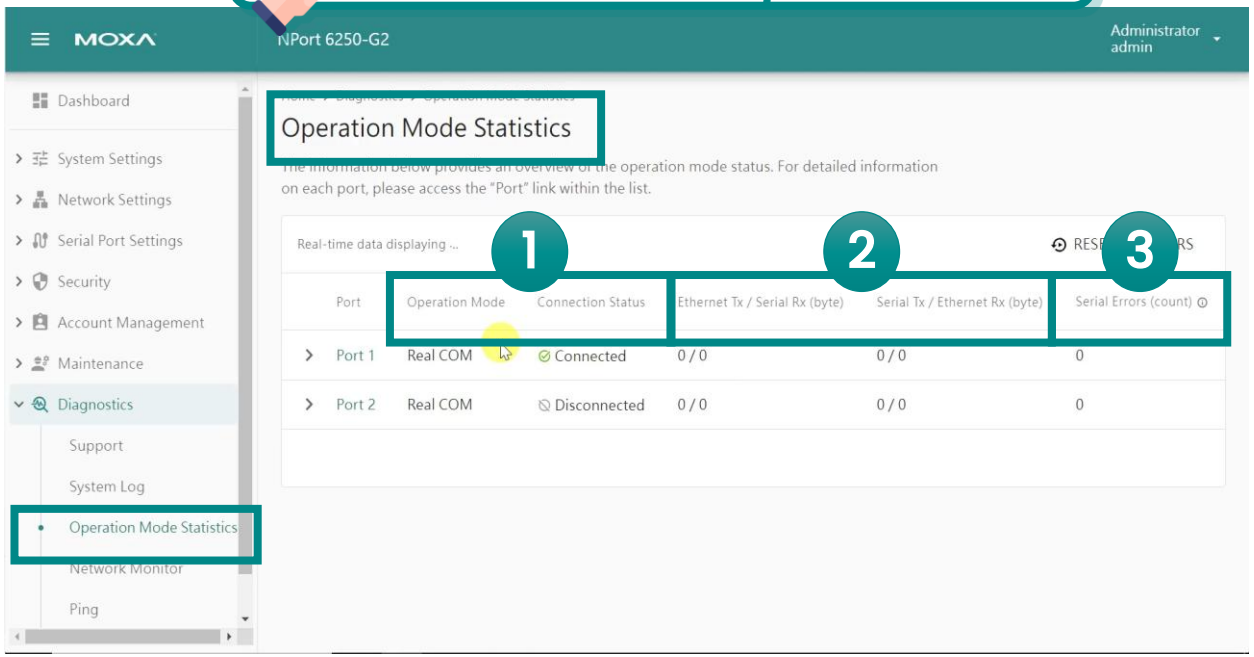
Szczegółowe logi



Stan pracy portu szeregowego

1. Tryb pracy / status połączenia
2. Liczniki danych (Tx/Rx count) dla interfejsu Ethernet i interfejsu szeregowego
3. Licznik błędnych ramek interfejsu szeregowego

