Plat' Home
TECHNOLOGY to serve you.

OpenBlocks IoT Family
Security Guide

Ver.3.1.0

Plat'Home Co., Ltd.

■ About trademarks

- Linux is a trademark or registered trademark of Linus Torvalds in the United States and/or other countries.
- Company and product names mentioned in this Security Guide may be trademarks or registered trademarks of their respective companies.
- Product names and other proper nouns in this Security Guide are trademarks or registered trademarks of their respective companies.

■ Before using this product

- No reproduction of this material is allowed without written permission of Plat'Home Co., Ltd.
- Content and information contained within this material may be changed or updated without prior notice.
- We consistently aim to keep the content in this material as precise as possible. However, should any errors in descriptions, etc. be noticed, please contact Plat'Home Co., Ltd. The latest version of this material can be downloaded from our website.
  While using this product, please be aware that it is not designed or assumed for use in fields where there is a risk to life.
- Regardless of the aforementioned, in no event will Plat'Home be liable for any special, incidental, indirect or consequential damage arising out of use of this product, including but not limited to damage to profits or loss.

Table of contents

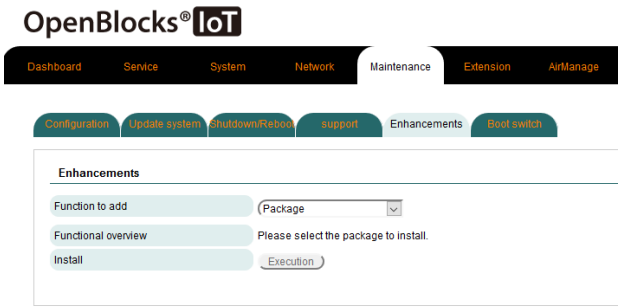
Chapter 1 General

This manual describes how to use security setups against illegal access that can be installed in the OpenBlocks IoT Family, including web user interface (hereinafter referred to as "WEB UI").

Chapter 2 Security setup

2-1. Installing security functions

At the time of shipment from our factory, a WEB UI security setup is not installed in this product. WEB UI security setup can be performed using the **[Maintenance]-[Enhancements]** tab.



Choose the **[Maintenance]** tab in WEB UI and click on the **[Enhancements]** tab to choose a package for extension.

Choose "Security" from the pull-down menu next to Function to add.

Press the "Execution" button to install extension.

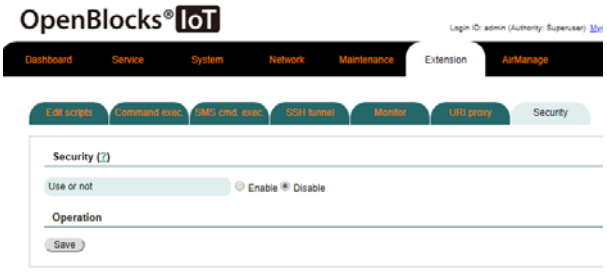
After completing the extension, the unit will require rebooting to make the installation effective. Choose the Shutdown/Reboot tab to reboot the unit.

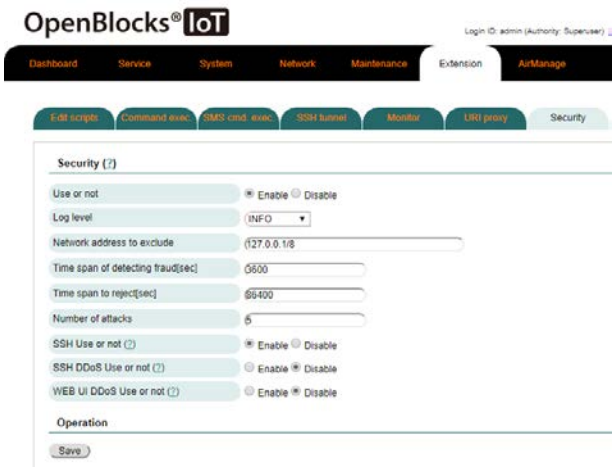
2-2 Security use settings

With security functions installed, the **[Security]** tab will be added to the **[Extension]** tab, showing security setting items.

Choose "To be use" for the To be use line to enable the security functions to be applied and press the "Save" button to apply desired security functions.

