# SECURITY NOTES FOR CLASSIC PLCs

## Measures to protect devices based on classic control technology

Application note
110637_en_00



## 1 Introduction

Devices based on classic control technology are developed for use in closed industrial networks.

The following controllers are based on classic control technology in accordance with IEC 61131:

- Controllers of type ILC 1xx
- AXC 1050 (XC)
- AXC 3050
- Controllers of typy RFC 4xx
- FC 350 PCI ETH
- PC WORX SRT
- PC WORX RT BASIC

Device management and configuration for these devices are executed without authentication.

If you operate the devices in a public network, you must take organizational and technical measures to protect components, networks, and systems from unauthorized access and to ensure data integrity.

## 2 Recommended measures for devices and solutions

### 2.1 Do not integrate components and systems into public networks

- Avoid integrating your components and systems into public networks.
- If you have to access your components and systems via a public network, use a VPN (Virtual Private Network).

### 2.2 Set up a firewall

- Set up a firewall to protect your networks and the components and systems integrated into them against external influences.
- Use a firewall to segment a network or to isolate a controller.

Make sure you always use the latest documentation.
It can be downloaded at phoenixcontact.net/products.

### 2.3 Use a secure communication protocol

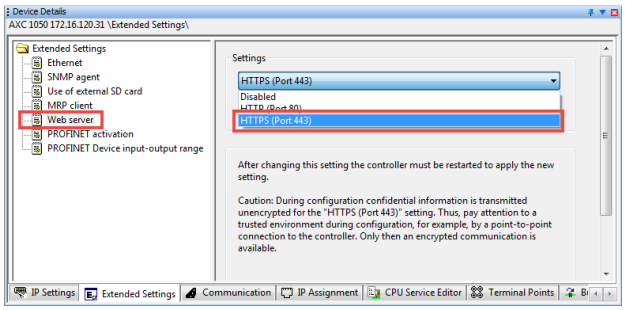
- Always use a secure communication protocol, if possible.
- Open your PC Worx application.
- Open the Bus Configuration workspace.
- Select the controller in the “Bus Structure” window.
- In the “Device Details” window, switch to the “Extended Settings” tab.
- Under “Extended Settings” select the “Web server” setting.
- Select “HTTPS (Port 443)” from the drop-down list.
- Click “Send” to transmit the setting to the controller.
- Restart the controller.

**NOTE: Unencrypted communication**

For the “HTTPS (port 443)” setting, confidential information is transmitted unencrypted during configuration. This puts data integrity at risk.

- Ensure a trusted environment during configuration (e.g., by using a point-to-point connection to the controller).

The encrypted communication does take effect until the controller is restarted.




### 2.4 Deactivate unneeded communication channels

- Deactivate all unneeded communication channels in the PC Worx software or via the WBM of the controller.

#### 2.4.1 (De)activating ports in PC Worx

The function is only available for the following controllers:

| Type | Item no. | From FW version |
|---|---|---|
| ILC 1x1 (alle Varianten) | – | 4.42 |
| ILC 151 GSM/GPRS | 2700977 | 4.42 |
| ILC 3xx (alle Varianten) | – | 3.98 |
| AXC 1050 | 2700988 | 3.01 |
| AXC 1050 XC | 2701295 | 3.01 |
| AXC 3050 | 2700989 | 5.60 |
| RFC 480S PN 4TX | 2404577 | 6.10 |
| RFC 470 PN 3TX | 2916600 | 4.20 |
| RFC 470S PN 3TX | 2916794 | 4.20 |
| RFC 460R PN 3TX | 2700784 | 5.00 |
| RFC 460R PN 3TX-S | 1096407 | 5.30 |

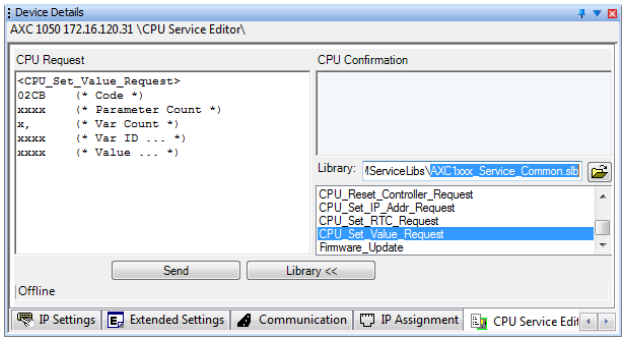
In the PC Worx software you (de)activate ports via the CPU_Set_Value_Request service.
A port is deactivated as soon as the corresponding service has been executed.
Activation of a port does take effect until the controller is restarted.