Szybkie sprawdzenie transmisji

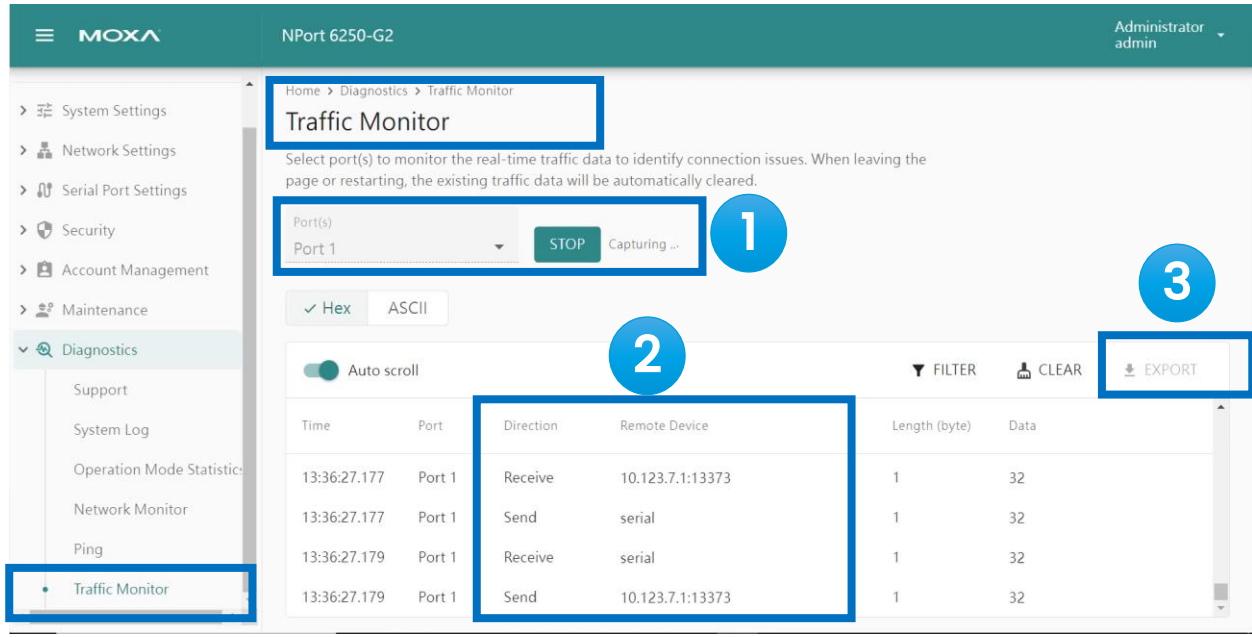


Real-time Traffic Monitoring

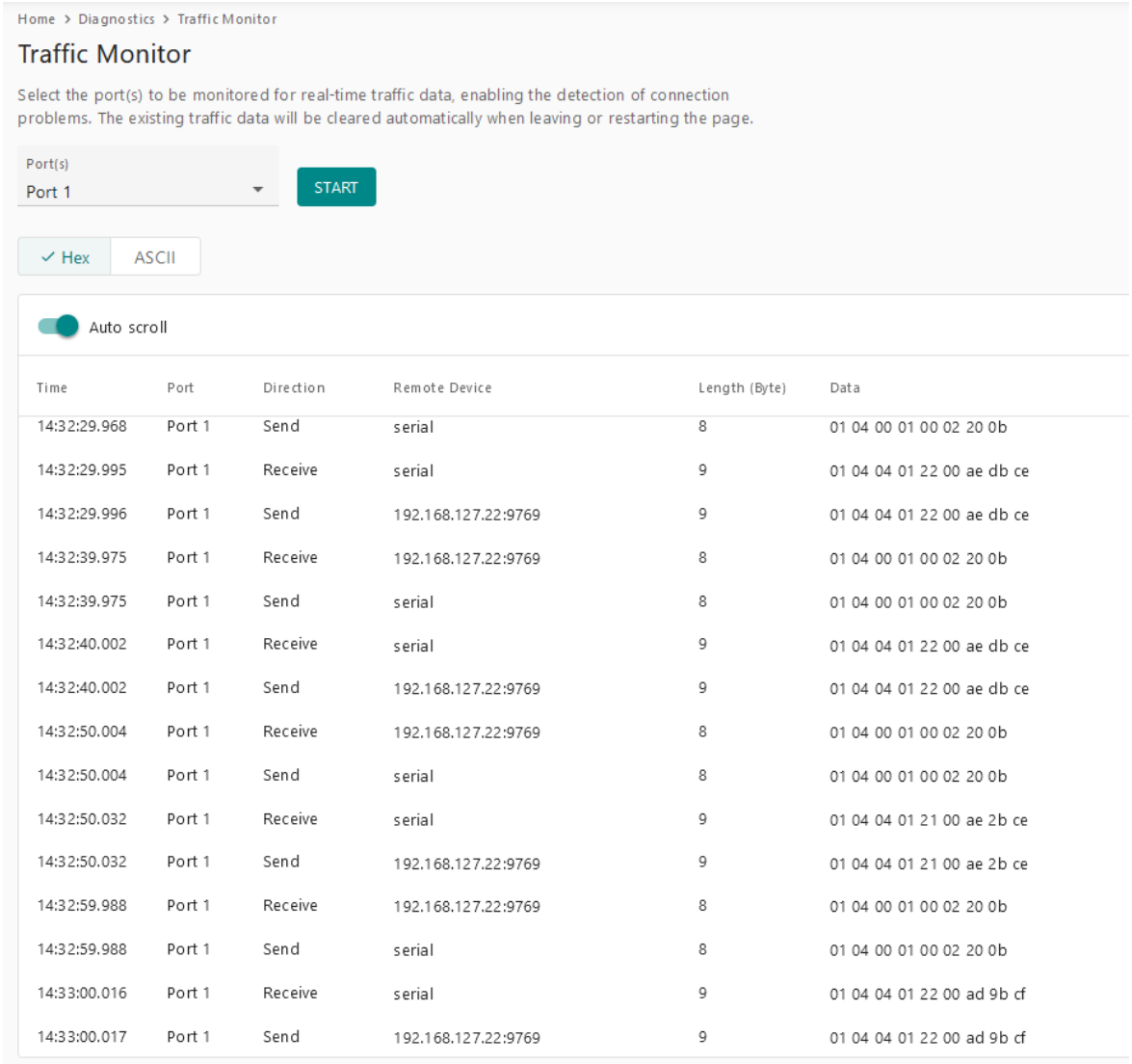
NEW

1. Wybierz port do monitorowania
2. Pakiety serial / Ethernet
3. Możliwość eksportu

Rozwiązywanie problemów



Online Traffic Monitor



Time	Port	Direction	Remote Device	Length (Byte)	Data
14:32:29.968	Port 1	Send	serial	8	01 04 00 01 00 02 20 0b
14:32:29.995	Port 1	Receive	serial	9	01 04 04 01 22 00 ae db ce
14:32:29.996	Port 1	Send	192.168.127.22:9769	9	01 04 04 01 22 00 ae db ce
14:32:39.975	Port 1	Receive	192.168.127.22:9769	8	01 04 00 01 00 02 20 0b
14:32:39.975	Port 1	Send	serial	8	01 04 00 01 00 02 20 0b
14:32:40.002	Port 1	Receive	serial	9	01 04 04 01 22 00 ae db ce
14:32:40.002	Port 1	Send	192.168.127.22:9769	9	01 04 04 01 22 00 ae db ce
14:32:50.004	Port 1	Receive	192.168.127.22:9769	8	01 04 00 01 00 02 20 0b
14:32:50.004	Port 1	Send	serial	8	01 04 00 01 00 02 20 0b
14:32:50.032	Port 1	Receive	serial	9	01 04 04 01 21 00 ae 2b ce
14:32:50.032	Port 1	Send	192.168.127.22:9769	9	01 04 04 01 21 00 ae 2b ce
14:32:59.988	Port 1	Receive	192.168.127.22:9769	8	01 04 00 01 00 02 20 0b
14:32:59.988	Port 1	Send	serial	8	01 04 00 01 00 02 20 0b
14:33:00.016	Port 1	Receive	serial	9	01 04 04 01 22 00 ad 9b cf
14:33:00.017	Port 1	Send	192.168.127.22:9769	9	01 04 04 01 22 00 ad 9b cf

Rezystory terminujące oraz pull high/low włączane/wyłączane z poziomu konsoli www

Configure Port(s)

Baudrate (bps)
9600

Parity
None

Data Bits
8

Stop Bit(s)
1

Flow Control
None

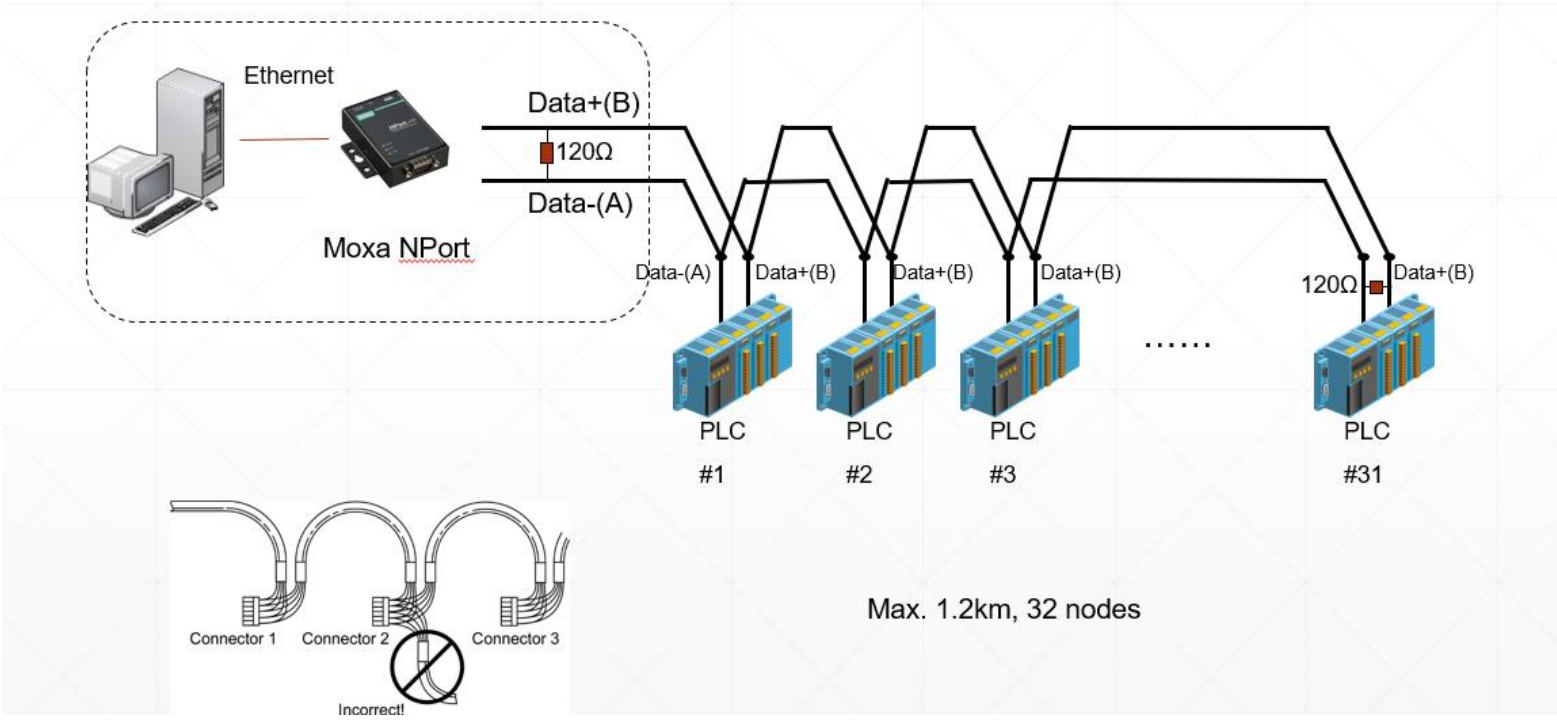
Advanced Settings

Enable FIFO
Enabling FIFO results in increased throughput for serial communication. Disabling FIFO reduces latency.

Enable terminator (120 Ω)
For RS-422/485, especially for long distance communication, we recommend you enable the terminator to prevent the reflection of serial signals on the first and the last RS-422/485 devices.

