# The Security Hardening Guide for the ioLogik E1200 Series

***Moxa Technical Support Team***

***support@moxa.com***

## Contents



 Released on Nov 10, 2022

**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. With 35 years of industry experience, Moxa has connected more than 82 million devices worldwide and has a distribution and service network that reaches customers in more than 80 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

**How to Contact Moxa**

Tel: 1-714-528-6777
Fax: 1-714-528-6778

# 1 Introduction

This document provides guidelines on how to configure and secure the ioLogik E1200 Series. We highly recommend that you follow the steps in this document, as they are best practices for security in most applications. We also highly recommend that you review and test the configurations thoroughly before implementing them in your production system to ensure that your application is not negatively affected.

# 2 General System Information

## 2.1 Basic information of the device

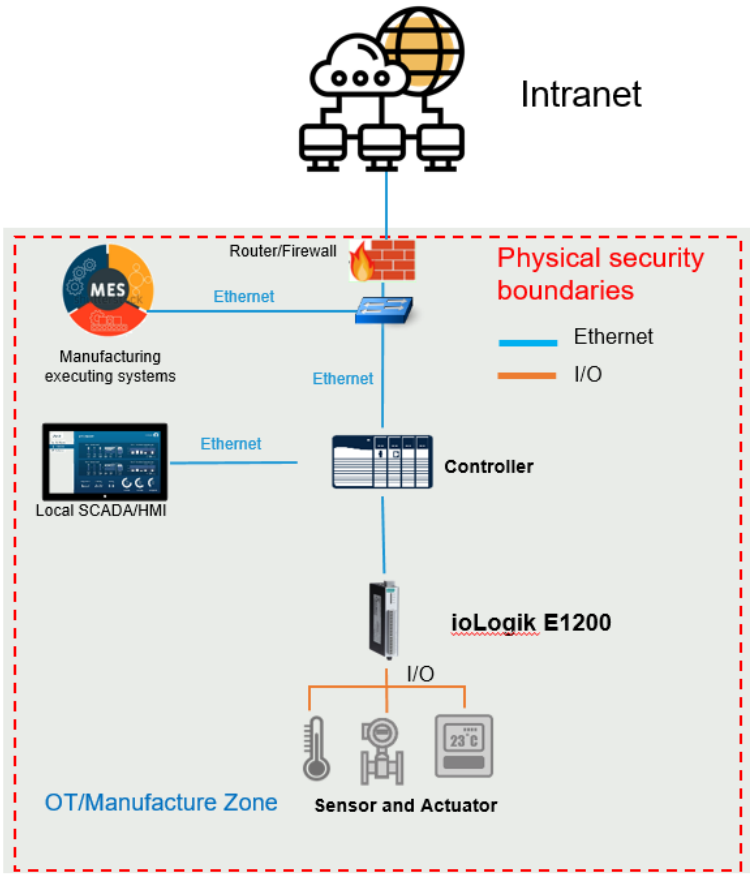
| Model | Function | Operating System | Firmware Version |
|---|---|---|---|
| ioLogik E1200 Series | Remote I/O | Embedded configurable operating system (eCos) | Version 3.2 |

The ioLogik E1200 Series supports the most often-used protocols for retrieving I/O data, making it capable of handling a wide variety of applications.

The ioLogik E1200 Series supports six different protocols: Modbus TCP, EtherNet/IP, and Moxa AOPC for OT engineers, and SNMP, RESTful API, and Moxa MXIO library for IT engineers. The ioLogik E1200 Series retrieves I/O data and converts the data to any of these protocols simultaneously, allowing your applications to get connected easily and effortlessly.

## 2.2 Deployment of the device

Deploy the ioLogik E1200 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 ioLogik E1200 Series devices and/or the system meet the security needs of your application. Depending on the environment and the threat situation, the form of protection can vary significantly.




## 2.3 Security Threats

The following security threats can harm the ioLogik E1200 Series:

1. **Attacks over the network**

   Threats from individuals with no rights to the ioLogik E1200 Series via networks such as intranets.

2. **Direct attacks through operations**

   Threats where individuals with no rights to the ioLogik E1200 Series directly operate a device to affect the system and steal important data.

3. **Theft of the ioLogik E1200 Series or I/O data**

   Threats where an ioLogik E1200 Series or I/O data is stolen, and important data is analyzed.

## 2.4 Security Measures

To fend off security threats, we arranged security measures applied in security guides for the general business network environment and identified a set of security measures for the ioLogik E1200 Series. We classify the security measures into three security types. The following table describes the security measures and the threats that each measure handles.

| Security Measure | Subcategory | Threat Handled | | |
|---|---|---|---|---|
| | | 1 | 2 | 3 |
| Access Control | – | Yes | Yes | No |
| Stopping unused services | – | Yes | No | No |
| Changing IT environment settings | Disabling the built-in Administrator account or changing its username | Yes | Yes | No |
| | IT firewall tuning | Yes | No | No |
| | Hiding the last logged-on username | Yes | Yes | No |
| | Applying the software restriction policies | Yes | Yes | No |
| | Applying AutoRun restrictions | No | Yes | No |
| | Applying the StorageDevicePolicies function | No | Yes | Yes |
| | Disabling USB storage devices | No | Yes | Yes |
| | Disabling NetBIOS over TCP/IP | Yes | No | No |
| | Applying the password policy | Yes | Yes | No |
| | Applying the audit policy | Yes | Yes | No |
| | Applying the account lockout policy | Yes | Yes | No |

