WAGO I/O SYSTEM 750

Security Settings in WAGO 758 Series IPCs

Application Note

A117600, English
Version 1.0.0

WAGO® INNOVATIVE CONNECTIONS

WAGO Kontakttechnik GmbH
Hansastraße 27
D-32423 Minden

Phone: +49 (0) 571/8 87 – 0
Fax: +49 (0) 571/8 87 – 1 69

E-Mail: info@wago.com

Web: http://www.wago.com

Technical Support
Phone: +49 (0) 571/8 87 – 5 55
Fax: +49 (0) 571/8 87 – 85 55

E-Mail: support@wago.com

Every conceivable measure has been taken to ensure the correctness and completeness of this documentation. However, as errors can never be fully excluded we would appreciate any information or ideas at any time.

We wish to point out that the software and hardware terms as well as the trademarks of companies used and/or mentioned in the present manual are generally trademark or patent protected.

TABLE OF CONTENTS

1 Important comments

To ensure fast installation and start-up of the units described in this manual, we strongly recommend that the following information and explanation is carefully read and adhered to.

1.1 Legal principles

1.1.1 Copyright

This manual is copyrighted, together with all figures and illustrations contained therein. Any use of this manual which infringes the copyright provisions stipulated herein, is not permitted. Reproduction, translation and electronic and photo-technical archiving and amendments require the written consent of WAGO Kontakttechnik GmbH. Non-observance will entail the right of claims for damages.

1.1.2 Personnel qualification

The use of the product detailed in this manual is exclusively geared to specialists having qualifications in PLC programming, electrical specialists or persons instructed by electrical specialists who are also familiar with the valid standards. WAGO Kontakttechnik GmbH declines all liability resulting from improper action and damage to WAGO products and third party products due to non-observance of the information contained in this manual.

1.1.3 Intended use

For each individual application, the components supplied are to work with a dedicated hardware and software configuration. Modifications are only admitted within the framework of the possibilities documented in the manuals. All other changes to the hardware and/or software and the non-conforming use of the components entail the exclusion of liability on part of WAGO Kontakttechnik GmbH.

Please direct any requirements pertaining to a modified and/or new hardware or software configuration directly to WAGO Kontakttechnik GmbH.

1.2 Range of validity

This application note is based on the stated hardware and software of the specific manufacturer as well as the correspondent documentation. This application note is therefore only valid for the described installation.

New hardware and software versions may need to be handled differently. Please note the detailed description in the specific manuals.

1.3 Symbols

Danger
Always observe this information to protect persons from injury.

Warning
Always observe this information to prevent damage to the device.

Attention
Marginal conditions must always be observed to ensure smooth operation.

ESD (Electrostatic Discharge)
Warning of damage to the components by electrostatic discharge. Observe the precautionary measure for handling components at risk.

Note
Routines or advice for efficient use of the device and software optimisation.

More information
References to additional literature, manuals, data sheets and INTERNET pages

2 Description

This document provides information on security settings for WAGO's Industrial PCs (IPCs)

3 Reference Material

WAGO strongly recommends changing the default passwords that are shipped with our products as these are publicly documented. Therefore they do not provide sufficient protection.

WAGO's IPC products have several passwords that need to be changed. This includes both the Web Based Management and the Linux Console.

To help reduce the risk of unwanted or unintended access to the IPC there are several functions that can be disabled to minimize the access to the IPC as outlined in section 6.

This procedure has been tested with WAGO's 758-874, 758-875 and 758-876 versions.

4 Web Based Management Passwords

4.1 Overview

The WAGO IPCs have implemented HTML pages for Web Based Management that are used to configure the IPC. To access the Web Based Management use the following procedure:

1. Connect the IPC with the LAN via X9 Ethernet interface.

2. Access the Web Based Management by starting your internet browser and enter the IP address in the address bar. The factory preset IP address is 192.168.2.17.

Refer to the product manual for addition connection information.

