The Security Hardening Guide for the ioThinx 4510 Series

Moxa Technical Support Team
support@moxa.com

Contents

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 www.moxa.com.

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

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.

Copyright © 2021 Moxa Inc.

2. General System Information

2.1. Basic Information About the Device

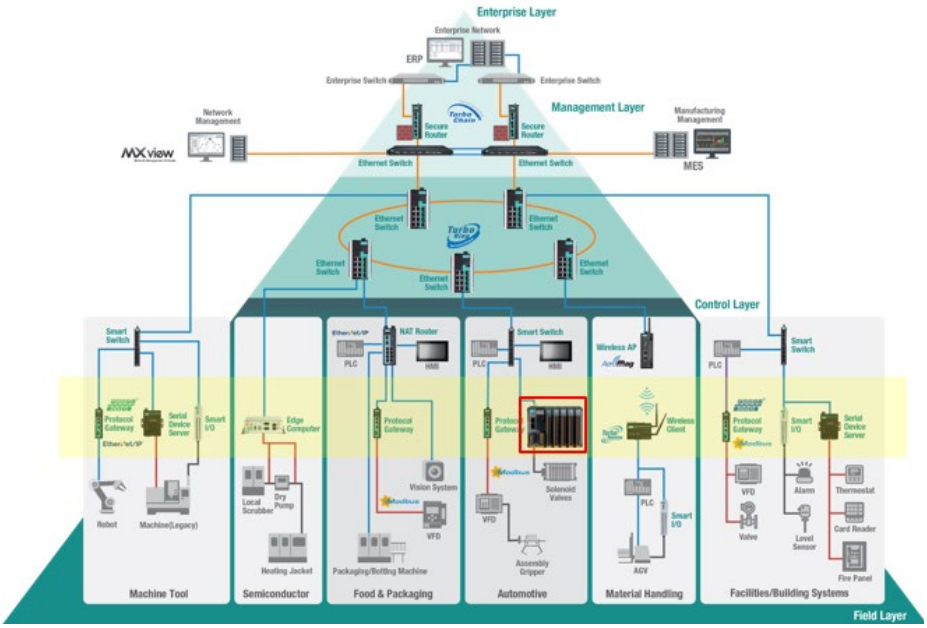
Model	Function	Operating System	Firmware Version
ioThinx 4510 Series	Modular Remote I/O	Mbed OS	Version 1.2

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.

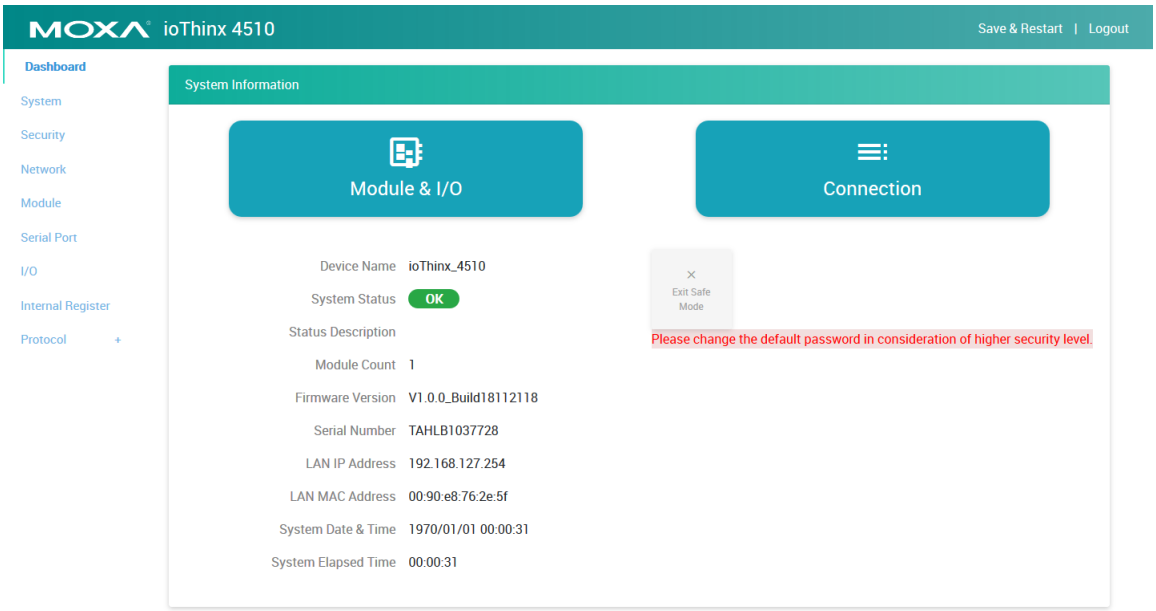
Make sure that the physical protection of the ioThinx 4510 Series devices and/or the system meets the security needs of your application. Depending on the environment and the threat situation, the form of protection can vary significantly.



