HIRSCHMANN

A BELDEN BRAND

User Manual

Security
MICE Switch Power MSP40
HiOS-3A-UR

UM Security MSP40 HiOS-3A-UR
Release 10.0 04/2025

Technical support
https://hirschmann-support.belden.com

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2025 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You find the latest user documentation for your device at: doc.hirschmann.com

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany

Contents

Safety instructions

⚠ WARNING

UNCONTROLLED MACHINE ACTIONS

To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.

Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Safety information

⚠ WARNING

WARNING indicates a potentially hazardous situation which, if not avoided, **can result in** death or serious injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

About this Manual

The “Configuration” user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

The “Installation” user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

The “Graphical User Interface” reference manual contains detailed information on using the graphical user interface to operate the individual functions of the device.

The “Command Line Interface” reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The “Device Security and Network Security Support” user manual contains an introduction, considerations for system security planning, and policy development, and an enumeration of device security measures. It also suggests how a secured device can assist in both securing and improving the availability of your network. Furthermore, password strength and specific mitigation measures are discussed, completed with a guide to password policy.

The Industrial HiVision Network Management software provides you with additional options for smooth configuration and monitoring:

- Auto-topology discovery
- Browser interface
- Client/server structure
- Event handling
- Event log
- Simultaneous configuration of multiple devices
- Graphical user interface with network layout
- SNMP/OPC gateway

Key

The designations used in this manual have the following meanings:

• Item	General list item
– Sub-item	Sublist item
▶ Item	Parameter value item
□	Work or planning step
ⓘ	Marks a reference to an external user or reference manual.
⚠	The delivery state of the setting preceding the icon may be considered insecure.
Link	Cross-reference with link
Note:	A note emphasizes a significant fact or draws your attention to a dependency.
Boldface	Marks a key concept introduced for the first time.
"Chapter 1 > Chapter 1.1"	Practical reference to a chapter and sub-chapter in an external user manual or reference manual
[CR…][1]	Formal reference to an IEC 62443-4-2 Component Requirement
[CR…RE…][1]	Formal reference to the Requirement Enhancement of an IEC 62443-4-2 Component Requirement
[NDR…][1]	Formal reference to an IEC 62443-4-2 Network Device Requirement
<SL-C…>[2]	Formally marks content that relates to IEC 62443 Security Capability Level 2 (SL-C2) or higher. For example, <SL-C2> marks content that conforms to SL-C2.
[SR…][1]	Reference to an IEC 62443-3-3 System Requirement
[SR… RE…][1]	Formal reference to the Requirement Enhancement of an IEC 62443-3-3 System Requirement

[1] If a formal reference to the standard appears at the beginning of a chapter, it applies to the whole chapter. If a reference appears at the beginning of a paragraph or list item, it applies only to the respective paragraph or list item. If a reference appears in a comma-separated list, it applies only to the item tagged with the reference.

[2] If a formal reference to the SL-C level appears at the end of the of a chapter headline, it applies to the whole chapter. If a reference appears at the end of a sentence (before the period), it applies only to the respective sentence.

Synopsis

This document deals with how to achieve and improve the security of an industrial communication network using the IEC 62443 "Security of Industrial Automation and Control Systems" series of standards as a framework.

The general security level addressed in this document is the IEC 62443 Capability Security Level 1 (SL-C1). Content conforming to SL-C1 is not marked up. However, content conforming to SL-C2 is marked up with <SL-C2>.

The chapter "Security Planning" (see on page 15 “Security planning”) introduces the subject, describes required preparatory work, explains some key concepts, and gives a hierarchy of hardware and software measures. It also describes the interdependence of device, network and system requirements, and details the required planning steps, resulting in a collection of policies.

The chapter "Device security in the life cycle phases" (see on page 55 “Device security in the life cycle phases”) details particular measures and steps to help secure a network device, based on the policies developed in the planning chapter.

The chapter "Network security support" (see on page 99 “Network security support”) describes particular measures to set up a network device to help support the security and availability of the network. The prerequisite is that the device itself has been secured. ACL setup is described extensively.

The Appendix "Security seal" (see on page 119 “Security seal”) deals with the mechanical security methods of the device, their security properties, signs of tampering, the recommended procedures for checking the seals, and the recommended decommissioning procedure.