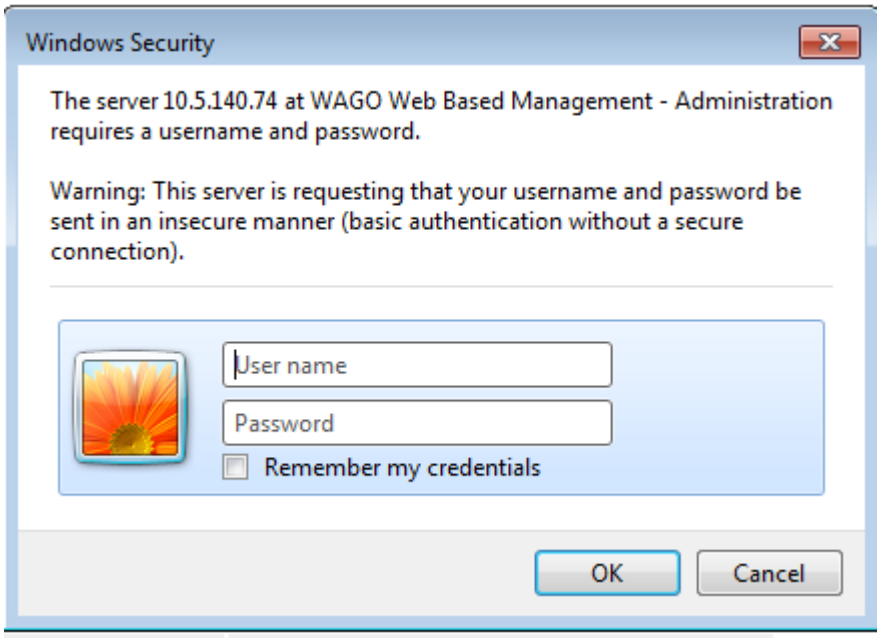
All the HTML pages are password protected except the Information and WebVisu pages.

4.2 Changing Passwords for Web Based Management

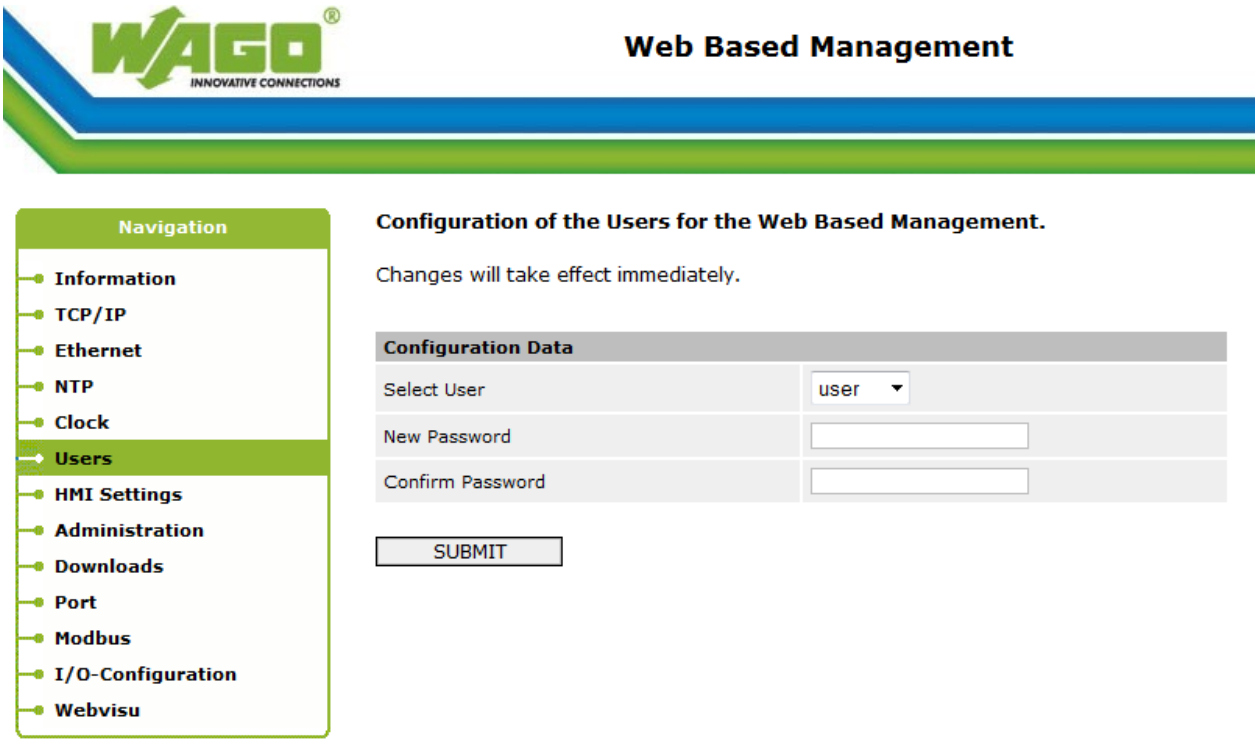
First go online with the Web-Based Management system as described above. Select the “Users” page. On this page you are able to change the passwords for the Web Based Management system user and admin privileges.