**Please note:**

If you deactivate port 1962 and/or port 41100, you will no longer be able to access the controller from PC Worx.
To reactivate port 1962 and/or port 41100 after deactivation, you must reset the controller to the default settings.
When you reset the controller to the default settings, the PC Worx application and all application-specific data is deleted.
**Exception:** AXC 1050 (XC) and AXC 3050
To reactivate port 1962 and/or port 4110 after deactivation, proceed as described in Section 2.4.2 “(De)activating ports in the WBM”.

### (De)activating ports

- Open your PC Worx application.
- Open the Bus Configuration workspace.
- Select the controller in the “Bus Structure” window.
- In the “Device Details” window, switch to the “CPU Service Editor” tab.
- Open the “[...]xx_Service_Common.slb" library for the device type used:
  – “ILC1xx_[...].slb” for ILC 1xx
  – “AXC1xx_[...].slb” for AXC 1050 (XC)
  – “AXC3xx_[...].slb” for AXC 3050
  – „RFC470_[...].slb“ for RFC 4xx
- Double-click to select the CPU_Set_Value_Request service.




- (De)activate the ports by entering “Var Count”, “Var ID” and “Value”.

The Var ID defines the port to be (de)activated.

### Port 7 (echo server)

| | | |
|---|---|---|
| Var Count | 1 | |
| Var ID | $0214_{hex}$ | |
| Value | $0000_{hex}$ | Deactivate port 7 |
| | $0001_{hex}$ | Activate port 7 |

### Port 21 (FTP access)

| | | |
|---|---|---|
| Var Count | 1 | |
| Var ID | $0172_{hex}$ | |
| Value | $0000_{hex}$ | Deactivate port 21 |
| | $0001_{hex}$ | Activate port 21 |

### Port 1962 (communication with PC Worx)

| | | |
|---|---|---|
| Var Count | 1 | |
| Var ID | $0213_{hex}$ | |
| Value | $0000_{hex}$ | Deactivate port 1962 |
| | $0001_{hex}$ | Activate port 1962 |

### Port 41100 (OPC and debug mode in PC Worx)

| | | |
|---|---|---|
| Var Count | 1 | |
| Var ID | $0192_{hex}$ | |
| Value | $0000_{hex}$ | Deactivate port 41100 |
| | $0001_{hex}$ | Activate port 41100 |

- Click „Send“ to send the settings to the controller.

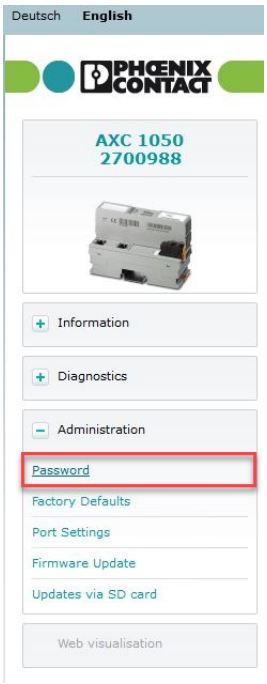
### 2.4.2 (De)activating ports in the WBM

The function is only available for AXC 1050 (XC) controllers from firmware version 5.00 and AXC 3050 controllers from firmware version 6.30.