The Appendix "Password strength and policy guide" (see on page 123 “Password strength and policy guide”) (informational only) deals with password strength, explains key concepts like password classes, password policies, password schemes, the strengths and weaknesses of password classes, shows how to calculate and improve the provided attack resistance time, shows how to calculate the required password entropy for an effective mitigation, and finally offers to look up a password policy that satisfies the desired level of attack resistance.

Audience

This security user manual primarily addresses Ethernet network planners, commissioners, administrators, operators, maintainers, and decommissioners.

The contents may also be useful for solution providers, sales partners, and system integrators.

1 Security planning

1.1 Basics

If you are new to security for industrial networks, you may find this chapter a good start. **The main security terms and concepts are set in boldface.**

1.1.1 Security terminology

The term "Security" typically can be subdivided into the following aspects.

Table 1: Aspects of security

Aspect	Description
Confidentiality	Only authorized entities have read access to specified information or devices.
Integrity	Only authorized entities have write or modify access to specified information. For devices, only authorized entities have the privileges to set up specified devices, and to install or update device software.
Availability[1]	Only authorized entities have the privileges to delete, modify, or deny access to specified information, or to remove or disable specified devices.
Authenticity	Specified information contains proof of which entity created or modified the specified information, or which entity installed, set up or a updated specified device.
Nonrepudiability[2]	Authenticated information or devices can be traced to the entity that created or modified the information, or updated or set up a device. This entity then cannot plausibly deny its creatorship.

[1] Availability can be regarded as a part of integrity.

[2] Nonrepudiability can be regarded as a part of authenticity.

Note:
Depending on your actual situation, some or all of the above aspects must be satisfied to consider a situation secure.

Example for confidentiality and integrity

For management of the device, the device offers different user account roles. These roles offer different degrees of access. This helps control confidentiality and integrity.

Table 2: Example for confidentiality and integrity, based on user account roles

User account role	Description	Security consequences
`unauthorized`	A user with this account role cannot log into the device.	Device management data remains confidential and integer.
`guest`	A user with this account role can log into the device to read data, except the audit trail. The user does not have write access to any data.	This user account role can read confidential data. Integrity is provided by read-only access.
`auditor`	A user with this account role can log into the device to read data, including the audit trail. The user can write the audit trail to a log file.	This user role can read confidential data. Integrity is provided by the immutable audit trail in the device.
`operator`	A user with this account role can log into the device to read and write device management data. Access to security-relevant settings and the audit trail is read-only.	This user role can read and write confidential data. Integrity is provided by read-only access to security settings and the immutable audit trail.
`administrator`	A user with this account role can log into the device to read and write data, including security-relevant settings. This role can also read the audit trail.	This user role can read and write confidential data. Integrity is provided by the immutable audit trail in the device

More terms

Most of the terms in the following table are used and explained in more detail in the remainder of this main chapter.

Table 3: Security terms

Aspect	Description
Vulnerability	A flaw or weakness of a system. Vulnerabilities can be unintentional (like an unintended software problem), or they can be unavoidable (like a system that offers a login). The union set of all vulnerabilities of a system is called an attack surface.
Threat	A potentially negative action, event, or circumstance that results in an unwanted impact to a system. A threat is related to a specific vulnerability of the system. A threat can be deliberate or accidental.
Threat model	A threat model is a model that defines the logical borders of a given asset, and the conditions under which threats are assumed. By defining these fundamental conditions, a threat model enables the reasonable, structured collection and description of perceivable threats. The outcome of a threat model is a threat collection.
Threat collection	A threat collection is the outcome when perceivable threats are applied to a threat model. It lists the perceivable threats that are deemed applicable to the threat model. It contains all collected threats, regardless of their exploitability, exploit severity, or their associated mitigation effort or effectiveness.
Threat profile	A threat profile is a threat collection ordered by threat risk, the combined treat/ mitigation criticality, or other, appropriate criteria.