Users have access to the “TCP/IP”, “NTP”, “Clock”, “Port” and “Modbus” pages. Admin has access to all pages.

To access the “User” page you must have admin privileges. When you select the “User” page, you will be prompted for a user name a password in a window that looks like the following:

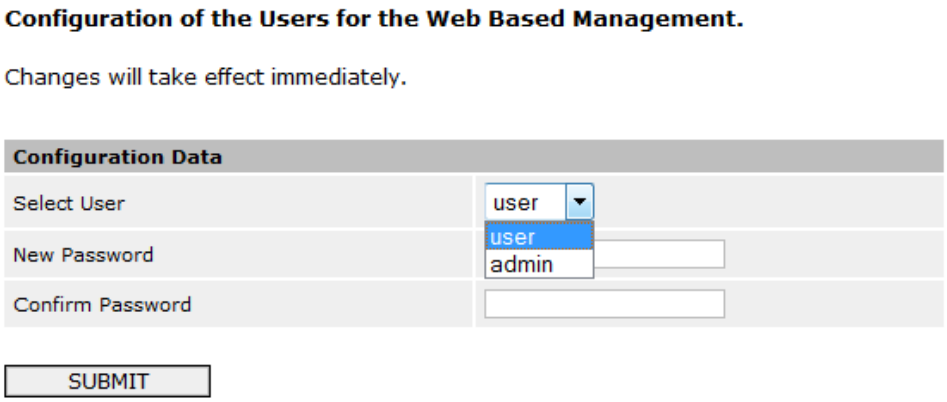


Once you have access to this page you will see a page that looks like this:



T
o change the user password, simply type the new password in the New Password input field and verify it in the Confirm Password Field, then click on SUBMIT.

To change the admin password, select the drop down and click on admin.



Follow the same steps as above. Note that the password changes will take effect immediately after clicking the SUBMIT button.

5 Changing the Password in the Linux Console

5.1 Overview

The WAGO IPCs are Linux based PCs and you can connect to the Linux Console through a variety of different paths including through Telnet through the RS-232 port, Telnet through the Ethernet port, or through a monitor on the DVI-I interface in combination with a keyboard connected to the USB interface.

The WAGO IPCs are shipped with several different user names and default passwords.

- Root / wago
- Admin / wago
- User / user
- Guest /guest

The passwords for these login names must be changed to help secure your system. Note the login name and passwords are independent from the Web Based Management login name and passwords.

It is strongly recommend selecting passwords that will be difficult for someone to discover. The WAGO IPCs are optimized for using a minimum of 8 characters that include one or more of the following sets.

- Lower case alphabetic
- Upper case alphabetic
- Digits 0 thru 9
- Punctuation marks

5.2 Changing the Linux Console passwords

To change the passwords in the Linux Console, you must first connect to the IPC via one of the methods described in the overview section.

The next step is to log into the operating system. For the purpose of changing passwords, it is recommend to login as root.

At the login prompt type:

root

and then press enter. Next you will be asked for the password. Type in wago and press enter.

```
WAGO-IO-IPC login: root
Password:
root@WAGO-IO-IPC:~
```

The root and admin logins provide you with super user settings and therefore can change all the passwords at once.

Note that user and guest logins, can only change their own passwords.

