

The Security Hardening Guide for the ioLogik E2200 Series

Moxa Technical Support Team

support@moxa.com

Contents

1	Introduction	2
2	General System Information	2
2.1	Basic Information About the Device.....	2
2.2	Deployment of the Device	3
2.3	Security Threats	4
2.4	Security Measures.....	4
3	Configuration and Hardening Information.....	5
3.1	TCP/UDP Port Status	6
3.2	Change the Password	7
3.3	Accessibility IP List.....	8
4	Patching/Upgrades	9
4.1	Patch Management	9
4.2	Firmware Upgrades	9
5	Decommission	10
6	Security Information/Vulnerability Feedback	11

Copyright © 2025 Moxa Inc.

Released on Nov 7, 2025

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 over 35 years of industry experience, Moxa has connected more than 111 million devices worldwide and has a distribution and service network that reaches customers in more than 91 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

MOXA®

1 Introduction

The ioLogik E2200 Series configuration and security guidelines are detailed in this document. Consider the recommended steps in this document as best practices for security in most applications. We 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 About the Device

Model	Function	Operating System	Firmware Version
ioLogik E2200 Series	Active Remote I/O	Moxa operating system	V3.14 (E2212) V3.13 (E2210, E2260) V3.12 (Others)

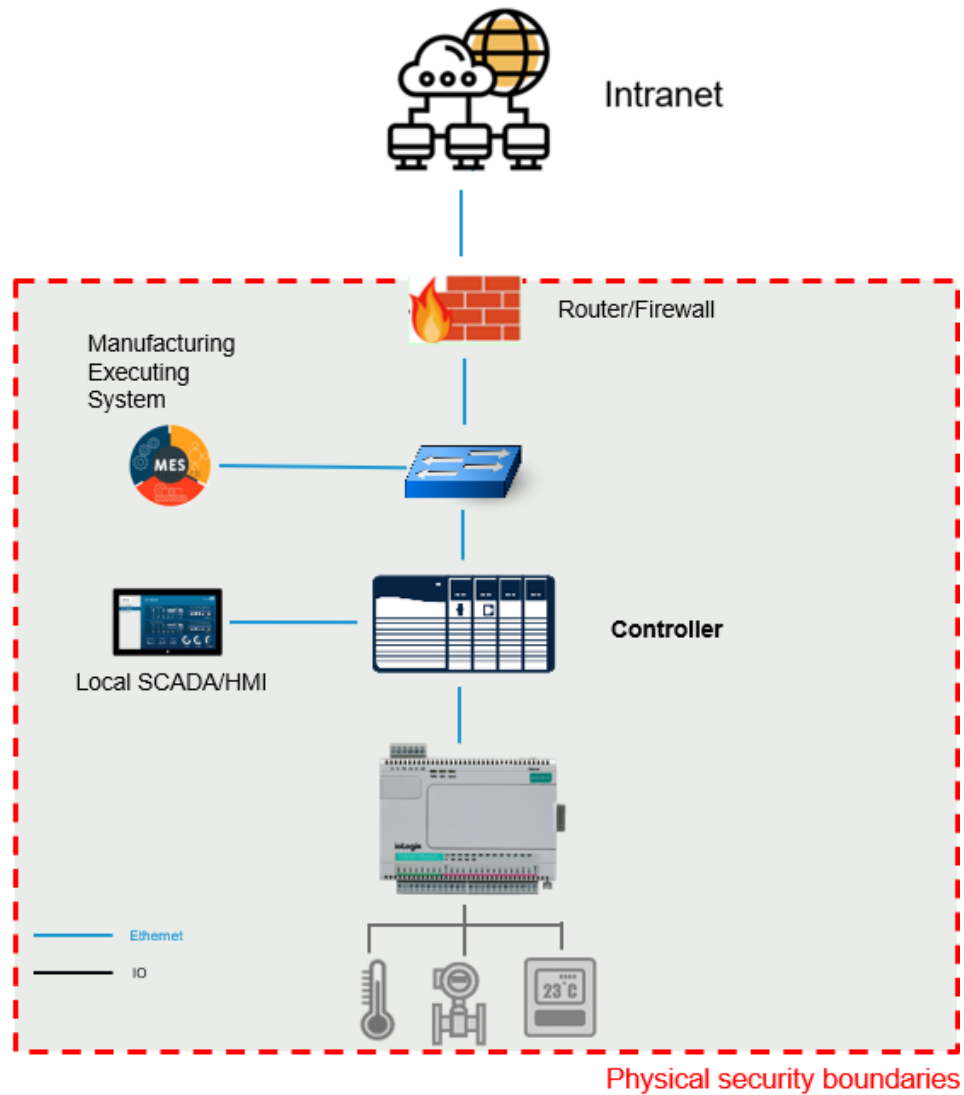
The ioLogik E2200 Series supports the most often-used protocols for retrieving I/O data, making it capable of handling a wide variety of applications.