Resistor
150 KΩ

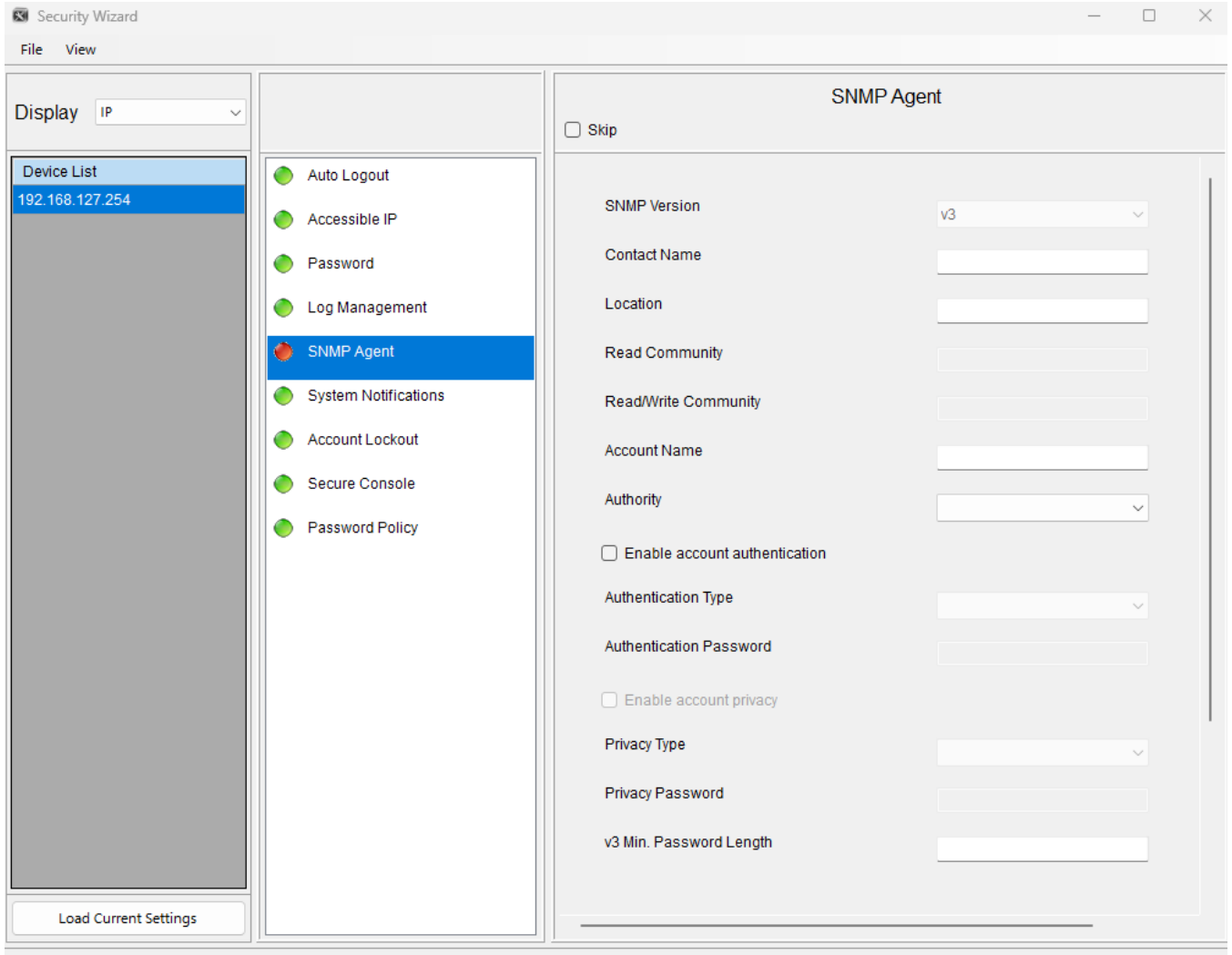
CANCEL SAVE



IEC 62443-4-2: Security Wizard

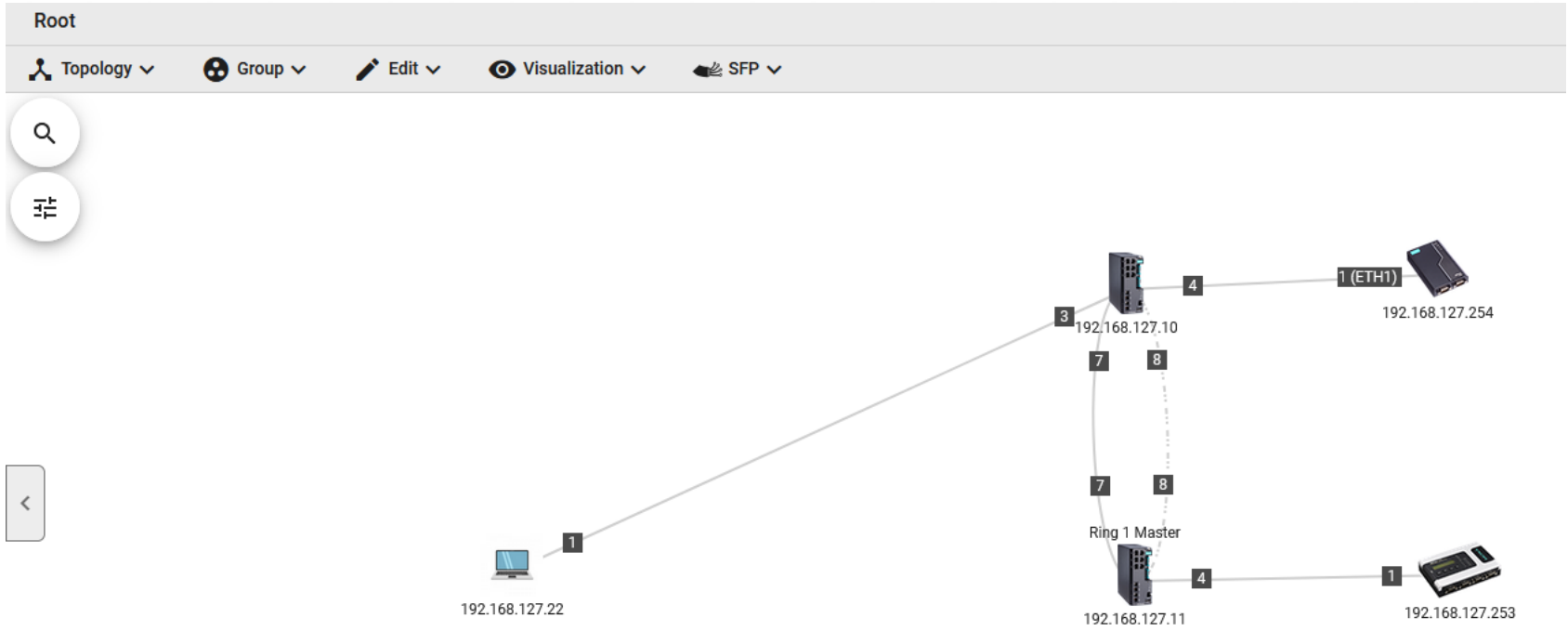
- **Security Wizard w oprogramowaniu MXConfigCS**
  - łatwa implementacja zasad cyberbezpieczeństwa zgodnych z IEC 62443-4-2

- **Security View w oprogramowaniu MxView One**
  - audyt cyberbezpieczeństwa zgodnie z IEC 62443-4-2



