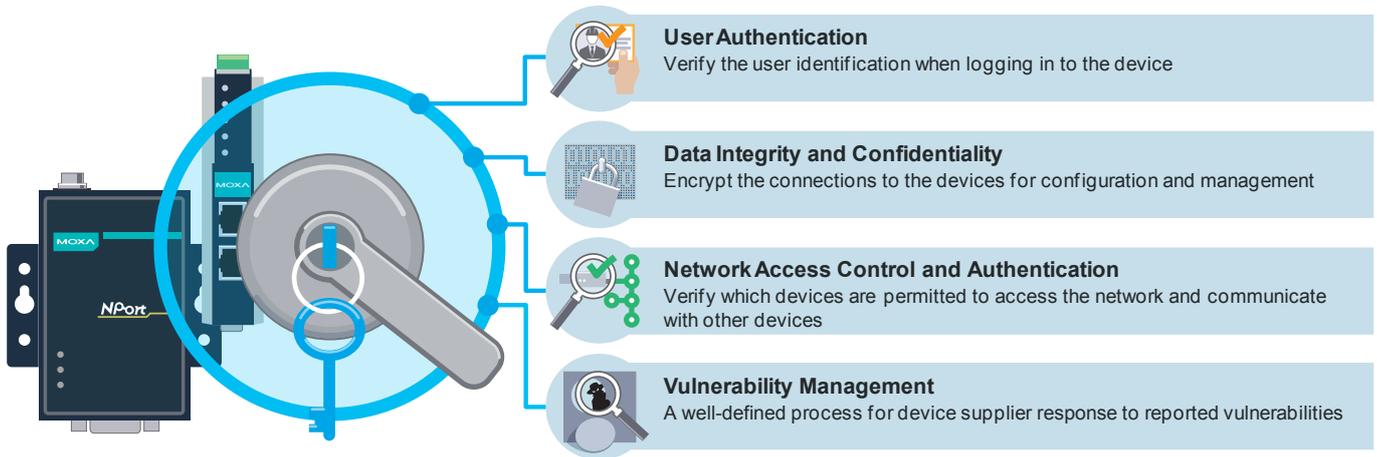


Checklist for Implementing Industrial Cybersecurity on Your Serial-to-Ethernet Devices

Serial-to-Ethernet devices are capable of remotely managing industrial edge devices, such as power meters, or factory equipment, such as CNC machines. As the Industrial Internet of Things (IIoT) has accelerated the adoption of IP-enabled industrial applications, the importance of information security is being stressed more than ever because systems are now all connected. Device security measures should include a number of built-in attributes and need to be implemented when serial-to-Ethernet devices are in operation.



To establish a solid foundation for network security, the following checklist lists security measures that you need to implement when configuring your serial-to-Ethernet devices.



User Authentication

- 1 Enable user/password protection**
Verifies the identity of a user
- 2 Enforce password complexity**
Enhances access control
- 3 Define User Level**
Only authorized personnel has the right to manage the system's administration

1

Username:

Password:

3

User Account

User Account

Active	Account Name	User Level
<input checked="" type="checkbox"/>	admin	Read Write
<input checked="" type="checkbox"/>	user	Read Write

2

Account Password and Login Management

Account Password Policy

Password minimum length: (4 - 16)

Password complexity strength check: Enable Disable

At least one digit (0~9): Enable Disable

Mixed upper and lower case letters (A~Z, a~z): Enable Disable

At least one special character (~!@#%&^*~_!;:.-<>[]{}()): Enable Disable

Password lifetime: (0 - 180 day; 0 for Disable)

Account Login Failure Lockout

Account login failure lockout: Enable Disable

Retry failure threshold: (1 - 10 retry)

Lockout Time: (1 - 60 min)



Data Integrity and Confidentiality

- 1 Turn down unused ports and services after device configuration has been done**
Allows secure connections (e.g., HTTPS) only
- 2 Encrypt configuration data**
To increase confidentiality
- 3 Encrypt serial data if it is considered to be confidential**
To ensure data integrity (This feature is now only supported by the NPort 6000 Series)

1 Console Settings

HTTP console Enable Disable

HTTPS console Enable Disable

Telnet console Enable Disable

Serial console Enable Disable

Moxa Service Enable Disable

Maximum Login Users For HTTP+HTTPS (1-6)

Auto Logout Setting (min) (1-1440)

Reset button protect No Yes

3 Cipher Settings

Port 1

Use up/down to sort the cipher list.

Secure Mode (SSL/TLS) Ciphers

ECDHE-ECDSA-AES256-GCM-SHA384
 ECDHE-RSA-AES256-GCM-SHA384
 ECDHE-ECDSA-AES128-GCM-SHA256
 ECDHE-RSA-AES128-GCM-SHA256
 ECDHE-ECDSA-AES256-SHA384
 ECDHE-RSA-AES256-SHA384
 ECDHE-ECDSA-AES128-SHA256
 ECDHE-RSA-AES128-SHA256

Up
Down

SSH/Reverse SSH Ciphers

aes128-cbc
 3des-cbc
 aes192-cbc
 aes256-cbc
 twofish256-cbc
 twofish-cbc
 twofish128-cbc
 blowfish-cbc

Up
Down

Apply the above settings to P1 P2
 All ports

Submit

2 Pre-shared Key

Pre-shared Key

Cipher key for encrypting the configuration file



Network Access Control and Authentication

- 1 Whitelist the IP addresses that have the right to access the system**
Verify authorized devices before they gain access to the network and communicate with other devices