The ioLogik E2200 Series supports different protocols, including Modbus TCP, Moxa AOPC, SNMP, and Moxa MXIO library. The ioLogik E2200 Series retrieves I/O data and converts the data to any of these protocols at the same time, allowing you to get your applications connected easily and effortlessly.

The embedded Click&Go control logic provides easy and stable if-then-else event-based rules to control I/O channels on-site, hugely decreasing the system complexity and development time.

2.2 Deployment of the Device

Deploy the ioLogik E2200 Series behind a secure firewall network that has sufficient security features in place to ensure that networks are safe from internal and external threats. Make sure that the physical protection of the ioLogik E2200 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.



2.3 Security Threats

The following security threats can harm the ioLogik E2200 Series:

1. Attacks over the network

Threats from individuals with no rights to the ioLogik E2200 Series via networks such as intranets.

2. Direct attacks through operations

Threats where individuals with no rights to the ioLogik E2200 Series directly operate a device to affect the system and steal important data.

3. Theft of the ioLogik E2200 Series or I/O data

Threats where an ioLogik E2200 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 by security guides for the general business network environment and identified a set of security measures for the ioLogik E2200 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 Measurement	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 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

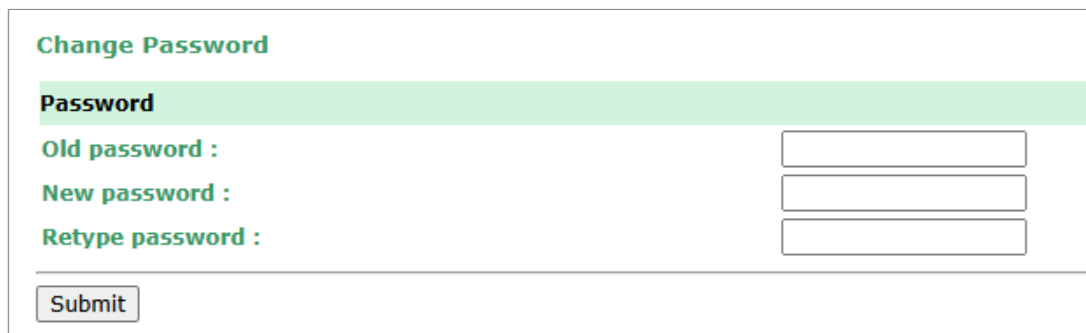
Note Threat 1: Attacks over the network.
Threat 2: Direct attacks through the operation.
Threat 3: Theft of the ioLogik E2200 Series or I/O data

To defend against the theft of the ioLogik E2200 Series or I/O data, we recommend you use the ioLogik E2200 Series within a secure local network, as mentioned above. We also suggest that you enable the Accessible IP List function (for more details, refer to Chapter 3.3) to only allow the necessary hosts/IPs to access the device and protect the device from attacks from unknown clients.

3 Configuration and Hardening Information

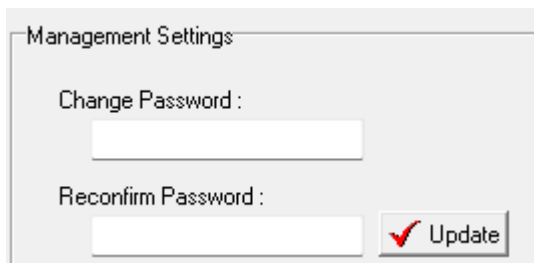
Log in to the device by entering the default IP address in the web console or using Moxa ioAdmin utility. Remember to set the password after entering the ioLogik E2200 console to protect your system.