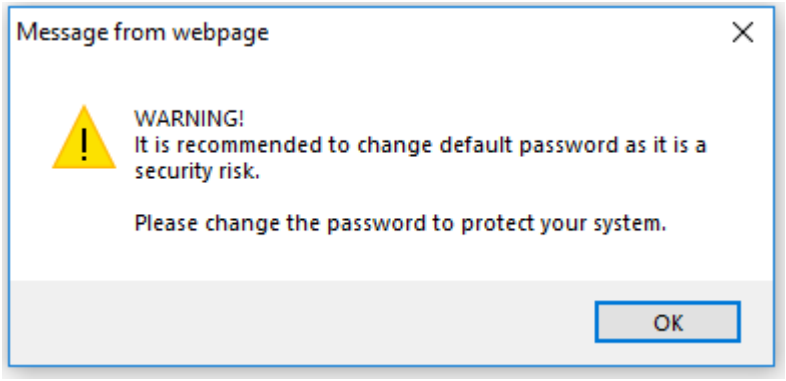
**Note** Threat 1: Attacks over the network.
Threat 2: Direct attacks through the operation.
Threat 3: Theft of the ioLogik E1200 Series or I/O data

To defend against the theft of the ioLogik E1200 Series or I/O data, we recommend you to use the ioLogik E1200 Series within a secure local network, as mentioned above. We also suggest that you enable the Accessible IP List function (for more details, please refer to chapter 3.3) to only allow the necessary hosts/IPs to access the device and protect the device from attacks of unknown client.

# 3 Configuration and Hardening Information

Log in the device by entering the default IP address in the web console. Once you have successfully logged in, a notification will pop up to remind you to change the password. The snapshot below is the GUI for the web console.

To protect your system, remember to set the password after entering the ioLogik E1200 web console.




## 3.1 TCP/UDP ports status

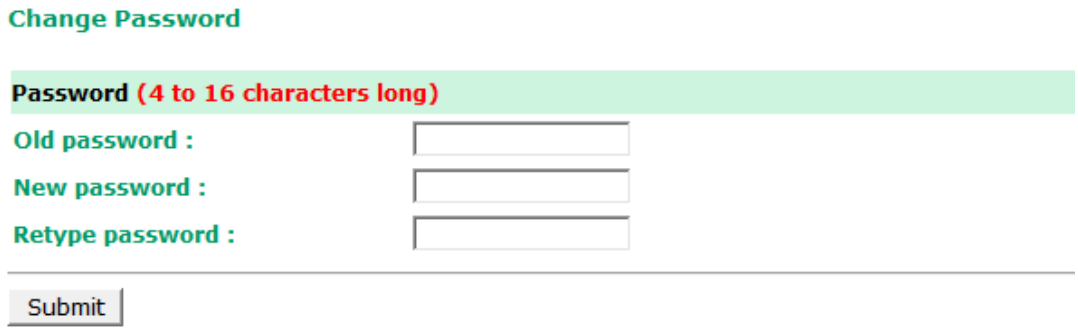
Please refer to the table below for all the ports, protocols, and services that are used to communicate between ioLogik E1200 Series and other devices.

**ioLogik E1200 Network Port Usage**

| Port | Type | Usage |
|---|---|---|
| 68 | UDP | BOOTP/DHCP |
| 69 | UDP | Export/import configuration file |
| 80 | TCP | Web console service |
| 161 | UDP | SNMP Agent |
| 502 | TCP | Modbus/TCP communication |
| 2222 | UDP | EtherNet/IP implicit message |
| 4800 | UDP | Auto search |
| 9020 | TCP | Peer-to-peer (default) |
| 9200 | TCP | ioLogik 2500's expansion |
| 10124 | TCP | Configuration port (ioSearch) |
| 44818 | TCP | EtherNet/IP explicit message |