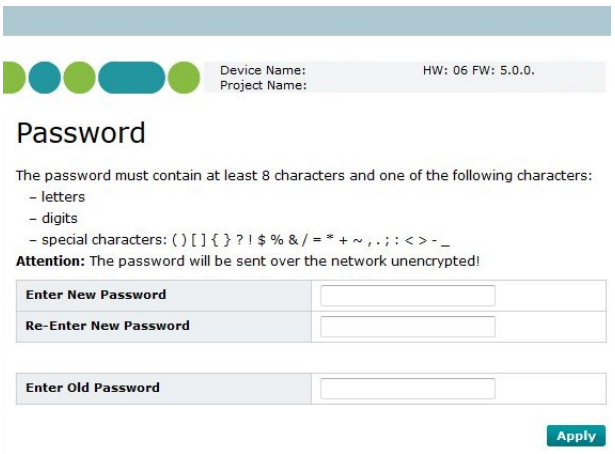
In the Web-based Management (WBM) of the controller you (de)activate ports via the “Port Settings” page.
A password is required to (de)activate ports.

#### Assigning a password

- Open the WBM.
- In the “Administration” area, open the “Password” page.



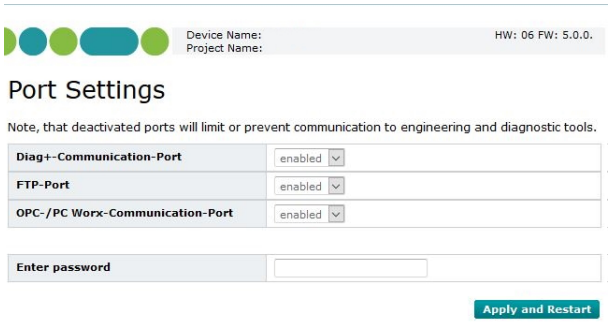

- Enter the desired password in the “Enter New Password” and “Re-Enter New Password” input fields.
- Enter the current password in the “Enter Old Password” input field (default: “private”).
- Click “Apply” to save the new password.




#### (De)activating ports

- In the “Administration” area, open the “Port Settings” page.


- To (de)activate a port, select the entry “deactivated” or “activated” in the corresponding drop-down list.
- Enter your password in the “Enter password” input field.
- Click “Apply and Restart” to apply the changed port settings.



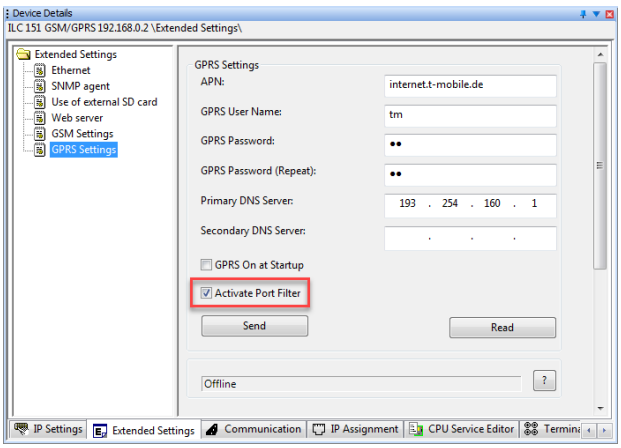

## 2.5 ILC 151 GSM/GPRS: Use port filter and SIM service with VPN

Note when using GPRS:

- Enable the port filter in PC Worx.
- Use a SIM service with VPN (e.g. CDA).

To activate the port filter in PC Worx, proceed as follows:

- Open your PC Worx application.
- Open the Bus Configuration workspace.
- Select the controller in the “Bus Structure” window.
- In the “Device Details” window, switch to the “Extended Settings” tab.
- In the “Device Details” window, select the “GPRS Settings” setting under “Extended Settings”.
- Activate the “Activate Port Filter” check box.
- Click „Send“ to send the settings to the controller.




If the port filter is activated, ports 0 ... 2000 (exception: port 80) and port 41100 are blocked.

## 2.6 Take Defense-in-Depth strategies into consideration when planning systems

It is not sufficient to take measures that have only been considered in isolation when protecting your components, networks, and systems. Defense-in-Depth strategies encompass several coordinated measures that include operators, integrators, and manufacturers.

- Take Defense-in-Depth strategies into consideration when planning systems.

## 2.7 Restrict access rights

- Restrict access rights for components, networks, and systems to those individuals for whom authorization is strictly necessary.
- Deactivate unused user accounts.

### 2.8 Secure access

- Change the default password in the WBM after initial startup.
- Use a secure password reflecting the complexity and service life recommended in the latest guidelines.
- Change the password in accordance with the rules applicable for your application.
- Use a password manager with randomly generated passwords.