Below snapshot is the GUI from the Web Console.



The image shows a web console interface for changing a password. It has a title 'Change Password' in green. Below it is a green header bar with the word 'Password' in black. There are three input fields: 'Old password :', 'New password :', and 'Retype password :'. Each field has a corresponding text input box. At the bottom left is a 'Submit' button.

The snapshot below is the GUI from the ioAdmin utility.



The image shows a screenshot of the 'Management Settings' window in the ioAdmin utility. It contains two input fields: 'Change Password :' and 'Reconfirm Password :'. To the right of the 'Reconfirm Password :' field is an 'Update' button with a red checkmark icon.

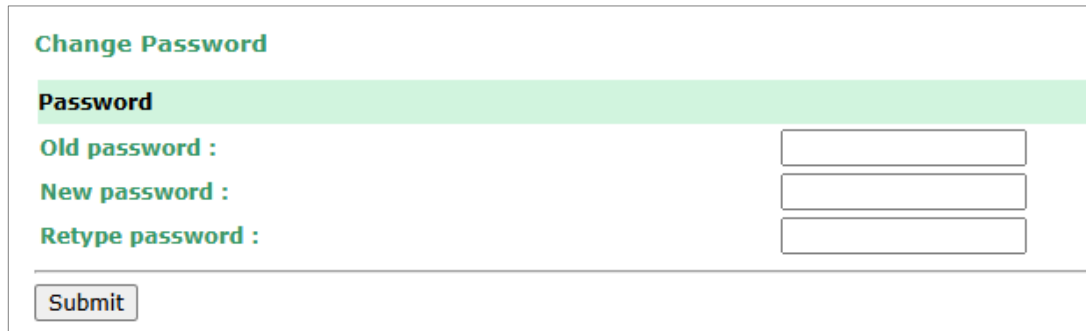
3.1 TCP/UDP Port Status

Refer to the table below for all the ports, protocols, and services that are used to communicate between the ioLogik E2200 Series and other devices.

Port	Type	Usage
68	UDP	BOOTP
68	UDP	DHCP
69	UDP	Export/import file
80	TCP	Web Server
161	TCP	SNMP
502	TCP	Modbus Communication
4800	UDP	Auto search
9020	TCP	Peer-to-peer function
9000	TCP	Active Message (Default)
9000	UDP	Active Message (Default)
9900	TCP	Active Tags updates (Default)
4040	TCP	ioEventLog
4900	TCP	ioAdmin
14900	TCP	ioAdmin
4800	UDP	ioAdmin
137	UDP	WIN Server
9010	TCP	Remote Action

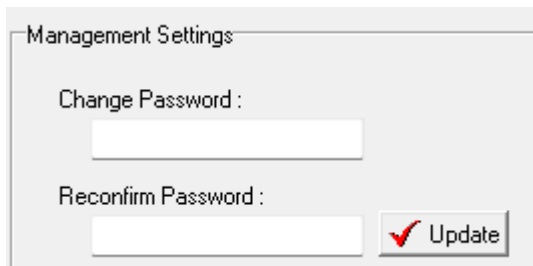
3.2 Change the Password

By default, users can access the device by entering the default IP address in the web console and/or the ioAdmin utility. To change the password, log in to the web console, and select **Main Menu > Change Password**. The snapshot below is the GUI from Web Console.



The screenshot shows the 'Change Password' interface in the Web Console. It features a title 'Change Password' in green. Below it, a green header bar contains the word 'Password'. The form includes three input fields: 'Old password :', 'New password :', and 'Retype password :'. A 'Submit' button is located at the bottom left of the form area.

If you are using ioAdmin, go to **Server Setting** tab, and find **Management Settings**. The snapshot below is the GUI from ioAdmin.