Table 3: Security terms

Aspect	Description
Threat risk	The combination of both the degree of exploitability of a given threat and the severity of the results if the threat is applied to the system. The easier a threat can be exploited and the more severe its results, the higher the threat risk.
Mitigation	A process or action of countermeasure with the goal to thwart or attenuate a threat risk, either by lowering the exploitability of the threat or to diminish its results. Mitigation can be seen as part of vulnerability management.
Mitigation efficiency	The degree to which a given mitigation measure thwarts or attenuates a threat risk. It consists of the mitigation’s effort and effectiveness. The lower the effort to implement a mitigation measure and the higher the effectiveness of the mitigation measure, the higher the mitigation effectiveness.
Criticality	The criticality applies to a specific threat risk in conjunction with a specific mitigation measure’s efficiency. The higher the threat risk and the lower the associated mitigation’s efficiency, the more critical this combination is.

1.1.2 Convenience vs. security: Navigating the field of tension

On a qualitative level (that is, not using a structured approach), the concepts of security and convenience are often seen as contradicting each other. As an example, consider a database that stores personal data, for example, of customers.

Convenience trumps security: If access to the database requires only one user name for any database user and requires only a trivial password for login:
- Such a system is convenient for the database users.
- At the same time, it is highly insecure because the confidentiality of the personal data is insufficient.

Security trumps convenience: If access to the database requires individual, hard-to-remember user names and enforces the use of system-generated, long and truly random passwords for login:
- Such a system is considerably inconvenient for the database users.
- At the same time, it can be regarded as highly secure because the confidentiality of the personal data is well protected.

In practice, often none of the above given extreme examples are feasible.

As a consequence, security planning needs an impartial approach, and should be based on metrics. This approach enables you to weigh threats against mitigation measures, helps you attain a reasonably secure system and also provides you with detailed, comprehensible points for your chosen mitigation measures.

Security is weighed against usability: If access to the database requires individual but short user names and allows memorable and user-chosen passwords according to an enforced password policy for login:
- This system can be seen as acceptable (convenient enough) for the database users.
- At the same time, it can be regarded as reasonably secure because the confidentiality of the personal data is appropriately protected.

Whitelist approach

In the context of network security, a whitelist approach is an implementation of the concept "Security trumps convenience", refined by the concept "Security is weighed against usability".

A whitelist approach means that only those network device functions shall be enabled that are clearly necessary for the network to function properly. All other device functions shall be disabled.

The functions that need to be disabled may include functions that are enabled in the factory setting, i.e., in a device out-of-the box. Therefore, plan a necessary function policy.

1.1.3 Skepticism vs. optimism: qualitative security philosophy

When considering security aspects and the associated concepts of threat risks and mitigation efficiency, people can be associated with two groups:

- **People with experience in security often tend to be conservative (skeptical)**, that is, they tend to give higher weight to security aspects and lower weight to convenience or usability aspects. The reason for that is that security considerations often involve examining seemingly uncritical details that can reveal unexpected threats, surprisingly high risks and unfortunately poor mitigation efficiency, possibly leading to the discovery of several critical, and as-yet, unmitigated vulnerabilities.
  - In a qualitative way, that is, not using a structured approach at all, this can be seen as leading to higher security but can sometimes also lead to poorer convenience or even usability.
- On the other hand, **people mainly concerned with usability and convenience, tend to be optimistic**, that is, they focus on convenience while at the same time tend to overlook the security aspects of a system. The reason for that is that convenience considerations aim at minimizing the effort (for example, cognitive load) for a user which in turn can unintentionally create or exacerbate vulnerabilities (exploitable threats) in a system.
  - In a qualitative way, that is, not using a structured approach at all, this can be seen as leading to good usability but can sometimes also lead to poor security.

As a consequence, a structured security approach that takes both aspects into account is indispensable.

1.1.4 Impartial assessment

To get an impartial overview over the security of a given or a planned system, an analysis is mandatory. This analysis typically consists of collecting the perceivable threats, based on a threat model, followed by an assessment of the individual threat risks.

This is typically followed by a collection and then an assessment of the available or perceivable mitigation measures.

The risk of a given threat can be combined with the efficiency of the respective mitigation. This combination can be regarded as a criticality value. This value can guide the priority with which a given threat/mitigation combination shall be pursued and also which mitigation strategy shall be employed.