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.



Copyright © 2021 Moxa Inc.

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	Type	Port Number	Description
DHCP client	Enable/Disable	Disable	UDP	68	The DHCP client needs to acquire the system IP address from the server
HTTP server	Enable/Disable	Enable	TCP	80	Web console
HTTPS server	Enable/Disable	Disable	TCP	443	Secured web console
RESTful API	Enable/Disable	Disable	TCP	80	RESTful API communication
RESTful API	Enable/Disable	Disable	TCP	443	RESTful API communication over HTTPS
SNMP agent	Enable/Disable	Disable	UDP	161	SNMP handling routine
Modbus TCP server	Enable/Disable	Enable	TCP	502	Modbus communication
Autosearch	Enable/Disable	Enable	UDP	4800	For Moxa utility communication
IOxpress/CLI (Moxa Utility)	Enable/Disable	Enable	TCP	10124	Sending the system logs to 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	Type	Port Number	Security Remark
DHCP client	**Disable**	UDP	68	Assign an IP address manually for the device
HTTP server	**Disable**	TCP	80	Disable HTTP to prevent plain text transmission
HTTPS server	**Enable**	TCP	443	Encrypted data channel with trusted certificate for ioThinx configuration
RESTful API	**Disable**	TCP	80	Disable to prevent plain text transmission
SNMP agent	**Disable**	UDP	161	Only enable this service if you use **SNMPv3**
Modbus TCP server	**Disable**	TCP	502	Use a more secure protocol for communication
Autosearch	**Disable**	UDP	4800	Disable this service as it is not commonly used

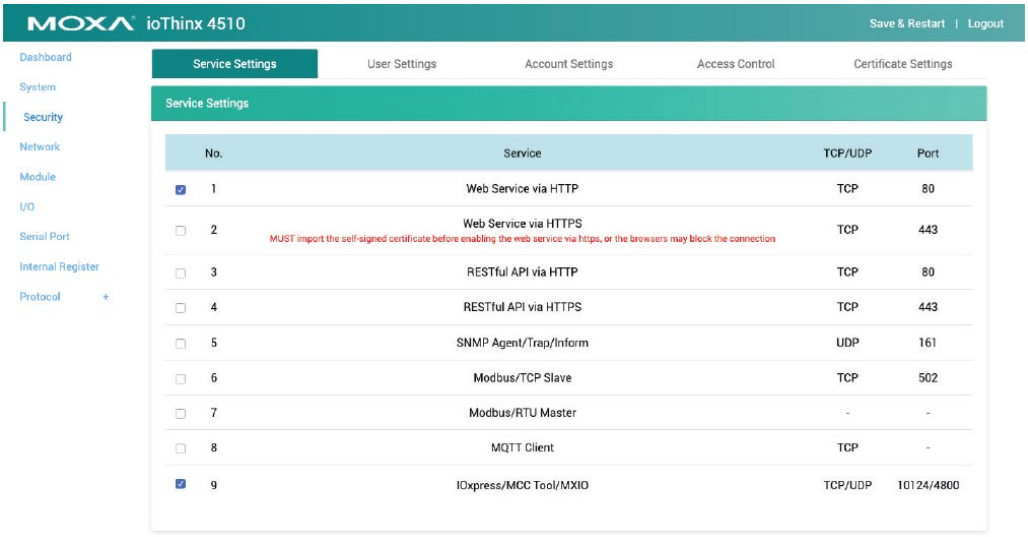
Copyright © 2021 Moxa Inc.