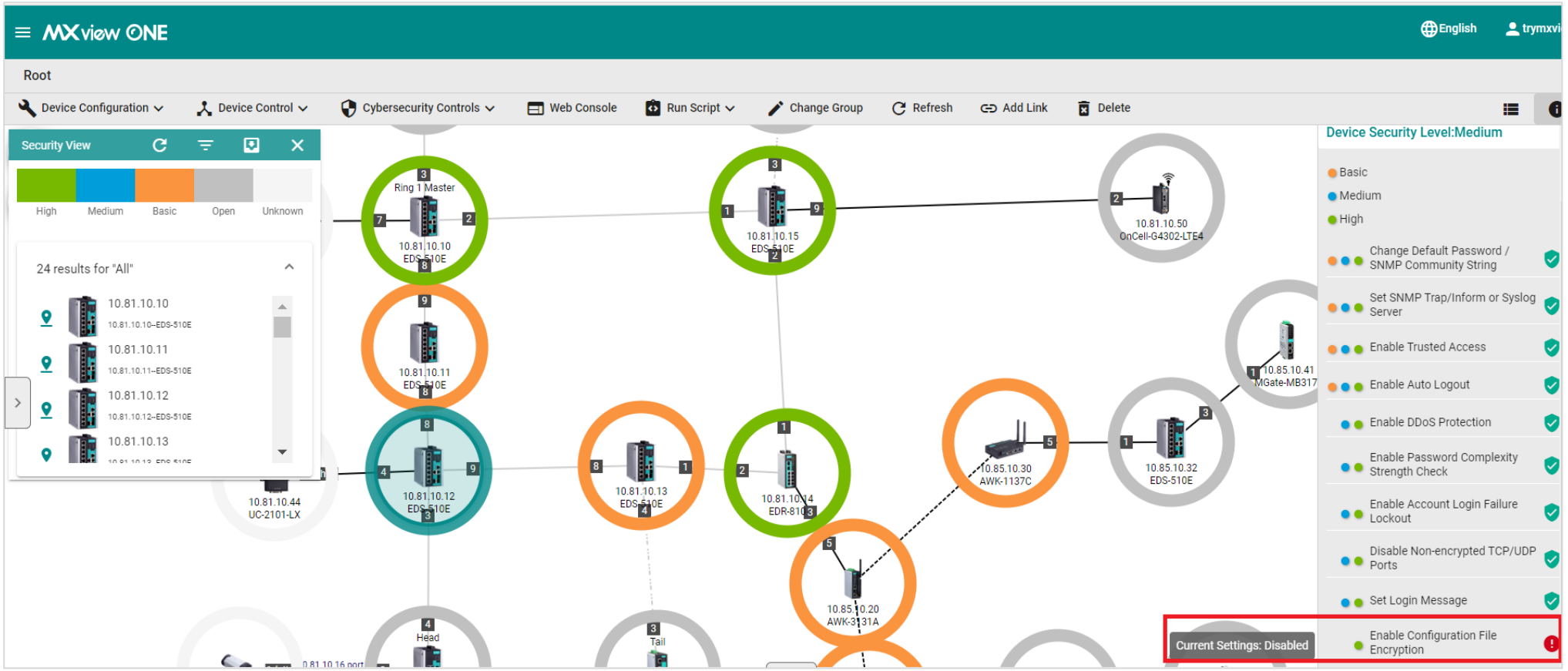
Współpraca z MxView One

- Oprogramowanie do monitoringu, diagnostyki i zarządzania przemysłową siecią Ethernet
- Zbieranie logów (serwer Syslog), trapów SNMP
- Alarmowanie (trapy SNMP, e-mail, Teams)
- Współpraca z urządzeniami innych producentów (SNMP, konieczny plik MIB)
- Zarządzanie urządzeniami (Import/Export konfiguracji, upgrade firmware, gwarancja)



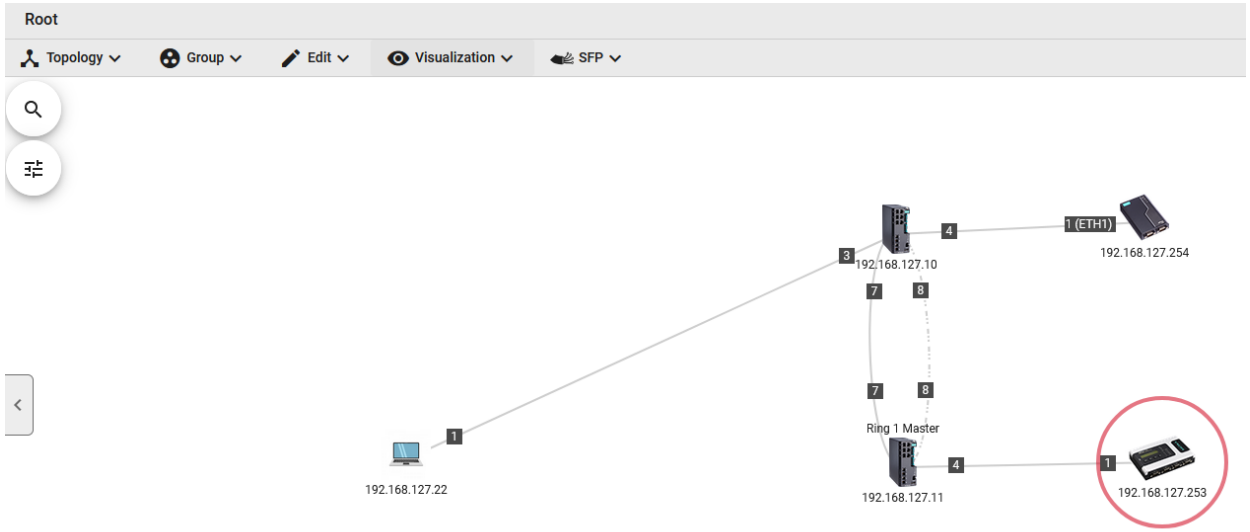
Security View (zgodność z IEC 62443-4-2)

- Sprawdza status zabezpieczeń poszczególnych urządzeń
- Dla wybranego urządzenia podaje informacje, które wytyczne IEC 62443-4-2 są spełnione, a które nie.