1.1.5 Threat analysis

A thorough and reasonable security concept can only be developed when the threats to the asset under consideration are both known and assessed to a reasonable degree.

In practice, the threats are modeled and assessed in 2 steps:

- **Develop a threat model** that defines the conditions that in turn help collect and describe the conceivable threats to your system as completely as possible.
  - **The result is a threat collection.**
- **Develop a threat assessment concept** that defines how to assess the collected threats individually and assign a risk to each threat.
  - **The result is a threat profile.**

Note:
Without a threat model, the threat collection is prone to be incomplete, possibly leaving high-risk threats undiscovered.
Without a threat assessment, the threat profile, although possibly complete, is prone to assign unreasonable ad-hoc weight to individual threats. This may result in both high-risk threats going unmitigated as well as unreasonable effort going into the mitigation of minor threats. It also impairs the development of mitigation strategies.

1.1.6 Mitigation: confidentiality example

Confidentiality is often one of the most important aspects of security. It can be regarded as the property of a system or system component permitting or denying read access to an entity.

Confidentiality can be implemented by erecting one or more barriers for an unauthenticated entity. An unauthenticated entity must first identify and also authenticate itself toward a system that guards the confidential information. Only after the entity is regarded as authenticated, the system allows read access.

Typical mitigation measures (each implementing a barrier) can be:

- Compulsory identification (demanding a username).
- Compulsory authentication (demanding a password associated with the username).
- Measures that impede brute-force attacks, for example, by denying login access attempts for a given time after a number of successive failed login attempts.
- Possible additional measures to restrict login attempts to, for example, certain ports, VLANs, management protocols or IP source addresses.

As a consequence, develop an assessment for mitigation measures, and assign an efficiency to the individual mitigation measures in conjunction with the threat profile.

1.1.7 Theoretical and practical degrees of security

Even for barriers that provide a high degree of confidentiality, there are limitations:

- Theoretical confidentiality:
  - **Perfect confidentiality is unattainable.**
- Practical confidentiality:
  - **Near-perfect confidentiality can be uneconomical**, for example, if the cost for guarding the information is higher than the assigned price if the respective information is leaked.
  - **Near-perfect confidentiality can be impractical**, for example, if it requires device- and user-specific usernames and very long, truly random, device-specific passwords that users cannot reasonably memorize.

As a consequence, develop an assessment for the efficiency of an individual mitigation measure addressing a specific threat risk.

1.1.8 Strategies to provide improved security: confidentiality example

Regarding the above example, there are 2 aspects for achieving confidentiality:

- **Real-world barriers are imperfect**: No single real barrier offers perfect confidentiality.
- **Mitigation strategies may be required**:
  - **Defense in depth**: Single barriers can be combined (chained along the attacker's intended access path).
  - **Hardening**: Barriers (single or combined) can be implemented on several, parallel access paths, so a strong barrier cannot be circumvented by exploiting another, weaker, barrier.

As a consequence, **develop an assessment for the criticality of a given threat risk in conjunction with the associated mitigation's efficiency**. Also assess which critical thread risk/ mitigation efficiency combinations need to be combined with other thread risk/mitigation combinations, for defense in depth. The resulting overview is also suitable for picking less critical thread risk/mitigation efficiency combinations as possible targets for hardening.

1.1.9 Skepticism: Approximations in this document

In this document, approximations are sometimes used. The goal is to make the security considerations more practical and concise as opposed to a theoretical approach that may be more exact but impractical to implement.

When approximations are used, they typically tend to the skeptical side. That is, in case of doubt:

- Threat exploitability is considered easier (making the threat more likely).
- Threat exploit severity is considered higher (making a breach more dangerous).
- As a result, threat risks are considered higher.
- Mitigation effort is considered higher (making mitigation harder).
- Mitigation effectiveness is considered lower (making mitigation less worthwhile).
- As a result, mitigation efficiency is considered lower.
- The criticality (threat risk combined with mitigation efficiency) is considered more critical.