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

- For the console services

HTTP	Disable
HTTPS	Enable
Moxa Command	Disable

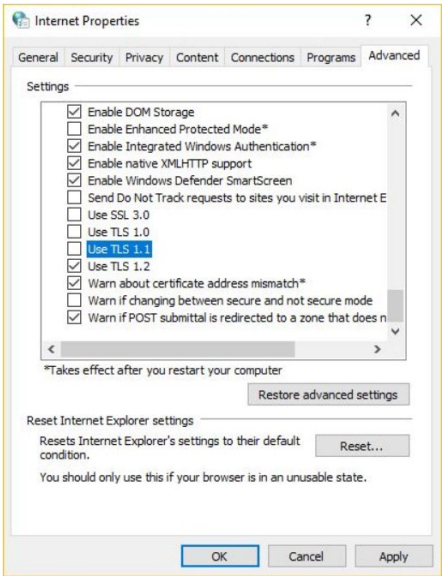
Log in to the HTTP/HTTPS console and select **Security → Service Settings**. Then, according to our suggestions, either enable or disable services.



Copyright © 2021 Moxa Inc.

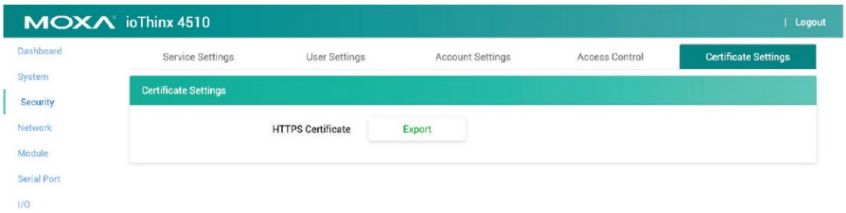
3.2. HTTPS and SSL Certificates

- 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.



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.

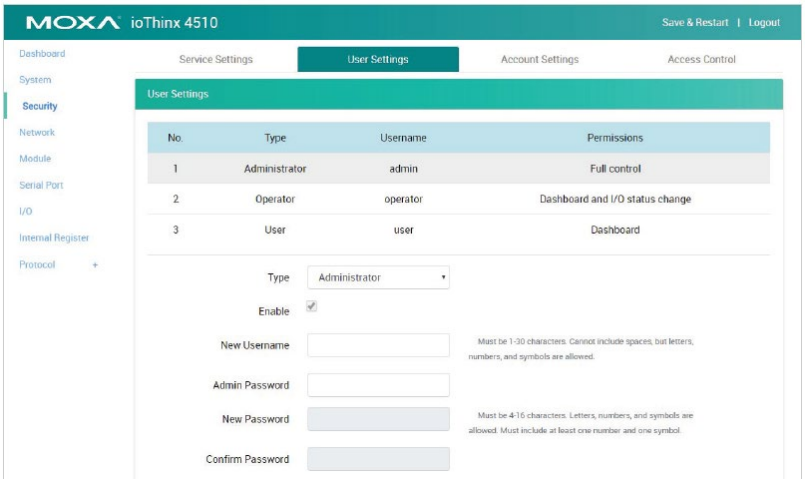
Behavior of the SSL certificate on an ioThinx device

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.