1 Accessible IP List

- Activate the accessible IP list (Operation modes are NOT allowed for the IPs NOT on the list)
- Apply additional restrictions (All device services are NOT allowed for the IPs NOT on the list)

No.	Activate the rule	IP Address	Netmask
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
6	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
8	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>



Vulnerability Scan

- 1 Check and subscribe to vendors' security advisories to keep up to date on vulnerability fixes
- 2 Patch device firmware to ensure timely security protection

1

Contact Us | Partner Zone | My Moxa | Sign In

MOXA Products Solutions Support How to Buy About Us

Home > Support > Security Advisories

PRODUCT SUPPORT
Security Advisories



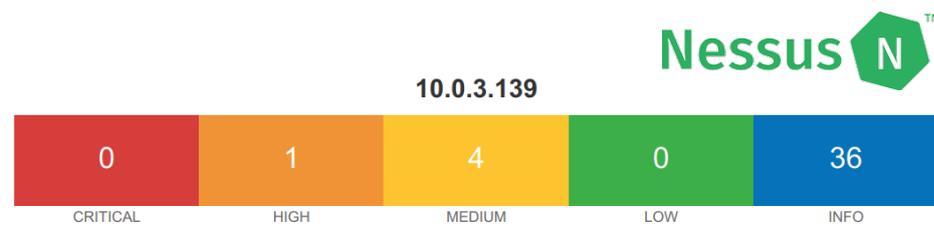
Industrial Cybersecurity

As adoption of the Industrial IoT (IIoT) continues to grow rapidly, security has become one of the top priorities. The Moxa Cyber Security Response Team (CSRT) is taking a proactive approach to protect our products from security vulnerabilities and help our customers better manage security risks.

<p>Check Moxa's Product Security Advisories</p> <p>Our security advisories include details of our product vulnerabilities as well as the solutions available.</p>	<p>Subscribe to Moxa's Security Advisories</p> <p>Subscribe to our security advisories to receive the latest vulnerability information about our products.</p>	<p>Report a Potential Vulnerability to Moxa</p> <p>If you find a potential security vulnerability with our products, please contact us via the form below and we will be in touch with you shortly.</p>
--	---	--

Moxa's serial-to-Ethernet devices actively scan for vulnerabilities periodically to check whether Moxa's devices are affected by any new vulnerabilities that require a remedy patch.

2



Vulnerabilities Total: 41

SEVERITY	CVSS	PLUGIN	NAME
HIGH	7.5	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported

It is not only the key components of a system that matters, but also the management process behind the running of the system. Therefore, securing the device first is a good start.

Choose Product Designs Based on IEC 62443-4-2 Standard

Choosing a product that eases your security concerns is essential. Our NPort and MGate Series of products have various security features that meet the IEC 62443 standard, keeping your devices safe and sound.

Product Category	Product Features Based on IEC 62443-4-2 Standard
Serial Device Servers	NPort 5100A Series 1-port RS-232/422/485 serial device servers
	NPort P5150A Series 1-port RS-232/422/485 PoE serial device servers
	NPort 5200A Series 2-port RS-232/422/485 serial device servers
	NPort 5400 Series 4-port RS-232/422/485 serial device servers
	NPort 5600 Series 8 and 16-port RS-232/422/485 rackmount serial device servers
	NPort 5600-DT Series 8-port RS-232/422/485 serial device servers
	NPort 5600-DTL Series 8-port RS-232/422/485 serial device servers
	NPort IA5000A Series 1, 2, and 4-port serial device servers for industrial automation
	NPort 5000AI-M12 Series Railway 1, 2, and 4-port RS-232/422/485 serial device servers
	NPort 6100/6200 Series 1/2-port RS-232/422/485 secure terminal servers
	NPort 6400/6600 Series 4/8/16/32-port RS-232/422/485 secure terminal servers
	NPort S9450I Series 4-port rugged device server with managed Ethernet switch
	NPort S9650I Series 8/16-port rugged device server with managed Ethernet switch
	Industrial Protocol Gateways
MGate MB3180/3280/3480 Series 1, 2, and 4-port standard serial-to-Ethernet Modbus gateways	
MGate MB3660 Series 8 and 16-port redundant Modbus gateways	
MGate 5101-PBM-MN Series 1-port PROFIBUS-to-Modbus TCP gateways	
MGate 5102-PBM-PN Series 1-port PROFIBUS-to-PROFINET gateways	
MGate 5103 Series 1-port Modbus RTU/ASCII/TCP/EtherNet/IP-to-PROFINET gateways	
MGate 5105-MB-EIP Series 1-port Modbus RTU/ASCII/TCP-to-EtherNet/IP gateways	
MGate 5109 Series 1-port Modbus RTU/ASCII/TCP-to-DNP3 serial/TCP/UDP gateways	
MGate 5111 Series 1-port Modbus/PROFINET/EtherNet/IP to PROFIBUS slave gateways	
MGate 5114 Series 1-port Modbus RTU/ASCII/TCP/IEC 101-to-IEC 104 gateways	
MGate 5118 Series 1-port CAN-J1939 to Modbus/PROFINET/EtherNet/IP gateways	
MGate W5108/W5208 Series 1 and 2-port IEEE 802.11a/b/g/n wireless Modbus/DNP3 gateways	