1.2 Overview

1.2.1 Subject

The "Security" user manual contains:

- Specific security considerations and actions to help secure your network device (see on page 55 “Device security in the life cycle phases”)
- Specific security considerations and actions which enable a secured network device to help support and enhance the security and availability of your network (see on page 99 “Network security support”)

It deals with the following life cycle phases of your network device:

- Secure installation (see on page 59 “Suggested installation step sequence”)
- Secure setup (see on page 67 “Security setup overview”)
- Secure operation (see on page 92 “Operation”)
- Secure maintenance (see on page 93 “Maintenance”)
- Secure replacement (see on page 94 “Device hardware replacement”)
- Secure repair (see on page 95 “Device hardware repair”)
- Secure decommissioning (see on page 97 “Device decommissioning”)

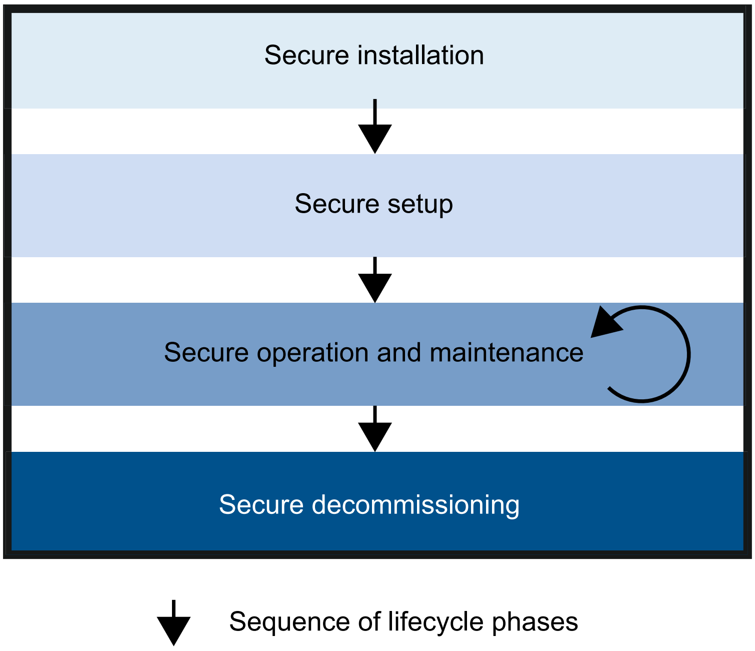
Secure installation
Secure setup
Secure operation and maintenance
Secure decommissioning
Sequence of lifecycle phases

Figure 1: Device life cycle overview

1.2.2 Scope

This document deals with device security measures throughout the device life cycle. These measures build the base for the following overarching concepts:

- Security planning:
  - Assessing the threat risk, the mitigation efficiency, and the resulting criticality
  - Defense in depth for the device
  - Hardening the device

- Device security in the life cycle phases:
  - Specifically set up and deploy the device to help achieve defense in depth for your system
  - Specifically set up and deploy the device to help harden your system
- Network security support:
  - Specifically set up and deploy the device to support the security and availability of your network

A network device is part of a superordinate system. Therefore, the device and the system are interdependent. The system life cycle and the requirements of the system for defense in depth are outside the scope of this document. References to the system life cycle are made only if necessary, and only for information purposes.

Note:
For your network, additional planning and implementation steps may be required. For example, you may need a Layer 3 (L3) network plan in addition to the VLAN plan mentioned in this document. The L3 network plan and the VLAN plan are both outside the scope of this document.

1.2.3 Capability security levels

The general security level addressed in this document is the IEC 62443 Capability Security Level 1 (SL-C1). SL-C1 means protection against casual or coincidental access by unauthenticated entities.

Content conforming to SL-C2 or higher is marked up, for example, with <SL-C2>.

1.2.4 Required preparatory work

This manual focuses on the security measures for your network device and how a secured device can help maintain the security and availability of your system.

To be effective, these measures need a solid base. The prerequisite for working through this manual is that you have already performed the required high-level security planning steps.

These planning steps may include:
□ Research standards that are applicable to your situation, for example, IEC 62443.
□ Define your system scope.
□ Define the security zones in your system.
□ Define the required subsystem and device functions in each zone.
□ Compile the threats to the individual system zones.
□ Assess the threats’ properties (yielding the threats’ risks).
□ Compile a threat profile per zone.
□ Contextualize your threat profile with regard to applicable standards.
□ Collect mitigation measures (create a pool).
□ Assess the mitigation measures’ properties (yielding the mitigation measures’ efficiencies).
□ Associate the mitigation measures with the threat profile.
□ Develop a mitigation strategy.
□ Develop an overarching system security concept.
□ Develop a defense in depth concept.
□ Develop a hardening concept.