The screenshot shows the 'Management Settings' window in ioAdmin. It has a title bar 'Management Settings'. Inside, there are two input fields: 'Change Password :' and 'Reconfirm Password :'. An 'Update' button with a red checkmark icon is positioned to the right of the second input field.

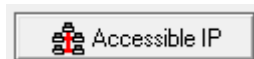
3.3 Accessibility IP List

The ioLogik E2200 Series has a feature that can add or block remote host IP addresses to prevent unauthorized access to the remote I/O. That is, if a host's IP address is in the accessible IP table, then the host will be allowed to access the ioLogik E2200 Series. To configure it, log in to the web console and select **Main Menu > System Management > IP Accessibility**. The snapshot below is the GUI from Web Console.

The screenshot shows the 'Accessibility IP List' configuration page in a web console. At the top, there is a checkbox labeled 'Enable the accessibility IP List (if unchecked, all connection requests will be accepted.)'. Below this is a table with four columns: 'No.', 'Enable', 'IP Address', and 'Netmask'. The table has 10 rows, numbered 1 to 10. Each row has an 'Enable' checkbox, an 'IP Address' input field, and a 'Netmask' input field. At the bottom left of the table area is a 'Submit' button.

No.	Enable	IP Address	Netmask
1	☐		
2	☐		
3	☐		
4	☐		
5	☐		
6	☐		
7	☐		
8	☐		
9	☐		
10	☐		

If you are using ioAdmin, go to **the Network** tab and find **IP Settings > Accessible IP**.



The snapshot below is the GUI from ioAdmin.

The screenshot shows the 'Accessible IP Settings' dialog box in ioAdmin. It has a title bar with a close button. Inside, there is a checkbox labeled 'Enable the accessibility IP List (if unchecked, all connection requests will be accepted.)'. Below this is a list of 10 items, each with an 'Enable' checkbox, an 'IP' input field, and a 'mask' input field. The IP and mask fields are pre-filled with '0.0.0.0'. At the bottom are 'OK' and 'Cancel' buttons.

No.	Enable	IP	mask
1	☐	0.0.0.0	0.0.0.0
2	☐	0.0.0.0	0.0.0.0
3	☐	0.0.0.0	0.0.0.0
4	☐	0.0.0.0	0.0.0.0
5	☐	0.0.0.0	0.0.0.0
6	☐	0.0.0.0	0.0.0.0
7	☐	0.0.0.0	0.0.0.0
8	☐	0.0.0.0	0.0.0.0
9	☐	0.0.0.0	0.0.0.0
10	☐	0.0.0.0	0.0.0.0

4 Patching/Upgrades

4.1 Patch Management

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

4.2 Firmware Upgrades

The instructions for upgrading firmware and/or software are below.

- We will release the latest firmware and software along with their release notes on our official website. We list the linkages below for the specified ioLogik E2200 Series items.
 - Firmware of the ioLogik E2200 Series:
<https://www.moxa.com/en/products/industrial-edge-connectivity/controllers-and-ios/universal-controllers-and-i-os/iologik-E2200-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.

Software, Firmware, and Drivers

FILTER Operating System ▾ All **Firmware** Library Software Package Utility

NAME	ITEM	RELEASE DATE ▾
Firmware for ioLogik E2200 Series (E2210) 2.4 MB		Jan 20, 2017 Release notes
Firmware for ioLogik E2200 Series (E2214) 1.2 MB		Jan 19, 2017 Release notes
Firmware for ioLogik E2200 Series (E2212) 1.2 MB		Jan 19, 2017 Release notes
Firmware for ioLogik E2200 Series (E2262) 1.2 MB		Jan 19, 2017 Release notes
Firmware for ioLogik E2200 Series (E2242) 1.3 MB		Jan 19, 2017 Release notes