Once you are logged in, you will see the prompt root@wago-IO-IPC. Now type:

passwd guest

and then press enter.

You will be prompted to enter the new password and also to confirm it a second time.

```
root@WAGO-IO-IPC:~ passwd guest
Changing password for guest
New password:
Retype password:
Password for guest changed by root
```

Now change the passwords for the user, admin and root logins, using the same process. For example to change the user password, type in:

passwd user

and the press enter at the command line.

6 Additional Security Features

There are many ways to help increase the security of an industrial control system. Several of these are outlined in section 7.

Limiting access to the control system will help reduce risks. The WAGO IPC offers several features that can help you reduce the access to the controller, thus limiting the risk of unwanted or unintended entry to the system.

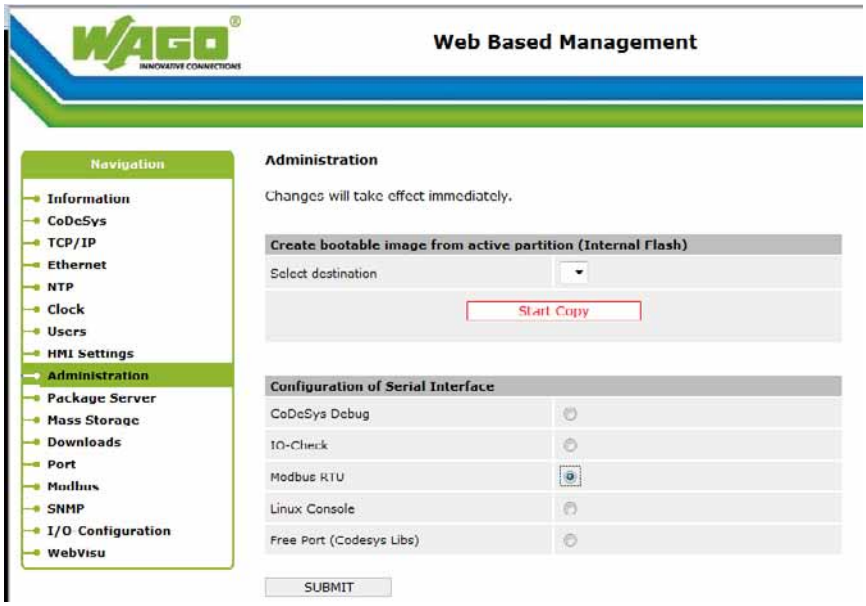
6.1 Limiting Access via the Serial Port

The WAGO IPC has an onboard RS-232 serial port that can be configured for multiple functions. The default of this port is set to Linux Console. With this setting the serial port can be used as a Telnet interface with a remote PC.

The serial port can be configured for other uses, thus blocking the port for Telnet operations. If this port is not intended to be accessed regularly as a Telnet port, then it is prudent to configure this for MODBUS RTU functions to reduce the risk of unwanted Telnet accesses.

The Telnet function of the serial port can be disabled by setting the use of the port to MODBUS RTU. This is accomplished through the Web Based Management page. The function can be found under the administration tab. Note that this page is password protected.

Once logged into the page, select the radio button next to the MODBUS RTU in the Configuration of Serial Interface section. Then click on SUBMIT.



