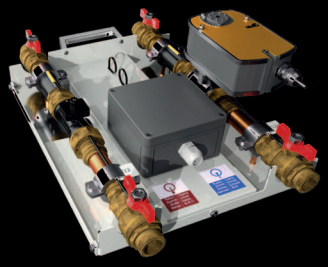
Rittal – The System.

Faster – better – everywhere.

LCP Rear Door CW





Active module

3314.020

3314.025

System Hardening Guide

EN

Contents

1 Overview 3
1.1 What is system hardening? 3
1.2 Goal of system hardening 3
1.3 Purpose of the document 3
1.4 Scope 3

2 Initial setup 3
2.1 Change the default password 3
2.2 Use secure passwords 3
2.3 Protect USB ports against access 3
2.4 Keep to the software up to date 3

3 Services 4
3.1 Time synchronisation 4
3.2 Disable HTTP and set up HTTPS 4
3.3 Disable FTP and enable FTPS only when needed 4
3.4 Disable Telnet 4
3.5 Disable SNMPv1/v2 and use SNMPv3 securely only when needed 4
3.6 Secure use of Modbus TCP only when required 5
3.7 Secure use of OPC UA only when required 5

4 Logging settings 5

5 Access and authorisation 5

6 Network and security 6
6.1 Keep the firmware of networked devices up to date 6
6.2 Do not connect products and systems to public networks 6
6.3 Use up-to-date security software 6
6.4 Perform regular threat analysis 6

7 Quick Hardening Checklist 6

EN

1 Overview

1.1 What is system hardening?

The German Federal Office for Information Security (BSI) defines hardening in IT security as: "…the removal of all software components and functions that are not absolutely necessary to fulfil the intended purpose of the program".

In other words: System hardening aims to eliminate attack vectors by patching vulnerabilities and disabling unnecessary services.

1.2 Goal of system hardening

The primary objectives of system hardening are to reduce the opportunities for exploiting vulnerabilities and to minimize possible attack methods. As a side effect, hardening often leads to reduced complexity and, consequently, a decrease in administrative errors.

Products, networks, and systems must be protected against unauthorized access to ensure the availability, confidentiality, and integrity of data.

1.3 Purpose of the document

The guidelines below aim to establish a secure configuration for the Rittal LCP Rear Door CW.

This document is intended for system and application administrators, security specialists, auditors, and helpdesk personnel responsible for securing the LCP Rear Door CW.

For additional information, please refer to the official website of the German Federal Office for Information Security (BSI):

– **BSI - IT-Grundschutz-Kompendium**
– **BSI - Allgemeine Empfehlungen**

1.4 Scope

The described measures primarily relate to the secure operation of the LCP Rear Door CW within a network, as well as to its local and network-based interfaces.

2 Initial setup

As a general rule, disable all unnecessary communication channels on the device. For many protocols, more secure alternatives are available—we strongly recommend consistently disabling insecure variants. In some cases, the security level can be further increased through appropriate configuration settings.

To define suitable protective measures, it is helpful to obtain a complete overview of all existing communication paths and interfaces, as these may represent potential attack surfaces.

2.1 Change the default password

Description:

Similar to routers, our LCP Rear Door CW also uses a default password that can be used to access the devices during initial setup. If the factory-set password remains unchanged, the attack surface is conveyable large.

Recommendation:

Default passwords are kind of a placeholder and should only be used during initial configuration. Admins and users should always change the default password during the initial configuration to reduce the risk.

Remedy:

Starting from software version V8.23.00, users are prompted to set a new and secure password upon their first login. If a different software version is in use, further information can be found in the LCP Rear Door CW operating manual, chapter 7.2.2.

2.2 Use secure passwords

Description:

Hackers have tools to automatically try out all possible character combinations, test entire dictionaries including common combinations of words and attached numbers, or try out access data once published on the internet for all possible services. To prevent this, a password should meet certain quality requirements and should only be used for one account.

Recommendation:

Follow the recommendations of the German Federal Office for Security and Information Technology for creating and handling passwords.

2.3 Protect USB ports against access

Description:

USB-based malware is a simple and common method for network infiltration and often represents the first step in establishing a persistent threat within a network environment.

Recommendation:

Restricting USB access on the system reduces the physical attack surface of the device and thus the risk of malware being introduced. Do NOT expose any ports externally (e.g., outside a locked enclosure), as this poses a major security risk.

Remedy:

Ensure that unauthorized persons do not have access to the USB ports and that these ports are disabled when not in use.

2.4 Keep to the software up to date

Description:

Up-to-date software reduces the time window in which known vulnerabilities can be exploited and decreases the overall attack surface. In addition, newer versions often include additional security features that were not present in older versions.

EN

Recommendation:
Whenever possible, update the software to the latest version.