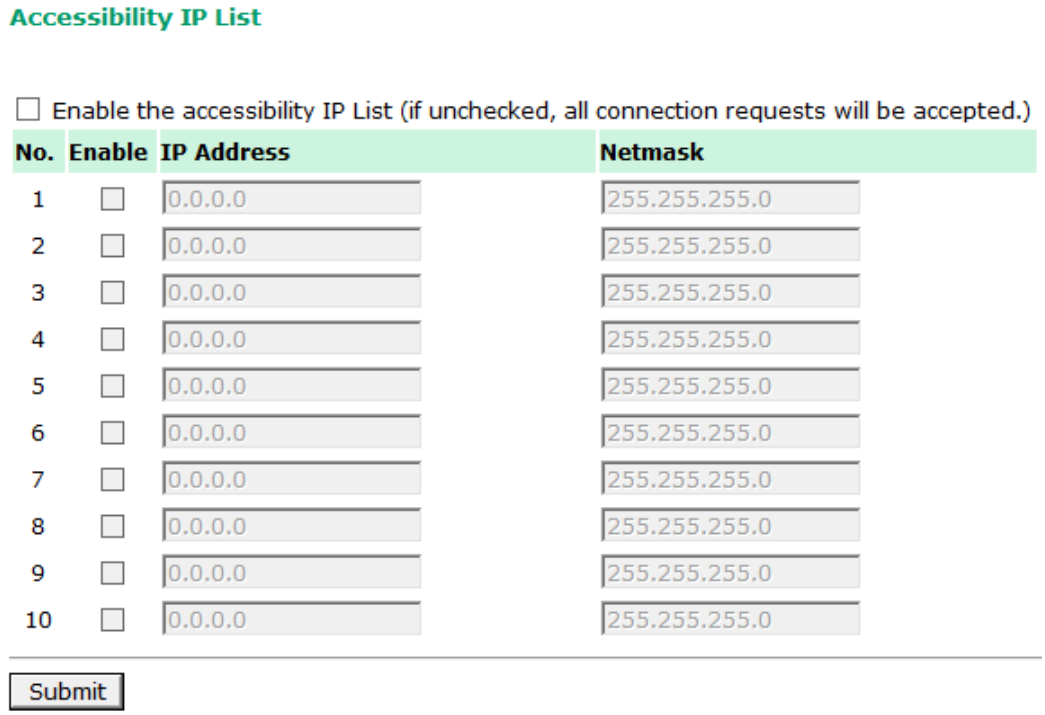
## 3.2 Change Password

By default, you can access the device by entering the default IP address in the web console. To change the password, please log in to the web console and select **Main Menu → Change Password**. The snapshot below is the GUI for the web console.




## 3.3 Accessibility IP List

The ioLogik E1200 Series has a feature that adds or blocks the IP addresses of remote hosts to prevent unauthorized access to the remote I/O. That is, if a host's IP address is in the Accessibility IP List, then the host will be allowed to access the ioLogik E1200 Series. To configure it, please log in to web console and select **Main Menu → System Management → IP Accessibility**. The snapshot below is the GUI for the web console.



# 4 Patching/Upgrades

## 4.1 Patch Management

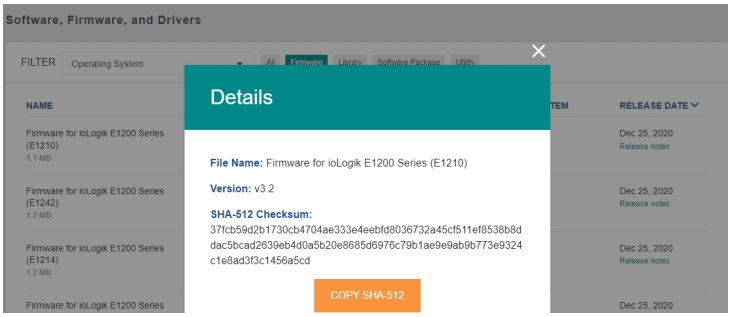
Regarding patch management, Moxa releases version enhancements with detailed release notes annually.

## 4.2 Firmware Upgrades

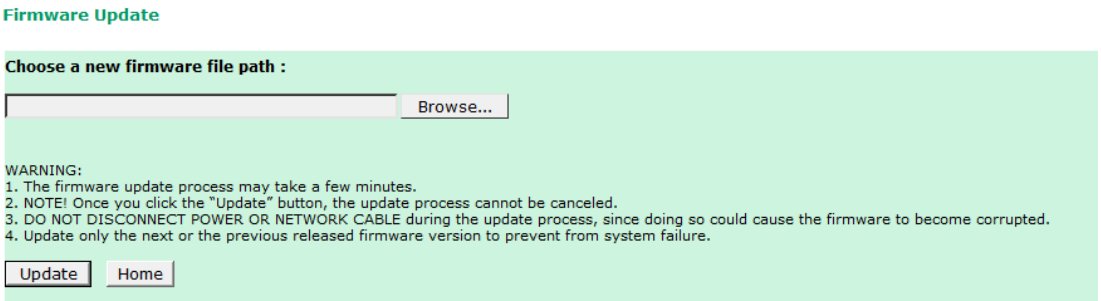
The process for firmware and/or software upgrades is as below.

- We will release the latest firmware and software, along with its release notes on our official website. The link below is listed for specified items of the ioLogik E1200 Series.
  - Firmware of ioLogik E1200 Series:

    https://www.moxa.com/en/products/industrial-edge-connectivity/controllers-and-ios/universal-controllers-and-i-os/iologik-e1200-series#resources
- Moxa's website provides the SHA-512 hash value for you to double-check if the firmware is identical to the one on the website.




- When you want to upgrade the firmware of the ioLogik E1200 Series, please download the firmware from the website first. Then log in to the web console and select **Main Menu → System Management → Firmware Update**. Click the **Browse** button to select the proper firmware and click **Update** to upgrade the firmware.



# 5 Security information/Vulnerability feedback

As the adoption of the Industrial Internet of Things (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.

Please follow the updated Moxa security information from the link below:
https://www.moxa.com/en/support/product-support/security-advisory