When attacks have occurred for a number of designated times of an attack during a predetermined period counted from and including an initial attack, this function will reject access by the attacking IP address.





Security

Use or not:

Sets use of the security function. To use this function, choose "Enable".

Log level:

Choose a log level to output from the following:

- INFO
- CRITICAL
- ERROR
- WARNING
- NOTICE
- DEBUG

Essentially, there is no need to change this item from "INFO."。

Network addresses to exclude:

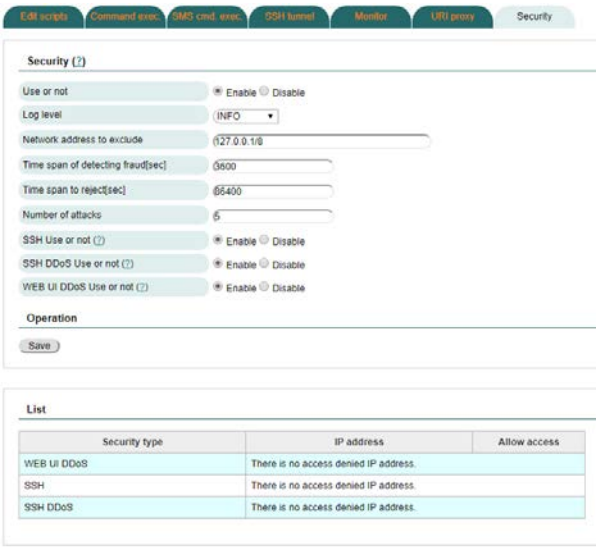
Designate network addresses to be excluded from security functions. To designate multiple addresses, separate by a space.

Ex.) To add a network of 192.168.254.0:

“127.0.0.1/8 192.168.254.0/24”

Time span of detecting fraud [sec] :

When attacks from a target address to a subject service have started, this setting specifies a period to group such attacks as a set of similar attacks.



Time span to reject [sec] :

Sets time to reject access from target IP address to a subject service.

Number of attacks:

Specifies the times to ascertain that access should be denied when attacks have been made specified times during a predetermined time span.

SSH use setting:

Sets use of the security function with login failure of an SSH.

Choose "To be use" to use this function.

SSH DDoS use setting:

Sets use of the security function against DDoS attacks on an SSH.

Choose "To be use" to use this function.

WEB UI DDoS use setting:

Sets use of the security function against 403/404 access attacks for HTTP/HTTPS access at the port WEB UI is using.

Choose "To be use" to use this function.

If individual use settings are set to "To be use," the security function will become effective.

2-3. Releasing access rejections against attacks

When the security function is enabled, a list of effective security functions will be displayed at the bottom of the **[Extension]-[Security]** tab.

It will also show a combination of IP addresses rejected for access as well as subject services.

*If no access rejections exists:

If there is no attack and the system is operating normally, no IP address rejected to access will be displayed as per the screen-shot on the left.

*If access rejections exists in an SSH

If attacks have been made and there is an IP address rejected for access, an IP address and the "Allow access" button will be displayed as per the screen-shot on the left.

The Allow access button will allow the target IP address to re-access the subject service. Use this button to enable a user without any issues to re-access after login failures, etc.

Chapter 3 Others

3-1. About extensions, etc.

This function uses fail2ban DAEMON. Should a customer want to extend security functions, refer to the page below. Plat'Home assumes no liability for file editions, additions or deletions as a result of an extension. The customer will assume this responsibility.

https://www.fail2ban.org/wiki/index.php

Using the Save button in the Extension tab of WEB UI, the following files will be re-generated.

・/etc/fail2ban/fail2ban.conf
・/etc/fail2ban/jail.local

If there is no need for these files to be overwritten, prepare the following file.

●File to prohibit overwriting
/var/webui/config/fail2ban.userlock

If files have been edited under existing /etc/fail2ban/, they cannot be recovered. To recover these files, conduct factory resetting and re-installation.

Plat'Home Co., Ltd.
NIHON BUILDING KUDANBEKKAN, 3F
4-1-3, Kudankita, Chiyoda-ku, TOKYO 102-0073, JAPAN