Remedy:
The latest software release is available via the LCP Rear Door CW product page or through our service. Instructions for performing an update can be found in the LCP Rear Door CW operating manual, chapter 8.6.

3 Services

3.1 Time synchronisation

Description:
The system time should be synchronized across all systems within an environment. This is typically achieved by setting up an authoritative time server or a group of servers with which all systems synchronize their clocks.

Recommendation:
Time synchronization is important to support time-dependent security mechanisms and to ensure that log files across the entire organization have consistent timestamps, which is helpful for forensic investigations.

Remedy:
Establish a connection to an NTP server, if one is in use in your system. Instructions for activating and configuring a connection to an NTP server can be found in the LCP Rear Door CW operating manual, chapter 8.6.

3.2 Disable HTTP and set up HTTPS

Description:
The Hypertext Transfer Protocol (HTTP) and the Hypertext Transfer Protocol Secure (HTTPS) are used for communication between web browsers and networked devices, for example to provide user interfaces or configuration options.

Recommendation:
HTTP is inherently insecure, as data—including login credentials—is transmitted unencrypted and can therefore be intercepted or manipulated by attackers.
It is strongly recommended to use HTTPS exclusively. Additionally, it should be ensured that HTTPS is operated with a current and secure configuration—this includes using the security level "Modern", which utilizes TLS 1.3.

Remedy:
Disable HTTP in the device settings and enable HTTPS exclusively with the security level "Modern". Detailed instructions can be found in the LCP Rear Door CW operating manual, chapter 8.6.

3.3 Disable FTP and enable FTPS only when needed

Description:
The File Transfer Protocol (FTP) and the Secure File Transfer Protocol (SFTP) allow networked computers and devices to transfer files.

Recommendation:
FTP is generally insecure because passwords are transmitted in plain text, completely unencrypted. It is therefore recommended to use SFTP when file transfer is required. Once SFTP is no longer needed, it should also be disabled to reduce the attack surface.

Remedy:
Disable FTP and SFTP in the settings and enable them only during active use. Instructions can be found in the LCP Rear Door CW operating manual, chapter 8.6.

3.4 Disable Telnet

Description:
The Telnet protocol can be used to establish connections to other systems. It enables remote communication but transmits all data in an unencrypted format.

Recommendation:
Telnet is considered insecure because it does not provide encryption for transmitted data. As a result, there is a risk that login credentials and other sensitive information can be intercepted and misused by unauthorized parties. Its use should therefore generally be avoided.

Remedy:
Disable the Telnet protocol in the device settings unless it is strictly required. Instructions for disabling it can be found in the LCP Rear Door CW operating manual, chapter 8.6.

3.5 Disable SNMPv1/v2 and use SNMPv3 securely only when needed

Description:
The SNMP server (Simple Network Management Protocol) is used to listen for SNMP commands from an SNMP management system, execute those commands or collect information, and then return the results to the requesting system.

Recommendation:
The SNMP server can communicate using SNMPv1/v2c or v3. However, versions v1/v2c are insecure. For example, SNMPv1 transmits data in plain text and does not require authentication to execute commands. It is strongly recommended to configure the server so that SNMPv1/v2c is not permitted.

In the current implementation, authentication is performed using MD5 or SHA-1, both of which are considered outdated and have known weaknesses. Encryption is performed using DES or AES, with DES also considered outdated and insecure.
Therefore, usage should only take place within trusted and secured networks.

Remedy:
Disable SNMP v1/v2c in the settings and enable SHA authentication and AES encryption in the SNMPv3 configuration. It is also recommended to define all hosts that are allowed to access the device via SNMP in the "Allowed Hosts" section and to change the default SNMP community string "public". If the "Allowed Hosts" list is empty, all systems can communicate with the device via SNMP. Assign the required permissions (either read or read/write) to the "Allowed Hosts". Further instructions can be found in the LCP Rear Door CW operating manual, chapter 8.6.

3.6 Secure use of Modbus TCP only when required

Description:
Modbus TCP is a widely used communication protocol in industrial automation for transmitting control and process data over IP-based networks.

Recommendation:
By default, Modbus TCP does not offer built-in security mechanisms such as authentication or encryption. As a result, data can be transmitted in plain text and potentially read or manipulated by unauthorized third parties. It is therefore recommended to enable Modbus TCP only when absolutely necessary. Additionally, appropriate security measures such as network segmentation, firewalls, or VPN connections should be implemented to restrict access to trusted systems.

Remedy:
Disable Modbus TCP if it is not actively required. If its use is necessary, ensure that access is restricted via the allowed hosts list. If the "Allowed Hosts" list is empty, all systems can communicate with the device via Modbus TCP. Assign the required permissions (either read or read/write) to the "Allowed Host". Further information on configuration can be found in the LCP Rear Door CW operating manual, chapter 8.6.

3.7 Secure use of OPC UA only when required

Description:
OPC UA (Open Platform Communications Unified Architecture) is a platform-independent communication protocol for secure and reliable data exchange in industrial applications.