Szybka informacja o utracie połączenia

- Topology View, Event View



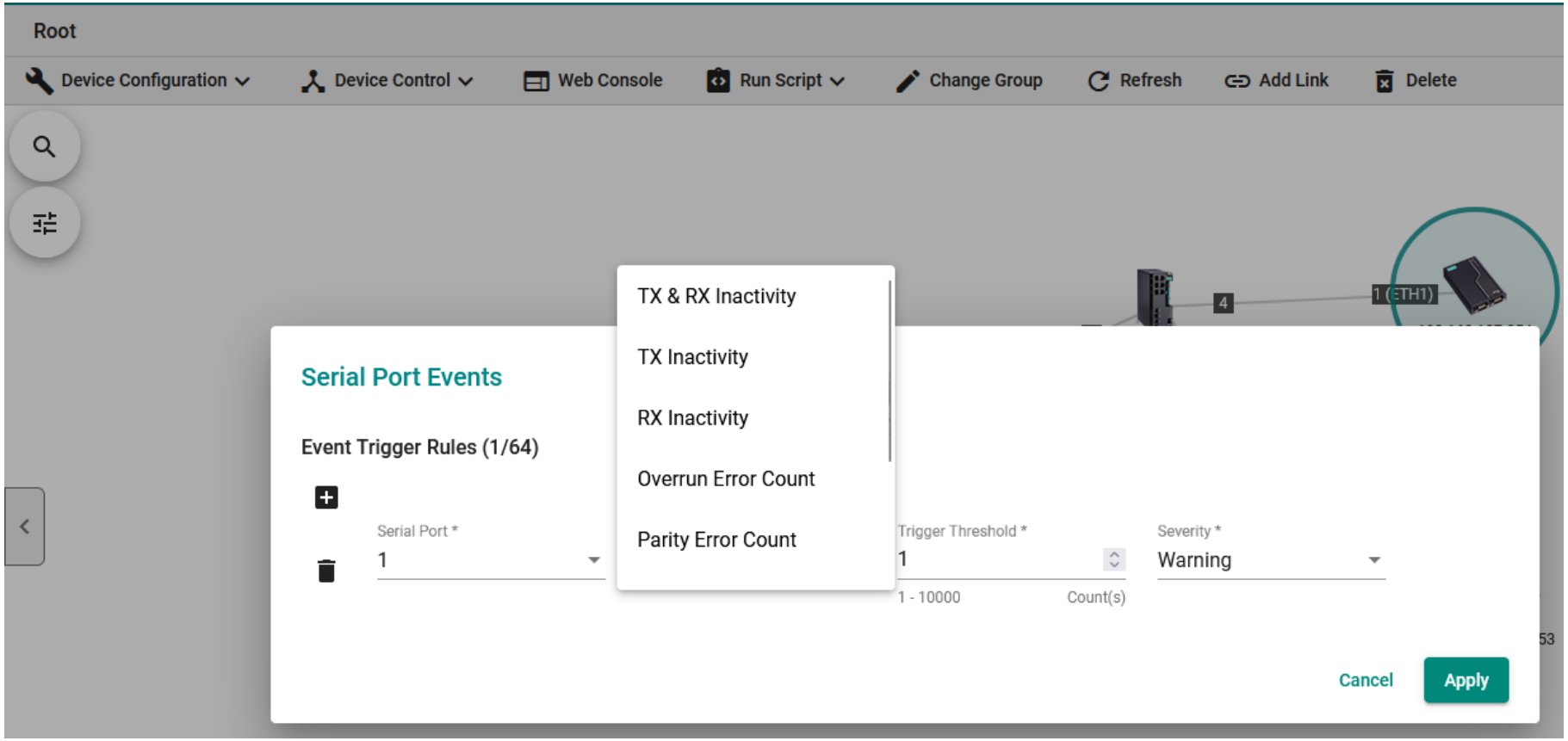
Event History

System | Network and Device

ID	Source	Source IP	Device Alias	Description	Time Issued
152	MXview One	192.168.127.11	192.168.127.11--EDS-4008-2MSC	Port 4 link up	2025-02-07 12:33:19
151	MXview One	192.168.127.253	192.168.127.253--NPort-6450	Device SNMP reachable	2025-02-07 12:32:55
150	MXview One	192.168.127.253	192.168.127.253--NPort-6450	Device ICMP reachable	2025-02-07 12:32:21
149	MXview One	192.168.127.11	192.168.127.11--EDS-4008-2MSC	Port 4 link down	2025-02-07 12:32:19
148	MXview One	192.168.127.253	192.168.127.253--NPort-6450	Device SNMP unreachable	2025-02-07 12:32:04
147	MXview One	192.168.127.253	192.168.127.253--NPort-6450	Device ICMP unreachable	2025-02-07 12:31:13
142	MXview One	192.168.127.11	192.168.127.11--EDS-4008-2MSC	Device SNMP reachable	2025-02-07 11:57:31
141	MXview One	192.168.127.11	192.168.127.11--EDS-4008-2MSC	Device ICMP reachable	2025-02-07 11:57:30
140	MXview One	192.168.127.10	192.168.127.10--EDS-4008-2MSC	Device SNMP reachable	2025-02-07 11:57:16
139	MXview One	192.168.127.10	192.168.127.10--EDS-4008-2MSC	Device ICMP reachable	2025-02-07 11:57:03
138	MXview One	192.168.127.254	192.168.127.254--NPort-6250-G2	Device ICMP reachable	2025-02-07 11:56:57
137	MXview	192.168.127.253	192.168.127.253--NPort-6450	Device ICMP reachable	2025-02-07 11:56:55

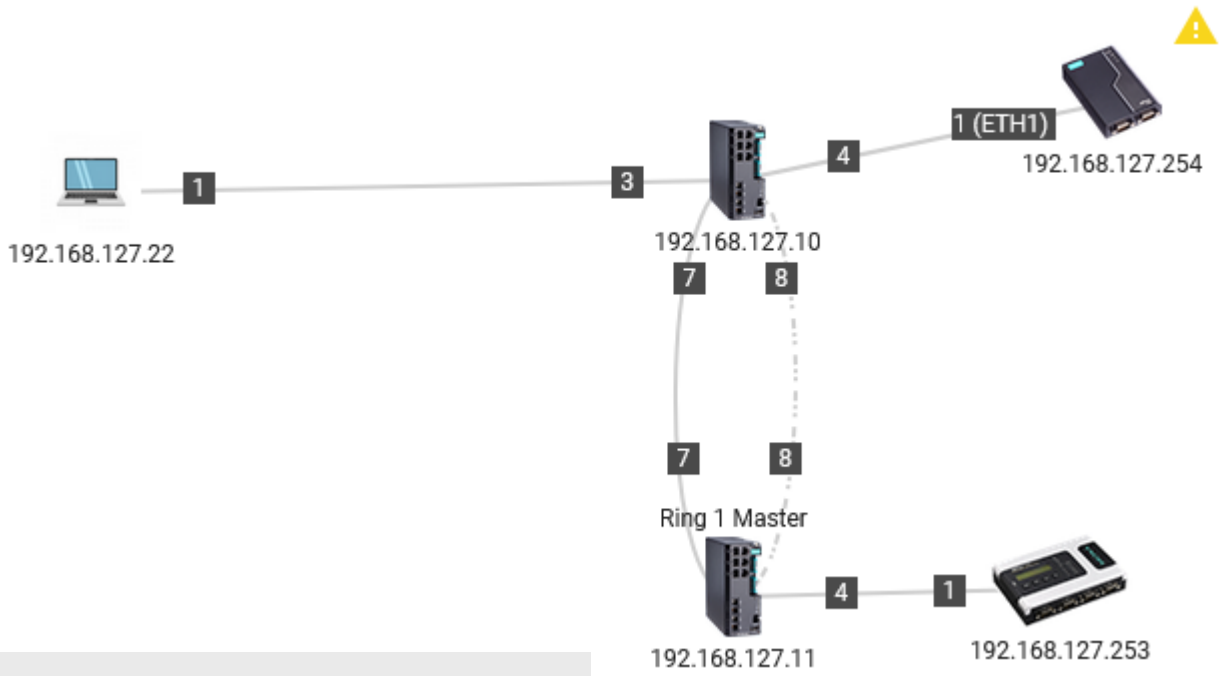
Serial Port Monitoring

- Monitorowanie aktywności interfejsu szeregowego



Serial Port Monitoring

- Monitorowanie aktywności interfejsu szeregowego

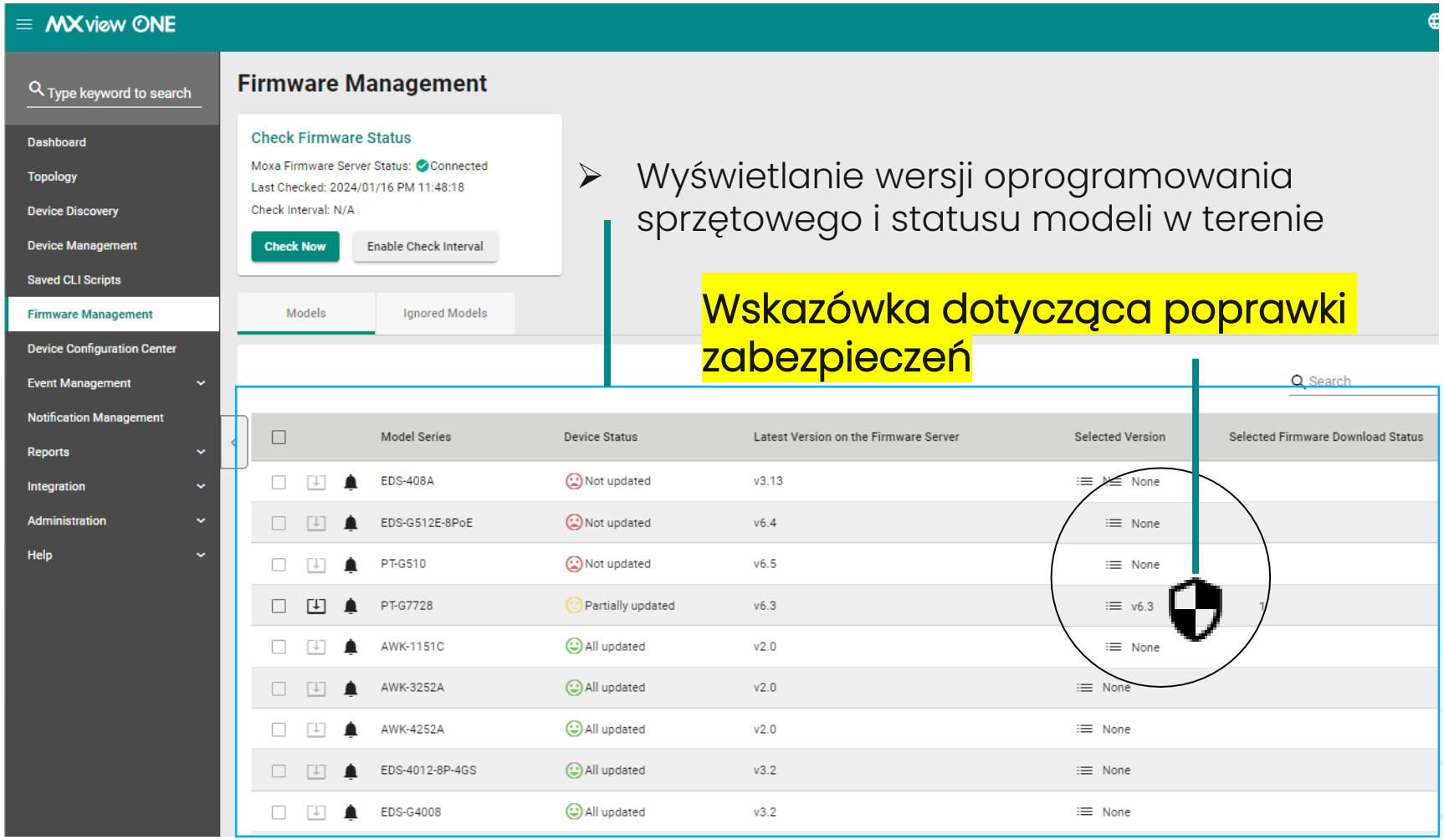


Event History

System | Network and Device

	ID	Source	Source IP	Device Alias	Description	Time Issued
	153	MXview One	192.168.127.254	192.168.127.254–NPort-6250-G2	The RX of serial port 1 did not receive any data in last 1 minute(s).	2025-02-07 12:44:00
	152	MXview One	192.168.127.11	192.168.127.11–EDS-4008-2MSC	Port 4 link up	2025-02-07 12:33:19
	151	MXview One	192.168.127.253	192.168.127.253–NPort-6450	Device SNMP reachable	2025-02-07 12:32:55