6.2 Limiting Access via the Ethernet Ports

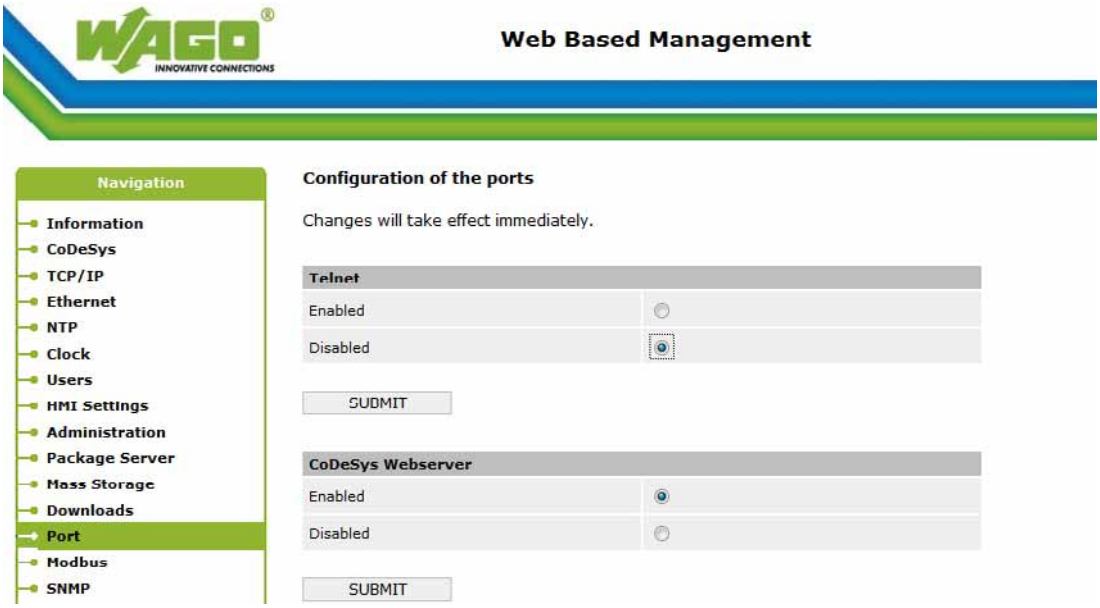
The WAGO IPC has two independent Ethernet ports onboard that can be used for a variety of functions. These functions can be limited via configuration, to help reduce the risk of unwanted access to the controller.

The WAGO IPC's Web Based Management is used to configure the use of these functions. The following configurations can be found on the "Port" page in the Web Based Management system. Note that this page is password protected.

6.2.1 Telnet

Most remote software tools used for Telnet applications can be configured to communicate either a serial connection or a TCP connection. Therefore it may be prudent to disable the Telnet function on the WAGO IPC.

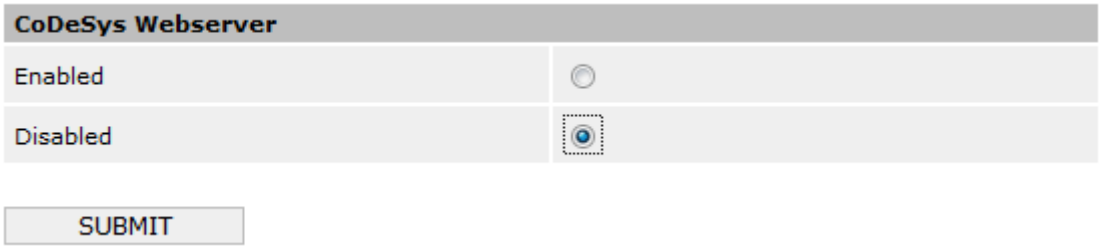
This may be accomplished via the Web Based Management "Port" page. In this tab you will find a section for Telnet configuration. By selecting the disable radio button and clicking on SUBMIT, you will block Telnet access via the Ethernet ports.



6.2.2 CoDeSys Web Server

The WAGO IPC has a built in web server that can be used to monitor and control your system. If this feature is not intended to be used in the system architecture, it can be disabled.

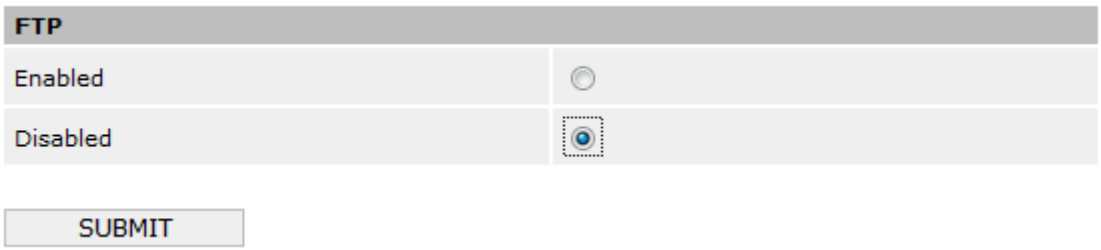
This may be accomplished via the Web Based Management “Port” page. In this page you will find a section for CoDeSys Webserver configuration. By selecting the disable radio button and clicking on SUBMIT, you will block access to / from the Webserver.