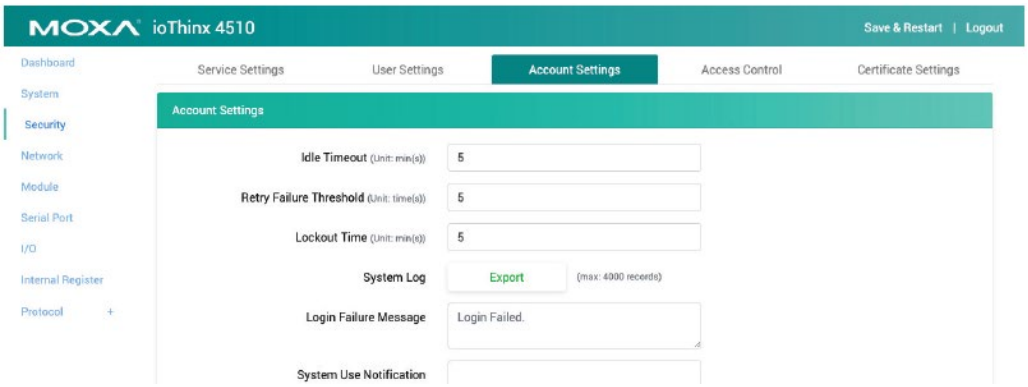
Copyright © 2021 Moxa Inc.

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.

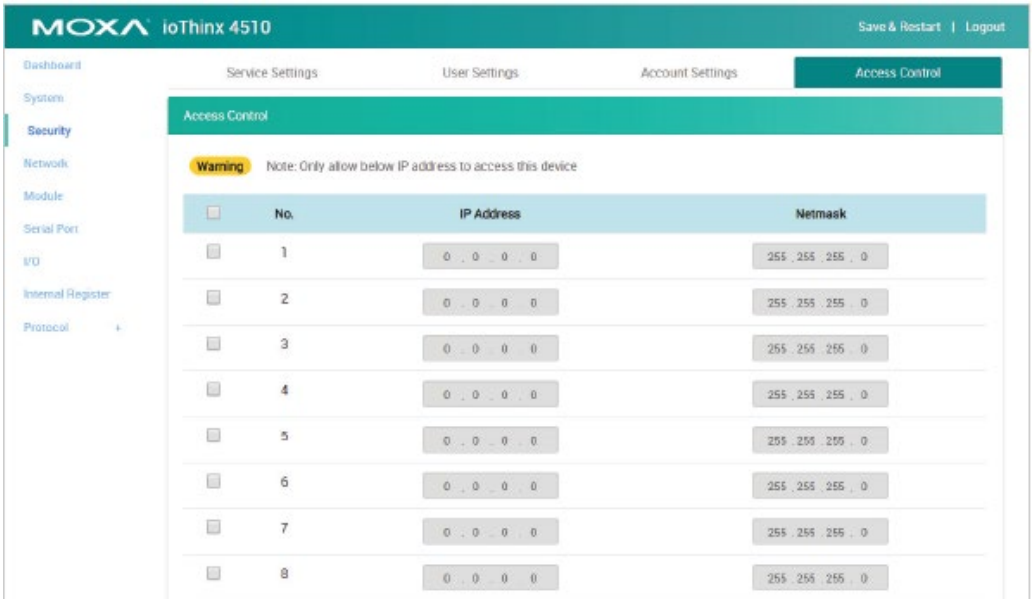


- To avoid brute-force attacks, the ioThinx 4510 Series has a built-in failure lockout feature. To configure it, log in to the HTTP/HTTPS console and select **Security->Account Settings**.
- For security requirements, a warning banner needs to be displayed to all users who want access to the device.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



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 → Access Control.**



.

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:

