The Security Hardening Guide for the ioThinx 4510 Series

Moxa Technical Support Team <u>support@moxa.com</u>

Contents

1.	Introduction	2
2.	General System Information	3
2.1.	. Basic Information About the Device	3
2.2.	. Deployment of the Device	3
3.	Configuration and Hardening Information	4
3.1.	. TCP/UDP Ports and Recommended Services	5
3.2.	. HTTPS and SSL Certificates	7
3.3.	. Account Management	
3.4.	Access Control	9
3.5.	. Logging and Auditing	10
3.6.	. SNMPv3	10
3.7.	. SNMP Trap/Inform	11
3.8.	. MQTT over TLS	12
4.	Patching/Upgrades	13
4.1.	Patch Management Plan	13
4.2.	. Firmware Upgrades	13
5.	Security Information and Vulnerability Feedback	14

Copyright © 2021 Moxa Inc.

Released on March 26, 2021

About Moxa

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things (IIoT). With over 30 years of industry experience, Moxa has connected more than 57 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industries with reliable networks and sincere service. Information about Moxa's solutions is available at <u>www.moxa.com</u>.

How to Contact Moxa Tel: +886-2-8919-1230



The Security Hardening Guide for the ioThinx 4510 Series

1. Introduction

This document provides guidelines on how to configure and secure the ioThinx 4510 Series. The recommended steps in this document should be considered as best practices for security in most applications. It is highly recommended that you review and test the configurations thoroughly before implementing them in your production system in order to ensure that your application is not negatively impacted.

The Security Hardening Guide for the ioThinx 4510 Series

2. General System Information

2.1. Basic Information About the Device

Model	Function	Operating System	Firmware Version
ioThinx 4510 Series	Modular Remote I/O	Mbed OS	Version 1.2

The ioThinx 4510 Series is an advanced modular remote I/O product with a unique hardware and software design, making it an ideal solution for a variety of industrial data acquisition applications. The ioThinx 4510 Series has a unique mechanical design that reduces the amount of time required for installation and removal, simplifying deployment and maintenance. In addition, the ioThinx 4510 Series not only supports the Modbus RTU Master protocol for retrieving field-site data from serial meters, but also supports OT/IT protocol conversion.

2.2. Deployment of the Device

You should deploy the ioThinx 4510 Series behind a secure firewall network that has sufficient security features in place to ensure that your networks are safe from internal and external threats.

Make sure that the physical protection of the ioThinx 4510 Series devices and/or the system meets the security needs of your application. Depending on the environment and the threat situation, the form of protection can vary significantly.



The Security Hardening Guide for the ioThinx 4510 Series

3. Configuration and Hardening Information

For security reasons, account and password protection is enabled by default, so you must provide the correct account and password to unlock the device before entering the web console of the remote I/O.

The default account and password are **admin** and **moxa** (both in lowercase letters), respectively. Once you are successfully logged in, a pop-up notification will remind you to change the password to ensure a higher level of security.

ΜΟΧΛ	ioThinx 4510		Save & Restart Logout
Dashboard	System Information		
System	System mornation		
Security	ſ	a.	
Network	Madu		—
Module	Modu		Connection
Serial Port			
1/0	Device Name	ioThinx_4510	×
Internal Register	System Status	ОК	Exit Safe Mode
Protocol +	Status Description		Please change the default password in consideration of higher security level.
	Module Count	1	
	Firmware Version	V1.0.0_Build18112118	
	Serial Number	TAHLB1037728	
	LAN IP Address	192.168.127.254	
	LAN MAC Address	00:90:e8:76:2e:5f	
	System Date & Time	1970/01/01 00:00:31	
	System Elapsed Time	00:00:31	

The Security Hardening Guide for the ioThinx 4510 Series

3.1. TCP/UDP Ports and Recommended Services

The following table lists the ports, protocols, and services that are used to communicate between the ioThinx 4510 Series and other devices.