6.2.3 FTP Function

The WAGO IPC has the ability to transfer files to / from the device using FTP technology. If this feature is not intended to be used regularly in the system, it can be disabled.

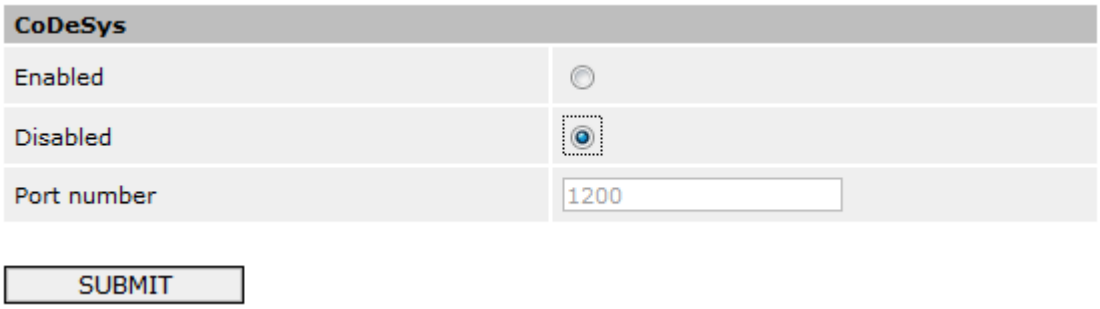
This may be accomplished via the Web Based Management “Port” page. In this page you will find a section for FTP configuration. By selecting the disable radio button and clicking on SUBMIT, you will block FTP access to / from the IPC.



6.2.4 CoDeSys

WAGO IPCs offer the powerful CoDeSys runtime. This allows you to program the IPC just like a programmable logic controller using the CoDeSys programming software. The developed program is typically downloaded via the Ethernet ports to the IPC. When the IPC's program is finalized, it may be prudent to disable CoDeSys access to the device to help prevent unwanted access.

This may be accomplished via the Web Based Management "Port" page. In this tab you will find a section for CoDeSys configuration. By selecting the disable radio button and clicking on SUBMIT, you will block CoDesys access to the IPC



7 Security recommendations

WAGO recommends that users of industrial control systems develop “Defense-In-Depth” practices to secure their assets. Defense-In-Depth is the implementation of multiple electronic and physical security techniques to help mitigate the risk of undesired access to control equipment and enhance overall system security. WAGO suggests you apply multiple technologies and complement them with your own company’s best practices. The following are some suggested control system security practices:

- Change the default passwords that are shipped with the devices to unique passwords and have a program to change the passwords on a regular basis.
- Enable user name and password protection on appropriate devices within your control system. Ensure only authorized personnel have access to this information and periodically change the passwords.
- Limit access to WAGO Ethernet networked controllers by disabling services available via the IP protocol. This can be accomplished through the device’s Web-based Management System’s Port tab. It is best to disable all services that are not required for normal operation.
- Locate control systems behind firewalls with intrusion detection and intrusion prevention technologies. These systems should be validated on regular basis to help ensure proper operation.
- Divide common control system architectures into zones to create clear boundaries in order to effectively apply multiple layers of defense. When possible, isolate the control system’s network from the corporate enterprise and external networks.
- Implement procedures that only allow trained and authorized people physical and electronic access to control systems.
- Develop well documented control system policies and procedures. Many of the same policies used for IT security and corporate systems could be applied directly to control system networks. The document should be reviewed annually to help ensure the best and latest security methods are in place.

Please contact WAGO’s technical support group at 1-800-DINRAIL if you have questions related to WAGO’s Ethernet based controllers and couplers.

WAGO Kontakttechnik GmbH
Postfach 2880 • D-32385 Minden
Hansastraße 27 • D-32423 Minden
Phone: 05 71/8 87 – 0
Telefax: 05 71/8 87 – 1 69
E-Mail: info@wago.com

Internet: http://www.wago.com