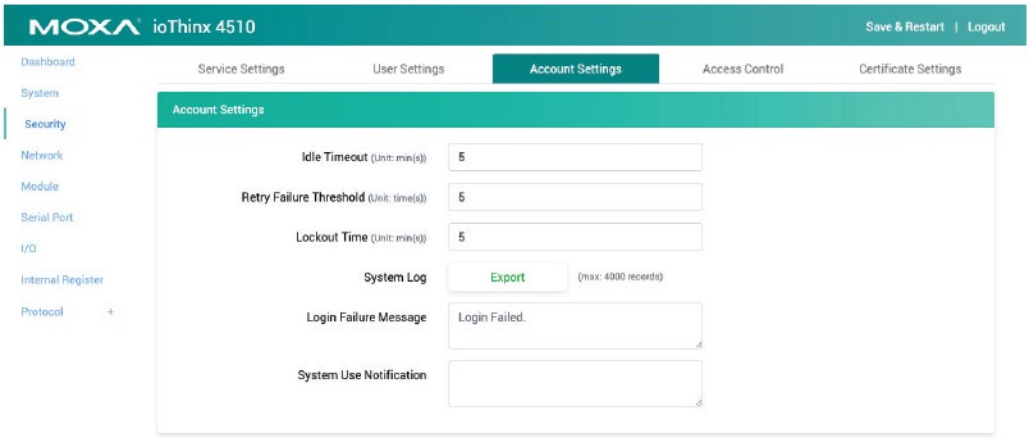
Desired IP Range	IP Address Field	Netmask Field
192.168.1.120	192.168.1.120	255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0	255.255.255.0
192.168.1.1 to 192.168.255.254	192.168.0.0	255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0	255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128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

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

Copyright © 2021 Moxa Inc.

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.

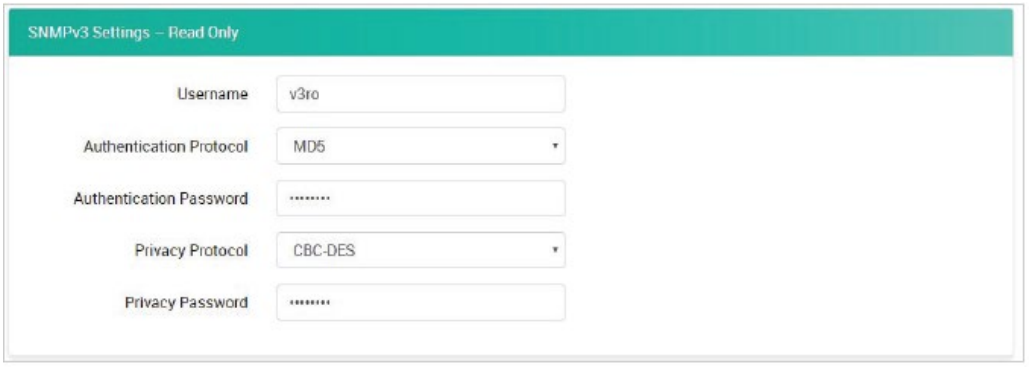


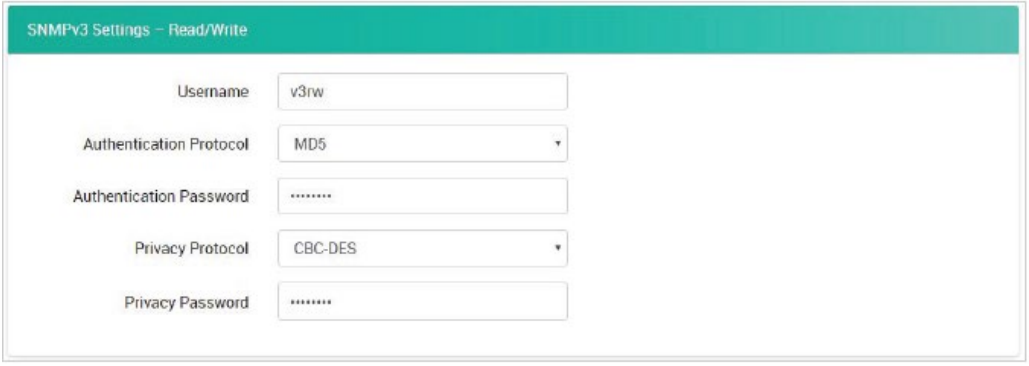
3.6. SNMPv3

- 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.

Copyright © 2021 Moxa Inc.