Service Name	Option	Default Setting	Туре	Port Number	Description
					The DHCP client needs to
DHCP client	Enable/Disable	Disable	UDP	68	acquire the system IP
					address from the server
HTTP server	Enable/Disable	Enable	ТСР	80	Web console
HTTPS server	Enable/Disable	Disable	ТСР	443	Secured web console
RESTful API	Enable/Disable	Disable	ТСР	80	RESTful API communication
RESTful API	Enable/Disable	Disable	ТСР	443	RESTful API communication
					over HTTPS
SNMP agent	Enable/Disable	Disable	UDP	161	SNMP handling routine
Modbus TCP	Enable/Disable	Enable	ТСР	502	Modbus communication
server					
Autosearch	Enable/Disable	Enable	UDP	4800	For Moxa utility
					communication
IOxpress/CLI	Enable/Disable	Enable	ТСР	10124	Sending the system logs to
(Moxa Utility)					the remote syslog server

For security reasons, you should consider disabling unused services. After initial setup, use services with stronger security for data communication. Refer to the table below for the suggested settings.

Service Name	Suggested Setting	Туре	Port Number	Security Remark
DHCP client	Disable	UDP	68	Assign an IP address manually for the
				device
HTTP server	Disable	ТСР	80	Disable HTTP to prevent plain text
				transmission
HTTPS server	Enable	ТСР	443	Encrypted data channel with trusted
				certificate for ioThinx configuration
RESTful API	Disable	ТСР	80	Disable to prevent plain text transmission
SNMP agent	Disable	UDP	161	Only enable this service if you use
				SNMPv3
Modbus TCP	Disable	ТСР	502	Use a more secure protocol for
server				communication
Autosearch	Disable	UDP	4800	Disable this service as it is not commonly
				used

I

The Security Hardening Guide for the ioThinx 4510 Series

To achieve the above suggested settings, follow the instructions below to configure the device:

• For the console services

НТТР	Disable
HTTPS	Enable
Moxa Command	Disable

Log in to the HTTP/HTTPS console and select **Security** \rightarrow **Service Settings**. Then, according to our suggestions, either enable or disable services.

	C	avian Cathing a	Lines Cattings	Annual California	Assess Control	Castifi	ante Cattinne
	56	Service Settings User Settings Account Settings Access Control					
	Service	Settings					
						_	_
		No.		Service		TCP/UDP	Port
		1	We	eb Service via HTTP		тср	80
Port	۵	Web Service via HTTPS MUST import the self-signed certificate before enabling the web service via https, or the browsers may block the connection				тср	443
ister	O	3	RESTful API via HTTP				80
+		4	RE	STful API via HTTPS		TCP	443
		5	SNM	1P Agent/Trap/Inform		UDP	161
		6	Ν	Nodbus/TCP Slave		TCP	502
		7	м	odbus/RTU Master		2	-
		8		MQTT Client		TCP	
		0	10			TODUDD	10104/4000

The Security Hardening Guide for the ioThinx 4510 Series

3.2. HTTPS and SSL Certificates

 HTTPS is an encrypted communication channel. As TLS v1.1 or lower has severe vulnerabilities that can easily be hacked, the ioThinx 4510 Series uses TLS v1.2 for HTTPS to ensure data transmissions are secured. Make sure your browser has TLS v1.2 enabled.

General	Security	Privacy	Content	Connections	Programs	Adva	ance
Setting	ps —						
	Enable Enable Enable Enable Enable Enable Enable Enable Use S Use T Use T	e DOM Sto e Enhance e Integrat e native X e Windows Do Not Tri SL 3.0 LS 1.0 LS 1.1	orage ed Protecte ed Window MLHTTP su s Defender ack reques	d Mode* Is Authenticatio pport SmartScreen Is to sites you	on* visit in Inter	net E	^
	V Use II Warn Warn Warn	about cer if changin if POST su	tificate ado g between ubmittal is r	dress mismatch secure and no edirected to a	* t secure mo zone that d	de oes n	
<	V Use II Warn Warn Warn	about cer if changin if POST su	tificate ado g between ubmittal is r	dress mismatch secure and no edirected to a	* t secure mo zone that d	de oes n	•
< *Ta	Warn Warn Warn Warn	about cer if changin if POST su after you	tificate add g between Jomittal is r restart you	ress mismatch secure and no edirected to a ur computer	* t secure mo zone that d	de oes n >	*
र *Ta	V Use II Warn Warn Warn	about cer if changin if POST su after you	tificate add g between ubmittal is r restart you	dress mismatch secure and no edirected to a ur computer Restore	* t secure mo zone that d	de oes n > setting	*
< *Ta Reset	Use II Warn Warn Warn Warn	about cer if changin if POST su after you	tificate add g between ubmittal is r restart you tings	dress mismatch secure and no edirected to a ur computer Restore	* t secure mo zone that d	de oes n > setting	> IS
< *Ta Reset Reset	Use II Warn Warn Warn Warn Internet Ex ets Interne Jition.	about cer if changin if POST su after you plorer set t Explorer	tificate add g between Jomittal is r restart you tings	ress mismatch secure and no edirected to a r computer Restore to their default	* t secure mo zone that d advanced s	de oes n > setting et	× ∣s