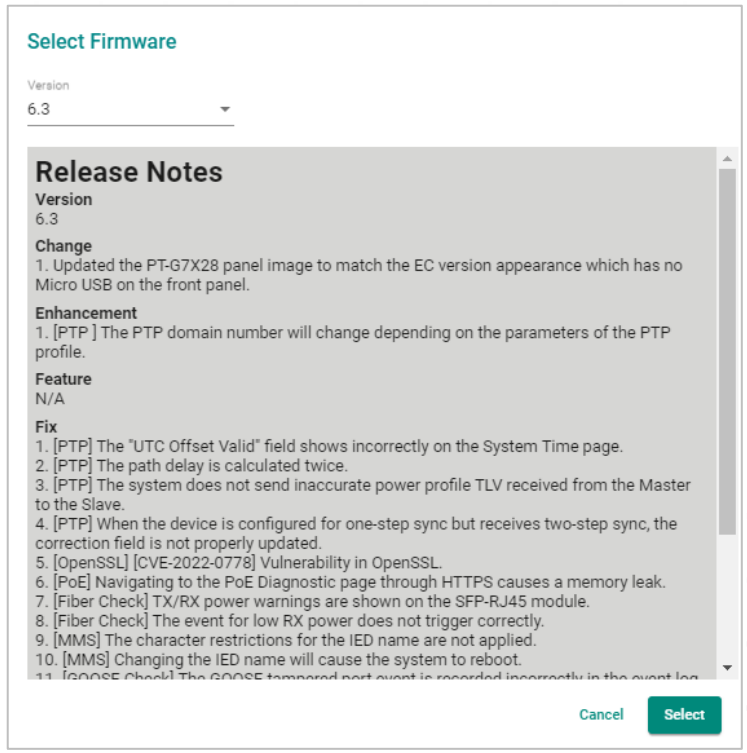
Firmware management



- Wyświetlanie wersji oprogramowania sprzętowego i statusu modeli w terenie

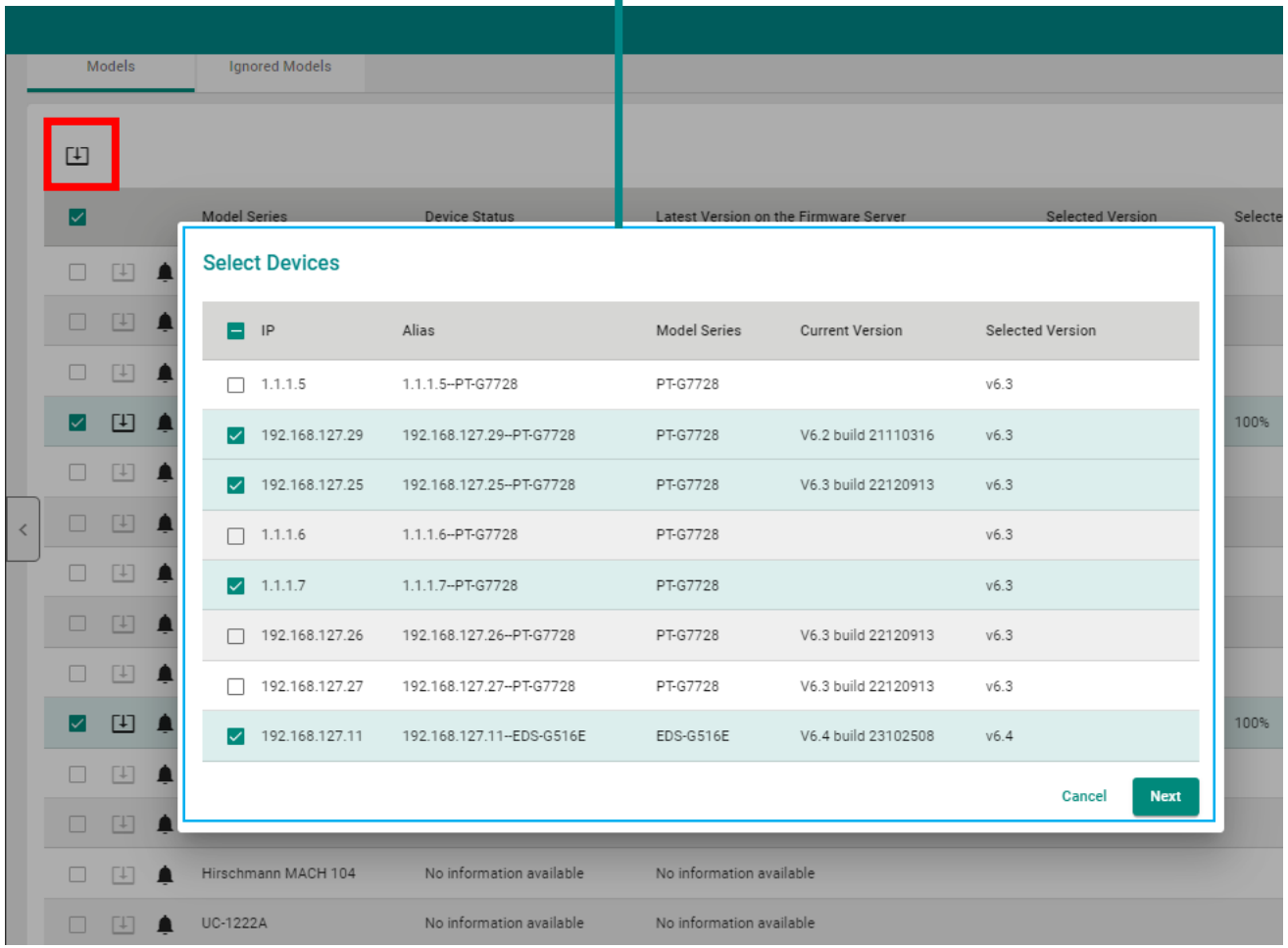
Wskazówka dotycząca poprawki zabezpieczeń