Details

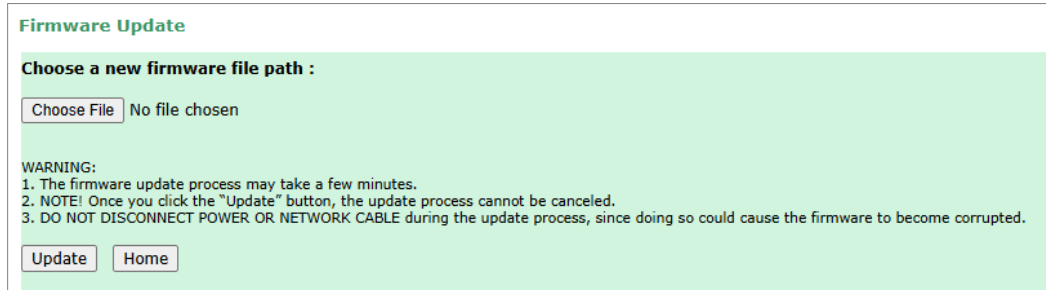
File Name: Firmware for ioLogik E2200 Series (E2210)

Version: v3.13

SHA-512 Checksum:
ebe57daee88804901ddb121e428f3eef3afbc21e6d7e476ea4be95f3
745581c4289e644383edbf1ef12c68fe4e9652db7c5f44c5cbc71d0b
87585fc1b3299ab2

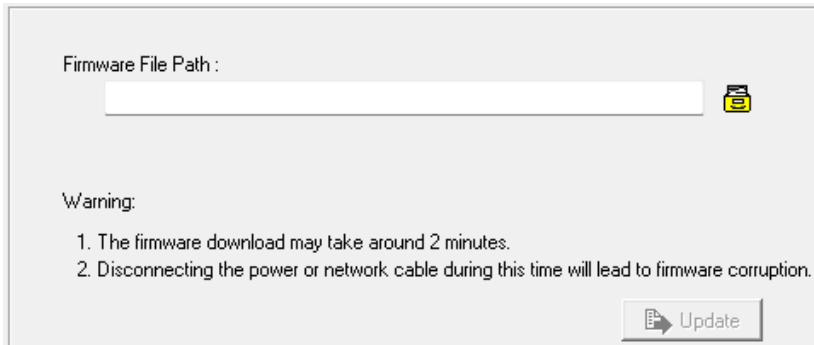
COPY SHA-512

- When you want to upgrade the firmware of the ioLogik E2200 Series, download the firmware from the website first. Then log in to the web console and select **Main Menu > System Management > Firmware Update**. Select the **Choose File** button to choose the proper firmware and select **Update** to upgrade the firmware.



The screenshot shows a web interface titled "Firmware Update". It has a green header bar. Below the header, it says "Choose a new firmware file path :". There is a "Choose File" button and the text "No file chosen". Below this, there is a "WARNING:" section with three numbered points: 1. The firmware update process may take a few minutes. 2. NOTE! Once you click the "Update" button, the update process cannot be canceled. 3. DO NOT DISCONNECT POWER OR NETWORK CABLE during the update process, since doing so could cause the firmware to become corrupted. At the bottom, there are two buttons: "Update" and "Home".

- If you are using ioAdmin, find the **Firmware Update** tab. Select the  button to choose the proper firmware and select **Update** to upgrade the firmware.



The screenshot shows a web interface titled "Firmware Update". It has a light gray header bar. Below the header, it says "Firmware File Path :". There is a text input field and a "Choose File" button. Below this, there is a "Warning:" section with two numbered points: 1. The firmware download may take around 2 minutes. 2. Disconnecting the power or network cable during this time will lead to firmware corruption. At the bottom, there is an "Update" button with a right-pointing arrow.

5 Decommission

Since the ioLogik E2200 Series is the primary device for transferring I/O data to Ethernet devices and a local I/O control device, decommissioning an ioLogik E2200 Series device requires arranging annual maintenance to replace the old unit with a new one. Follow these steps to complete the process:

- Export the configuration file from the old ioLogik E2200 and import it to the new unit. This will save you from having to configure the new unit manually.
- Stop communication and replace the old unit.
- Restart communication and check if everything works fine. If yes, proceed to step 4 to decommission the old unit. If not, you may need assistance to troubleshoot the issue.
- Keep the old unit powered on and press the Reset button for 5 seconds to restore the settings to factory default.
- After the device reboots and all user settings are removed or overwritten, you may scrap it.

6 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.

Follow the updated Moxa security information from the link below:

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