Recommendation:
In the present implementation, the only available security mechanism is authentication via username and password, without additional encryption of the transmitted data.
As a result, there is a risk that communication content may be intercepted or manipulated within the network. It is therefore recommended to use OPC UA only in trusted and appropriately secured network environments.

Remedy:
Enable OPC UA only when required for operation and restrict access to authorized users by using strong credentials.
Use the protocol exclusively in secured network environments and limit access through appropriate network measures. Additional measures such as network segmentation, firewalls, or VPN connections should be used to further secure communication.
Instructions for configuration can be found in the LCP Rear Door CW operating manual, chapter 8.6.

4 Logging settings

Description:
The LCP Rear Door CW generates logs of events and statuses and stores them on the device. For example, login and logout events are recorded, which can provide a system administrator with information about brute-force attacks on user accounts.
In a network environment with many different applications and systems, a large amount of complex information is typically generated, which can be difficult for administrators to evaluate and review.

Recommendation:
In this case, use a Syslog server or dedicated logging software that collects and archives all relevant information in a central location. Ensure that TLS is enabled to guarantee that all data records are encrypted and that TCP is activated to ensure reliable data transmission.

Remedy:
Instructions for configuring basic settings for sending log messages to a Syslog server can be found in the LCP Rear Door CW operating manual, chapter 8.6.

5 Access and authorisation

Description:
Efficient user management protects IT systems and data from unauthorized access and assigns each user a unique identity.

Recommendation:
Whenever possible, use an external user management system (LDAP or RADIUS), or create a user account

EN

on the device for each user who requires authorization, along with an associated user group. Keep user accounts and user groups up to date and disable any unused accounts.
Also define the necessary permissions for user accounts based on their roles and responsibilities.
Users belonging to a group with the administrator role enabled have unrestricted access via the web interface to the entire device configuration and all settings. They can modify them at any time.
For this reason, it is strongly recommended to keep the number of administrators to a minimum.
Users with data transfer permissions have access to all stored data and can modify it if write access is enabled – regardless of their assigned group.

Remedy:
Instructions for configuring basic settings for user groups, individual users, or user management systems can be found in the LCP Rear Door CW operating manual, chapter 8.6.

6 Network and security

6.1 Keep the firmware of networked devices up to date

Ensure that the latest firmware is installed on the devices, as it patches known security vulnerabilities and may also provide additional functionality. The firmware can be found on the product page of the respective device.

6.2 Do not connect products and systems to public networks

Do not operate the system directly on the internet, but only within internal networks that are protected externally by firewalls. If it is necessary to integrate your products and systems via a public network, use a VPN.

6.3 Use up-to-date security software

Security software should be installed on all PCs and kept up to date in order to identify and eliminate security risks such as viruses, trojans, and other malware.

6.4 Perform regular threat analysis

It is recommended to carry out regular threat analyses to determine whether the implemented protective measures are effective.

7 Quick Hardening Checklist

System Hardening
– All unnecessary services are disabled
– USB ports are disabled or physically protected and not exposed externally

Access & Authentication
– Default password has been changed
– Strong, individual passwords are used
– Unused user accounts are disabled
– The number of administrators is kept to a minimum
– User account permissions are restricted to the minimum required
– External user management system is integrated

Network & Data Transmission
– HTTP is disabled
– HTTPS is enabled (with the security level "Modern")
– FTP is disabled
– SFTP is enabled only when needed
– Telnet is enabled only when needed

Services & Protocols
– SNMPv1/v2c is disabled
– SNMPv3 is properly configured and enabled only when required, and used exclusively in secured networks.
– Modbus TCP is properly configured and enabled only when required, and used exclusively in secured networks.
– OPC UA is properly configured and enabled only when required, and used exclusively in secured networks.

Logging & Monitoring
– Connection to an NTP server is established
– Logging is enabled
– Logs are sent to a central Syslog server
– TLS for log transmission is enabled

Network Security
– Access is restricted via firewall
– Network segmentation is implemented
– The device is not directly accessible from the internet
– Access is limited to defined "Allowed Hosts" via Modbus TCP and SNMPv3

Operation & Maintenance
– Software is up to date
– Regular threat analyses are performed
– Security software is active on connected systems
– External access is carried out exclusively via VPN

Notes

Rittal – The System.

Faster – better – everywhere.

- Enclosures
- Power Distribution
- Climate Control
- IT Infrastructure
- Software & Services

You can find the contact details of all
Rittal companies throughout the world here.

www.rittal.com/contact

RITTAL GmbH & Co. KG
Auf dem Stuetzelberg · 35745 Herborn · Germany
Phone +49 2772 505-0
E-mail: info@rittal.de · www.rittal.com

06.2025/System Hardening Guide LCP Rear Door CW/V1.0 EN