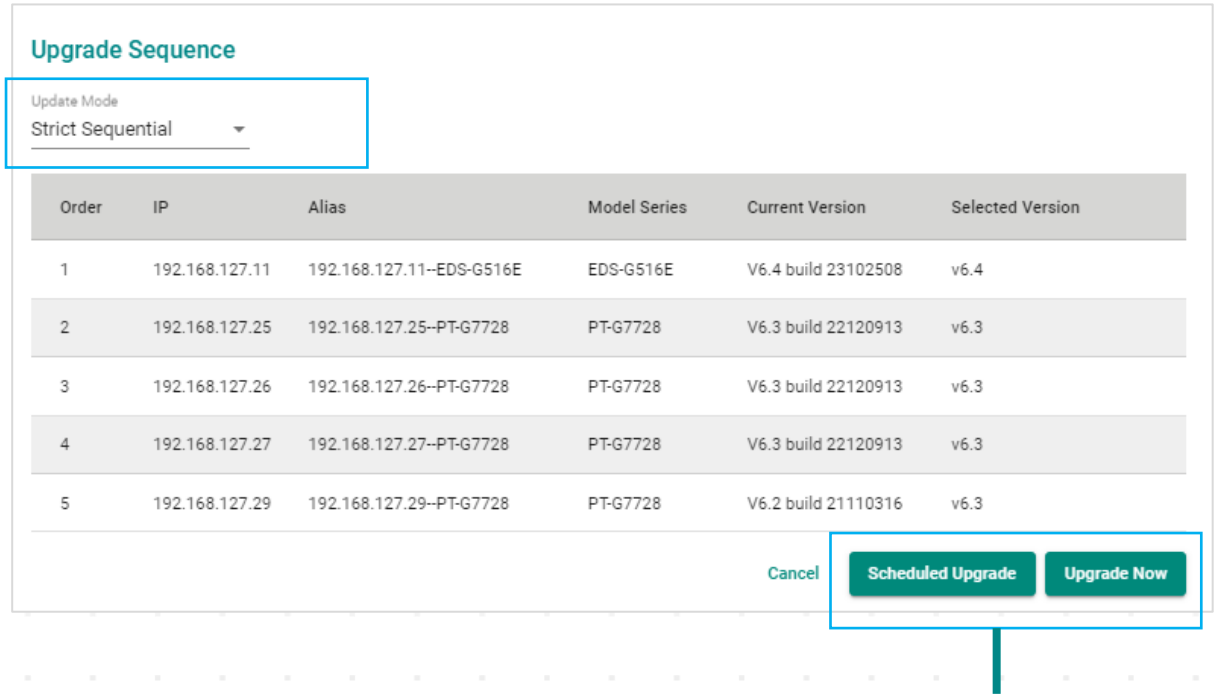
- Możliwość sprawdzenia Release Notes



Firmware management

- Wybierz urządzenia





- **Aktualizacja wg harmonogramu lub na żądanie**

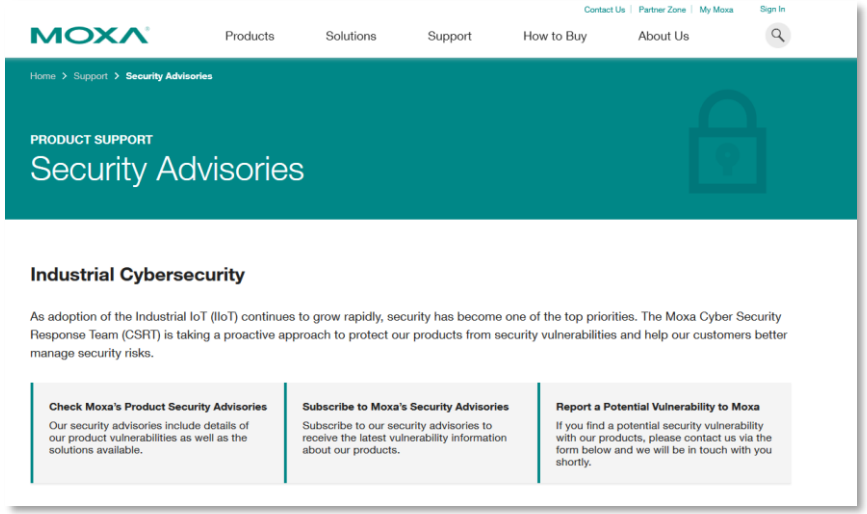
Moxa Product Security Advisory

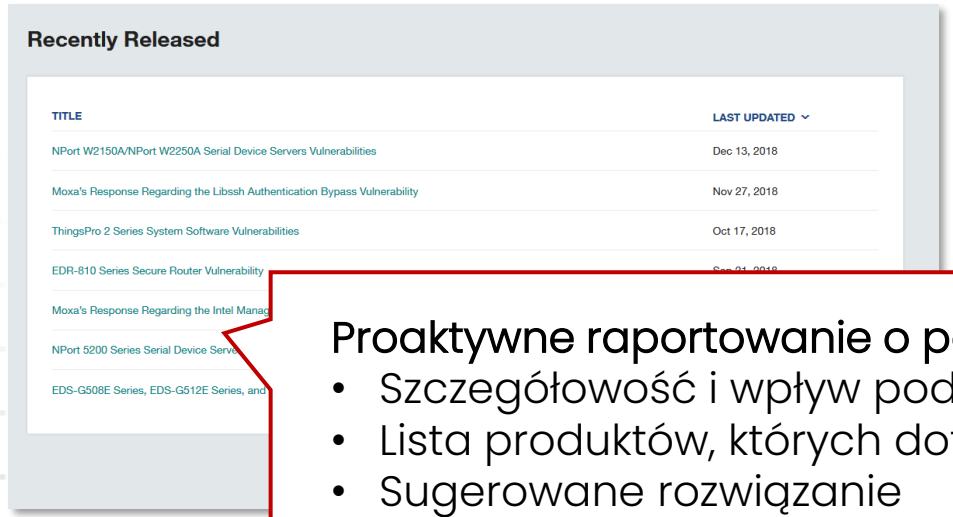
Publikacja ujawnionych podatności

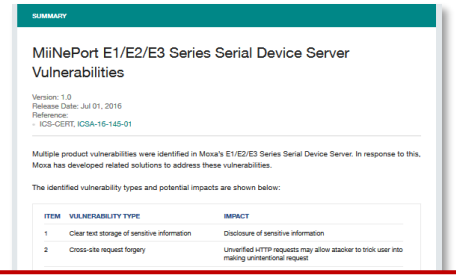
Możliwość subskrypcji kanału RSS z informacjami o najnowszych aktualizacjach i lukach

Raportowanie Podatności

https://www.moxa.com/en/support/product-support/security-advisory







Proaktywne raportowanie o podatnościach

- Szczegółowość i wpływ podatności
- Lista produktów, których dotyczy problem
- Sugerowane rozwiązanie

Szybkie rekomendacje

Poradniki – konfiguracja funkcji bezpieczeństwa


FAQ

Cybersecurity FAQ for Moxa Edge Devices

1. Introduction

While companies are tapping into the opportunities that the Industrial Internet of Things (IIoT) has to offer, digitalization has become a key initiative for industries. Digitalization has allowed the industrial control system (ICS) landscape to develop quickly in recent years. Originally, ICS networks were physically isolated and almost immune to cyberattacks. However, recently, there has been a rise in the sophistication of cyberattacks, which has prompted everyone from IT to OT personnel to produce solutions that enhance industrial cybersecurity. Thus, understanding industrial cybersecurity requirements will help companies mitigate cybersecurity risks. This FAQ collects the questions Moxa has been asked in past few years and also our responses to help the distributors, system integrators and customers to understand how Moxa products can help him to protect his network from cyberattacks.

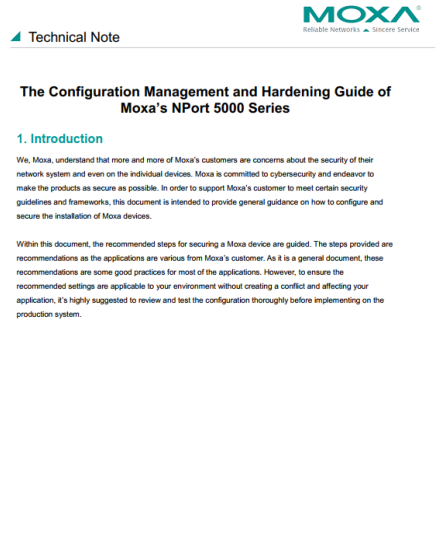
2. Frequently Asked Questions

2.1 Well-known Vulnerabilities Sharing

1. In October 2018, Apple, Google, Microsoft and Mozilla announced that they're going to disable the support of TLS v1.0/v1.1, will this affect the web consoles of Moxa devices?

The web consoles of Moxa devices will start to support TLS v1.2 by default after new firmware release end of 2020. The new firmware will also provide the ability to enable TLS v1.0/v1.1 (default disabled) to fulfill the users who are still using the old operation systems which may only support TLS v1.0/v1.1.

FAQ – najczęściej zadawane pytania


Technical Note

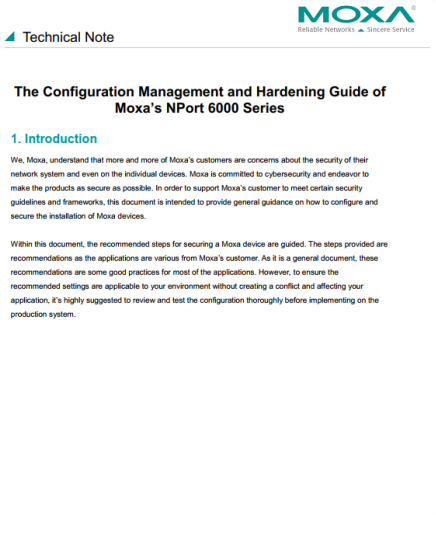
The Configuration Management and Hardening Guide of Moxa's NPort 5000 Series

1. Introduction

We, Moxa, understand that more and more of Moxa's customers are concerns about the security of their network system and even on the individual devices. Moxa is committed to cybersecurity and endeavor to make the products as secure as possible. In order to support Moxa's customer to meet certain security guidelines and frameworks, this document is intended to provide general guidance on how to configure and secure the installation of Moxa devices.