When using a web service via HTTPS, you must import the self-signed certificate before using the web service via HTTPS, or the browser may block the connection.

• Log in to the HTTP/HTTPS console and select **Security** → **Certificate Settings**.



Note: The HTTPS console is designed for configuration purposes. Because of device limitations, other services cannot operate in parallel with HTTPS.

Behavior of the SSL certificate on an ioThinx device

The ioThinx Series devices generate an SSL self-signed certificate automatically. Along with the self-signed certificate, you need to establish a local certificate server and import the certificate from the ioThinx Series.

The Security Hardening Guide for the ioThinx 4510 Series

3.3. Account Management

- The ioThinx 4510 Series provides three different user levels: administrator, operator, and user. With an administrator account, you can access and modify all the settings through the web console. With an operator account, you can access and modify the I/O status. With a user account, you can only view the dashboard.
- The default administrator account is admin, with the default password moxa. To manage accounts, log in to the web console and select Security -> User Settings. To change the password of an existing account, enter the existing account's username and then enter a new password.

shboard	Service Settings		User Settings		Account Settings	Access Control
stem ecurity	User Settings					
twork	No.	Туре	Username	e e	Permiss	ions
odule	1	Administrator	admin		Full co	itrol
nai Port	2	Operator	operator		Dashboard and I/O	I status change
emal Register	3	User	user		Dashbo	ard
tocol +		Туре	Administrator			
		Enable	v			
		New Username			Must be 1-30 characters. Cannot include numbers, and symbols are allowed.	spaces, but letters,
		Admin Password				
		New Password			Must be 4-16 characters. Letters, numbe	rs, and symbols are

- To avoid brute-force attacks, the ioThinx 4510 Series has a built-in failure lockout feature. To configure it, log in to the HTTP/HTTPS console and select Security->Account Settings.
- For security requirements, a warning banner needs to be displayed to all users who want access to the device. Log in to the HTTP/HTTPS console and select Security->Account Settings to type in the warning message in the System Use Notification field.

NOX/	10111111 4010				ourceriestari Eugo
Dashboard	Service Settings User Setting	s A	ccount Settings	Access Control	Certificate Settings
System					The second second second second
Security	Account Setungs				
Network	Idle Timeout (Unit: min(s))	5			
Module	Retry Failure Threshold (Unit: time(s))	5			
Serial Port		10000 (10000			
/0	Lockout Time (Unit: min(s))	5			
nternal Register	System Log	Export	(max: 4000 records)		
Protocol +	Login Failure Message	Login Failed.			
	System Use Notification				

Moxa Tech Note The Security Hardening Guide for the ioThinx 4510 Series

3.4. Access Control

The ioThinx 4510 Series can limit access to specific host IP addresses to prevent unauthorized access to the ioThinx 4510. If a host's IP address is in the Access Control list, then the host will be allowed to access the ioThinx 4510 device. To configure it, log in to the HTTP/HTTPS console and select **Security** \rightarrow **Access Control**.

MOXA	ioThinx 451	10		Save & Restart Lo
Dashboaril	Servi	ce Settings	User Settings	Account Settings Access Control
ystem Security	Access Cont	rol		
ctwork	Warning	Note: Only allow b	elow IP address to access this device	
lodule erial Port		No.	IP Address	Netmask
o		1	0 . 0 . 0 . 0	255 .255 .255 . 0
nemal Register		2	0 . 0 . 0 . 0	255 .255 .255 . 0
rotacol +.		з	0 _ 0 _ 0 _ 0	255 255 255 0
		4	0 . 0 . 0 . 0	255 , 255 , 255 , 0
		5	0 , 0 _ 0 , 0	255 .255 .255 . 0
	6	6	0 , 0 _ 0 , 0	255 255 255 0
		7	0 . 0 . 0 . 0	255 255 255 . 0
		8	0 , 0 _ 0 _ 0	255 255 255 0

You may add a specific address or range of addresses by using a combination of an IP address and a netmask as follows:

To allow access to a specific IP address: Enter the IP address in the corresponding field; enter 255.255.255.255 for the netmask.