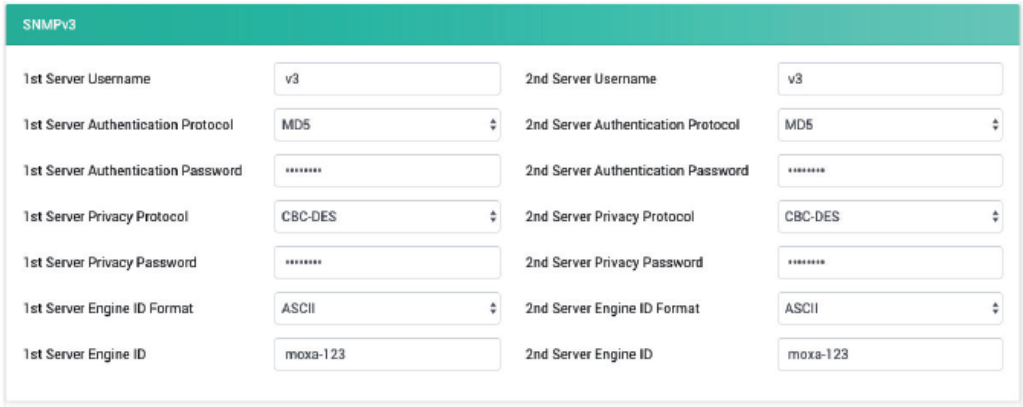
- You need to set the authentication method and privacy protocol for SNMPv3. To ensure the security level, use **SHA-256** for Authentication Protocol and **AES-128** for Privacy Protocol.





3.7. SNMP Trap/Inform

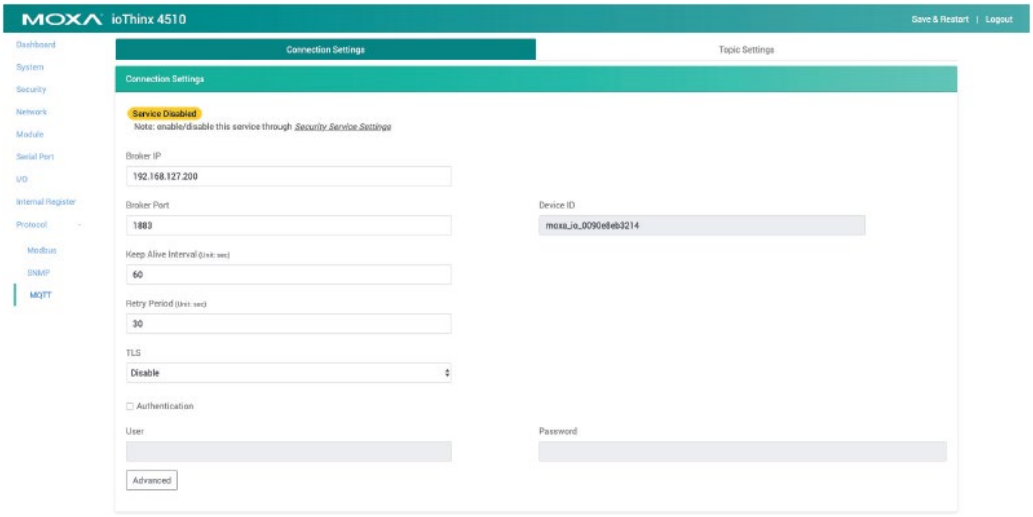
- SNMPv3 Trap/Inform provides secure notification of events. To set up SNMPv3 Trap/Inform, select **Protocol → SNMP → SNMP Trap/Inform**. Use **SHA-256** for the Authentication Protocol and **AES-128** for the Privacy Protocol.



Copyright © 2021 Moxa Inc.

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.