Within this document, the recommended steps for securing a Moxa device are guided. The steps provided are recommendations as the applications are various from Moxa's customer. As it is a general document, these recommendations are some good practices for most of the applications. However, to ensure the recommended settings are applicable to your environment without creating a conflict and affecting your application, it's highly suggested to review and test the configuration thoroughly before implementing on the production system.

NPort 5000


Technical Note

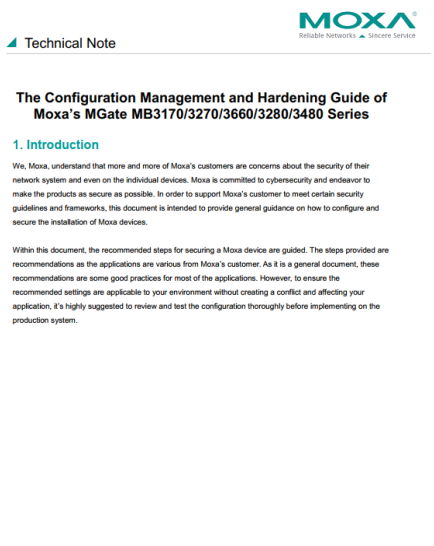
The Configuration Management and Hardening Guide of Moxa's NPort 6000 Series

1. Introduction

We, Moxa, understand that more and more of Moxa's customers are concerns about the security of their network system and even on the individual devices. Moxa is committed to cybersecurity and endeavor to make the products as secure as possible. In order to support Moxa's customer to meet certain security guidelines and frameworks, this document is intended to provide general guidance on how to configure and secure the installation of Moxa devices.

Within this document, the recommended steps for securing a Moxa device are guided. The steps provided are recommendations as the applications are various from Moxa's customer. As it is a general document, these recommendations are some good practices for most of the applications. However, to ensure the recommended settings are applicable to your environment without creating a conflict and affecting your application, it's highly suggested to review and test the configuration thoroughly before implementing on the production system.

NPort 6000


Technical Note

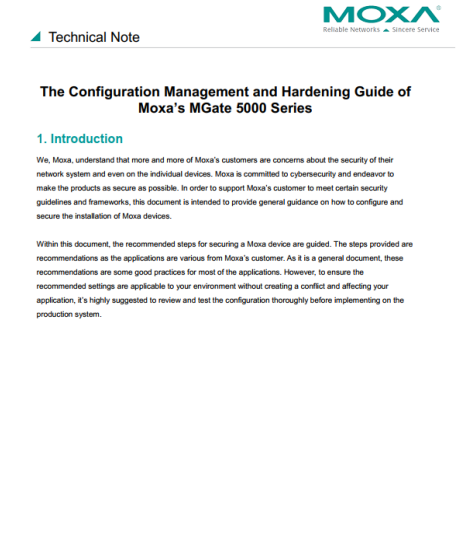
The Configuration Management and Hardening Guide of Moxa's MGate MB3170/3270/3660/3280/3480 Series

1. Introduction

We, Moxa, understand that more and more of Moxa's customers are concerns about the security of their network system and even on the individual devices. Moxa is committed to cybersecurity and endeavor to make the products as secure as possible. In order to support Moxa's customer to meet certain security guidelines and frameworks, this document is intended to provide general guidance on how to configure and secure the installation of Moxa devices.

Within this document, the recommended steps for securing a Moxa device are guided. The steps provided are recommendations as the applications are various from Moxa's customer. As it is a general document, these recommendations are some good practices for most of the applications. However, to ensure the recommended settings are applicable to your environment without creating a conflict and affecting your application, it's highly suggested to review and test the configuration thoroughly before implementing on the production system.

MGate MB3000


Technical Note

The Configuration Management and Hardening Guide of Moxa's MGate 5000 Series

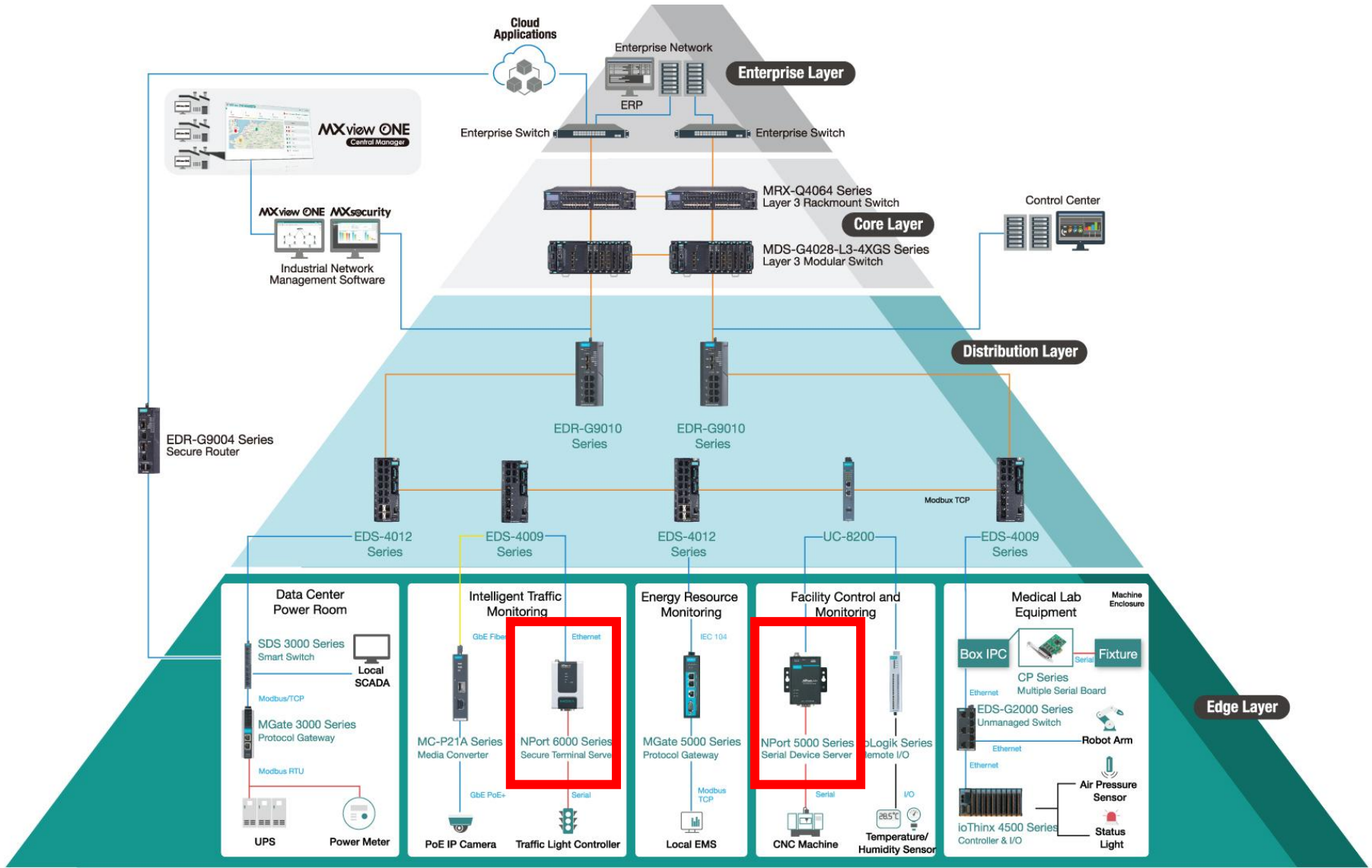
1. Introduction

We, Moxa, understand that more and more of Moxa's customers are concerns about the security of their network system and even on the individual devices. Moxa is committed to cybersecurity and endeavor to make the products as secure as possible. In order to support Moxa's customer to meet certain security guidelines and frameworks, this document is intended to provide general guidance on how to configure and secure the installation of Moxa devices.

Within this document, the recommended steps for securing a Moxa device are guided. The steps provided are recommendations as the applications are various from Moxa's customer. As it is a general document, these recommendations are some good practices for most of the applications. However, to ensure the recommended settings are applicable to your environment without creating a conflict and affecting your application, it's highly suggested to review and test the configuration thoroughly before implementing on the production system.

MGate 5000

Kompleksowe portfolio MOXA



Dziękuję za uwagę

Sprawdź:

www.elmark.com.pl