To allow access to hosts on a specific subnet: For both the IP address and netmask, use 0 for the last digit (e.g., "192.168.1.0" and "255.255.255.0").

Additional configuration examples are shown in the following table:

Desired IP Range	IP Address Field	Netmask Field
192.168.1.120	192.168.1.120	255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0	255.255.255.0
192.168.1.1 to 192.168.255.254	192.168.0.0	255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0	255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128	255.255.255.128

Warning Ensure the communication peer is listed in the accessible IP list for entering the web console.

Moxa Tech Note The Security Hardening Guide for the ioThinx 4510 Series

3.5. Logging and Auditing

 To review the system log from the ioThinx 4510, log in to the HTTP/HTTPS console and select Security → Account Setting. Click the Export button next to System Log to download it.

MOXA io	Thinx 4510					Save & Restart Logo
Dashboard	Service Settings	User Settings	Acc	ount Settings	Access Control	Certificate Settings
System	Account Settings					THE R. LEWIS CO., NAME
Security	Account Serongs					
Network	Idle Timeout	(Unit: min(s))	5			
vlodule	Retry Failure Threshold (Unit: time(s))	5			
Serial Port	Lockout Time	(Unit: min(s))	5			
nternal Register	S	ystem Log	Export	(max: 4000 records)		
Protocol +	Login Failure	e Message	Login Failed.			
	System Use N	lotification				

3.6. SNMPv3

 SNMP is a widely used protocol in IT environments and network management software (NMS). However, SNMPv1 and SNMPv2c are not secure protocols because they don't encrypt data. To limit SNMP access to SNMPv3, which is more secure, select Protocol → SNMP, and choose v3 only in the version dropdown list.

shboard	SNMP	SNMP Trap/Inform	Event Settings
item	SNMP Settings		
urity			
work	Service Enabled N	lote: enable/disable this service through <u>S</u>	Security Service Settings
dule	Version	v1 and v2c and v3	\$
al Port	Contact		
	Contact		
ernal Register	Location		
tocol -			
Aodbus	SNMPv1, SNMPv2c Set	ttings	
SNMP	Read Community	public	
ттри			
	Write Community	private	

Moxa Tech Note The Security Hardening Guide for the ioThinx 4510 Series

 You need to set the authentication method and privacy protocol for SNMPv3. To ensure the security level, use SHA-256 for Authentication Protocol and AES-128 for Privacy Protocol.

Username	v3ro	
Authentication Protocol	MD5	•
Authentication Password		
Privacy Protocol	CBC-DES	•
Privacy Password		
Privacy Password		
Privacy Password Pv3 Settings – Read/Write Username	v3rw	
Privacy Password Pv3 Settings - Read/Write Username Authentication Protocol	v3rw MD5	
Privacy Password Pv3 Settings – Read/Write Username Authentication Protocol Authentication Password	v3rw MD5	
Privacy Password Pv3 Settings – Read/Write Username Authentication Protocol Authentication Password Privacy Protocol	v3rw MD5 CBC-DES	

3.7. SNMP Trap/Inform

 SNMPv3 Trap/Inform provides secure notification of events. To set up SNMPv3 Trap/Inform, select Protocol → SNMP → SNMP Trap/Inform. Use SHA-256 for the Authentication Protocol and AES-128 for the Privacy Protocol.