4. Patching/Upgrades

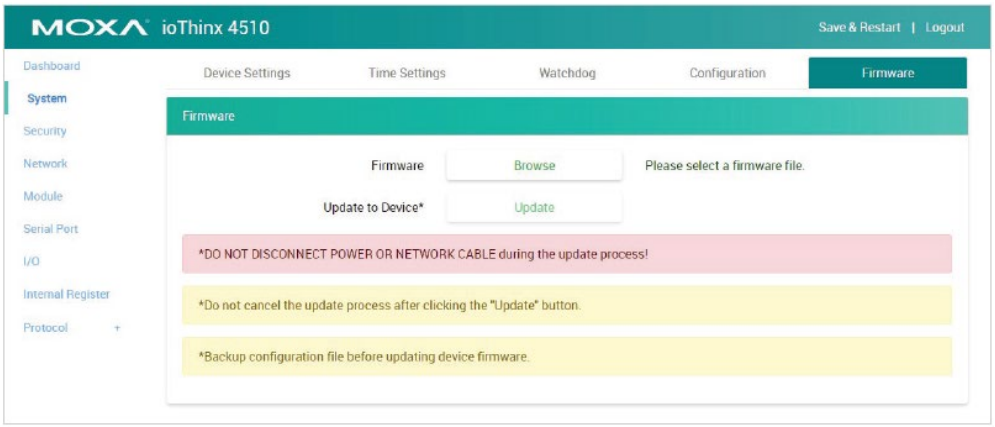
4.1. Patch Management Plan

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

4.2. Firmware Upgrades

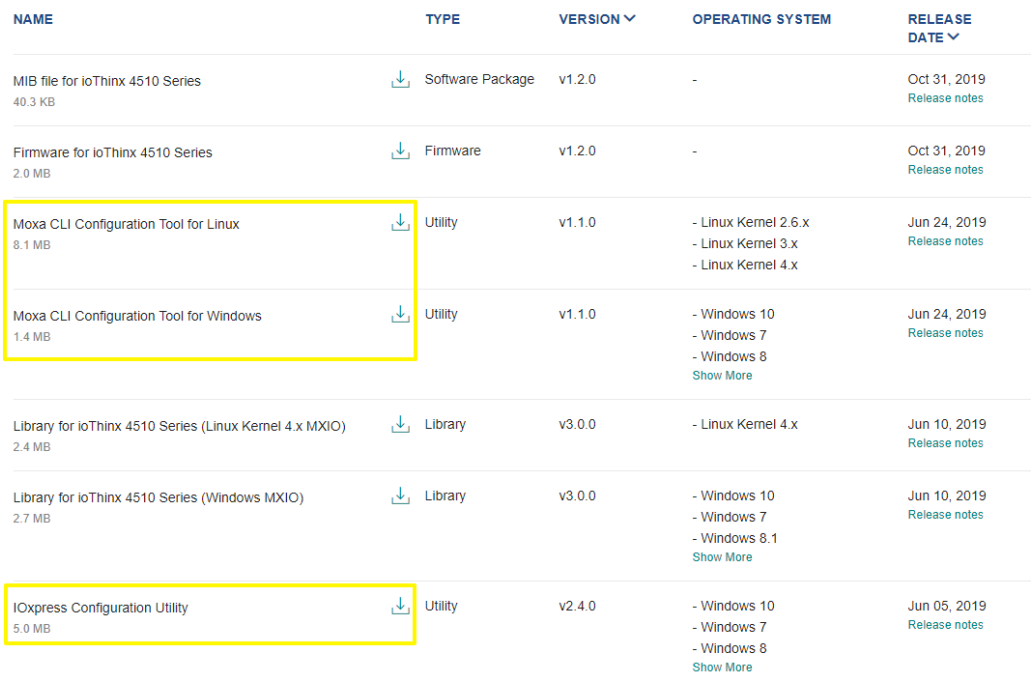
The process for upgrading firmware is as follows:

- Download the latest firmware for the ioThinx 4510 Series from the Moxa website: https://www.moxa.com/en/products/industrial-edge-connectivity/controllers-and-ios/advanced-controllers-and-i-os/iothinx-4510-series#resources
- 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.



Copyright © 2021 Moxa Inc.

- 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	VERSION	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	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

Copyright © 2021 Moxa Inc.