### 2.9 Use secure access paths for remote access

- Use secure access paths such as VPN (Virtual Private Network) or HTTPS for remote access.

### 2.10 Use the latest firmware version

Available firmware updates can be found on the product page of the respective device.

- Ensure that the firmware of all devices used is always up to date.
- Observe the Change Notes for the respective firmware version.
- Pay attention to the security advisories published on Phoenix Contact's Product Security Incident Response Team (PSIRT) website regarding any published vulnerabilities.

### 2.11 Use up-to-date security software

- Install security software on all PCs to detect and eliminate security risks such as viruses, trojans, and other malware.
- Ensure that the security software is always up to date and uses the latest databases.
- Use whitelist tools for monitoring the device context.
- Use an Intrusion-Detection system for checking the communication within your system.

To protect networks for remote maintenance via VPN, Phoenix Contact offers, for example, the mGuard product range of security appliances, see phoenixcontact.net/products.

### 2.12 Perform regular threat analyses

To determine whether the measures you have taken still provide adequate protection for your components, networks, and systems, threat analyses should be performed regularly.

- Perform a threat analysis on a regular basis.

### 2.13 Secure access to SD cards

Devices with SD cards require protection against unauthorized physical access. An SD card can be read with a conventional SD card reader at any time. If you do not protect the SD card against unauthorized physical access (such as by using a secure control cabinet), sensitive data is accessible to all.

- Ensure that unauthorized persons do not have access to the SD card.
- When destroying the SD card, ensure that the data cannot be retrieved.

# 3 Recommended measures for PC-based software

PC-based software is used, for example, to set up, configure, program, and monitor devices, networks, and solutions.

Engineering software can manipulate the device or solution.

- To reduce the risk of manipulation, perform security evaluations regularly.

## 3.1 PC-based hardening and organization measures

Protect any PCs used in automation solution environments against security-relevant manipulations. This can be facilitated, for example, by taking the following measures:

- Boot up your PC regularly, and only from data carriers that are secured against manipulation.
- Set up restrictive access rights for any personnel that absolutely must have authorization.
- Protect your systems against unauthorized access with strong passwords and with rules to ensure that they remain strong.
- Deactivate unused services.
- Uninstall any software that is not used.
- Use a firewall to restrict access.
- Use whitelist tools to protect important directories and data against unauthorized changes.
- Activate security-relevant event logging in accordance with the security directive and the legal requirements on data protection.
- Activate the update feature in accordance with the security directive.
- Activate the automatic screen lock function and automatic logout after a specified time.
- Perform backups regularly.
- Only use data and software from approved sources.
- Do not follow any hyperlinks listed that are from unknown sources, such as emails.

## 3.2 Use the latest software

- Always use the latest software version (for engineering software, operating systems, etc.).
- Check for any software updates available on the respective product page from Phoenix Contact.
- Observe the Change Notes for the respective software version.
- Pay attention to the security advisories published on Phoenix Contact's Product Security Incident Response Team (PSIRT) website regarding any published vulnerabilities.

## 3.3 Use up-to-date security software

- Install security software on all PCs to detect and eliminate security risks such as viruses, trojans, and other malware.
- Ensure that the security software is always up to date and uses the latest databases.

# 4 Phoenix Contact security advisories

## 4.1 Product Security Incident Response Team (PSIRT)

The Phoenix Contact Product Security Incident Response Team (PSIRT) gathers and analyzes any potential security vulnerabilities in Phoenix Contact products, solutions, and services. If a security vulnerability is identified, it will be listed on the PSIRT website under "Recent security advisories", and a corresponding security advisory will be published. The website is updated regularly.

To stay up to date, Phoenix Contact recommends subscribing to the PSIRT newsletter (under "GETTING UPDATES FROM PHOENIX CONTACT PSIRT", "Subscribe to PSIRT news").

Anyone can submit information on potential vulnerabilities to Phoenix Contact PSIRT via email.

The aim of PSIRT is to work with vulnerability reporters professionally to handle any vulnerability claim that is related to Phoenix Contact products, solutions, and services.