SNMPv3			
1st Server Username	v3	2nd Server Username	v3
1st Server Authentication Protocol	MD5 \$	2nd Server Authentication Protocol	MD5 \$
1st Server Authentication Password		2nd Server Authentication Password	******
1st Server Privacy Protocol	CBC-DES \$	2nd Server Privacy Protocol	CBC-DES \$
1st Server Privacy Password		2nd Server Privacy Password	
1st Server Engine ID Format	ASCII \$	2nd Server Engine ID Format	ASCII \$
1st Server Engine ID	тоха-123	2nd Server Engine ID	moxa-123

3.8. MQTT over TLS

MQTT is a lightweight, open, simple, and easily implemented protocol, but it is not secure unless it is encrypted using TLS. To enable MQTT over TLS, select Protocol
MQTT. Choose Enable from the dropdown list under TLS. Ensure the broker supports ECDHE-ECDSA-AES128-SHA256 or ECDHE-ECDSA-AES128-GCM-SHA256 cipher suite.

MOXA	ioThinx 4510				Save & Restart Lopout
Dashboard	Correction Settings			Topic Settings	
System			and the second se		
Socurity	Connection Settings				
Network	Service Disabled				
Module	NOCE, IN ADDRESS AND THE SERVICE THOUGH SECURITY SERVICE SECURITY				
Serial Port	Broker IP				
vo	192.168.127.200				
Internal Register	Broker Port		Device ID		
Protocol -	1883		moxa_io_0090e8eb3214		
Modzias	Keep Alive Interval (Unit: sec)				
SNMP	60				
MQTT	Retry Period (Unit: sec)				
	30				
	TLS				
	Disable	٥			
	Authentication				
	User		Paseword		
	Advanced				

4. Patching/Upgrades

4.1. Patch Management Plan

With regards to the patch management, Moxa releases version enhancements with thorough release notes annually.

4.2. Firmware Upgrades

The process for upgrading firmware is as follows:

- Download the latest firmware for the ioThinx 4510 Series from the Moxa website: <u>https://www.moxa.com/en/products/industrial-edge-connectivity/controllers-and-ios/advanced-controllers-and-i-os/iothinx-4510-series#resources</u>
- Log in to the HTTP/HTTPS console and select System -> Firmware. Click the Browse button to select the proper firmware and click Update to upgrade the firmware.

lashboard	Device Settings	Time Settings	Watchdog	Configuration	Firmware
System	The states			Statement of the local division of the local	
ecurity	Firmware				
etwork		Firmware	Browse	Please select a firmware file.	
lodule	ι	Jpdate to Device*	Update		
erial Port	*DO NOT DISCONNECT	POWER OR NETWORK CA	BLE during the update pro	cess!	
temal Register otocol +	*Do not cancel the upda	ate process after clicking t	he "Update" button.		
	*Backup configuration	file before undating device	firmware		

The Security Hardening Guide for the ioThinx 4510 Series

• If you want to upgrade the firmware for multiple units, then use the IOxpress Configuration Utility for the GUI interface, or the Moxa CLI Configuration Tool for the CLI interface.

NAME		TYPE		OPERATING SYSTEM	RELEASE DATE ❤
MIB file for ioThinx 4510 Series 40.3 KB	⊥	Software Package	v1.2.0	-	Oct 31, 2019 Release notes
Firmware for ioThinx 4510 Series 2.0 MB	⊥	Firmware	v1.2.0	-	Oct 31, 2019 Release notes
Moxa CLI Configuration Tool for Linux 8.1 MB	⊥	Utility	v1.1.0	- Linux Kernel 2.6.x - Linux Kernel 3.x - Linux Kernel 4.x	Jun 24, 2019 Release notes
Moxa CLI Configuration Tool for Windows 1.4 MB	↓	Utility	v1.1.0	- Windows 10 - Windows 7 - Windows 8 Show More	Jun 24, 2019 Release notes
Library for ioThinx 4510 Series (Linux Kernel 4.x MXIO) 2.4 MB	⊥	Library	v3.0.0	- Linux Kernel 4.x	Jun 10, 2019 Release notes
Library for ioThinx 4510 Series (Windows MXIO) 2.7 MB	↓	Library	v3.0.0	- Windows 10 - Windows 7 - Windows 8.1 Show More	Jun 10, 2019 Release notes
IOxpress Configuration Utility 5.0 MB	Ţ	Utility	v2.4.0	- Windows 10 - Windows 7 - Windows 8 Show More	Jun 05, 2019 Release notes

5. Security Information and Vulnerability Feedback

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

You can find the latest Moxa security information here: https://www.moxa.com/en/support/product-support/security-advisory