Note:
Depending on your circumstances, additional or different steps may be required.

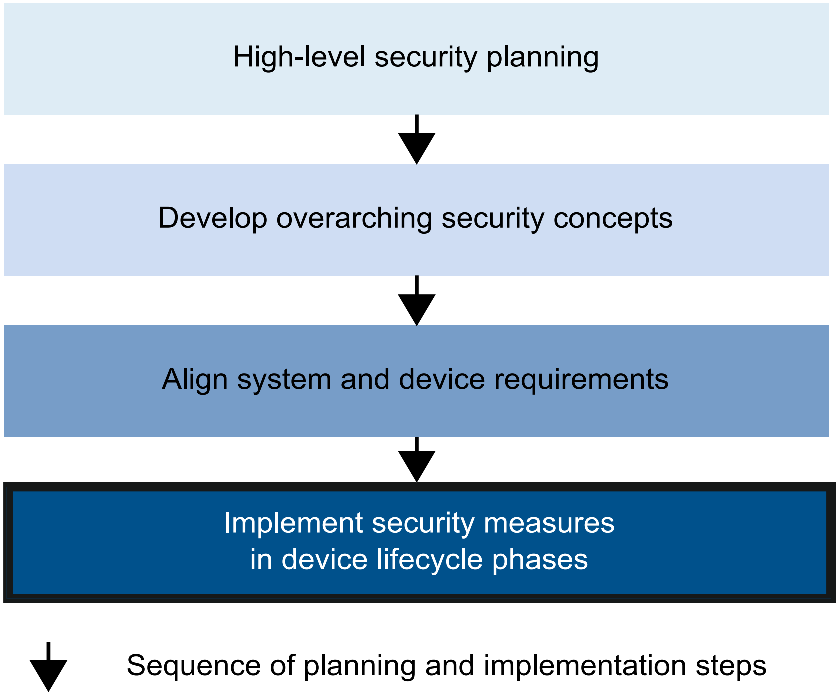
High-level security planning
Develop overarching security concepts
Align system and device requirements
Implement security measures
in device lifecycle phases
Sequence of planning and implementation steps

Figure 2: Required preparatory work hierarchy before implementation

The overarching system security concept may include:

Hardware-related concepts:
- A suitable physical location for the device
- [NDR3.13] Checking the security seal of a device
- Possible restrictions to the device’s hardware interfaces
- A decommissioning policy [CR4.2]

Setup- (software-) related concepts [CR7.6]:
- A user account login policy
- A user account password policy
- A user account and access role policy
- A secure management protocol policy [CR7.7]
- An SNMPv3 authentication and encryption types policy
- A remote logging policy
- A fall-back policy for protocols that offer fall-back
- An LLDP policy <SL-C2>

Organizational concepts:
- Network time synchronization considerations <SL-C2>
- Software update and configuration server considerations <SL-C2>
- Certificate and revocation management for authentication, logging and eMail servers <SL-C2>
- Authentication server considerations <SL-C2>
- Logging server considerations <SL-C2>
- eMail logging server considerations <SL-C2>
- A backup policy for device-related data [SR7.3] [SR7.3 RE1] [CR7.3]
- A policy for device hardware replacement and repair [CR7.4]

Note:
This manual refers to individual overarching security concepts when required. However, the details of developing the security concepts themselves are outside the scope of this document.

1.2.5 Software setup scenarios and hardware scenarios

The software setup scenario consists of the required software setup steps. A particular software scenario typically has a specific hardware scenario as its base.

The hardware scenario consists of a secure installation location, and of possible device hardware interface access restrictions. The resulting hardware scenario can by itself help mitigate a considerable part of the threats.

Note:
The hardware scenario planning is required as a base for the software setup planning. A specific hardware scenario base can make the planning and deployment of the software setup steps significantly easier.
When planning device security, the hardware scenario is typically planned first, followed by the software setup scenario. The practical implementation sequence may deviate from the planning sequence.

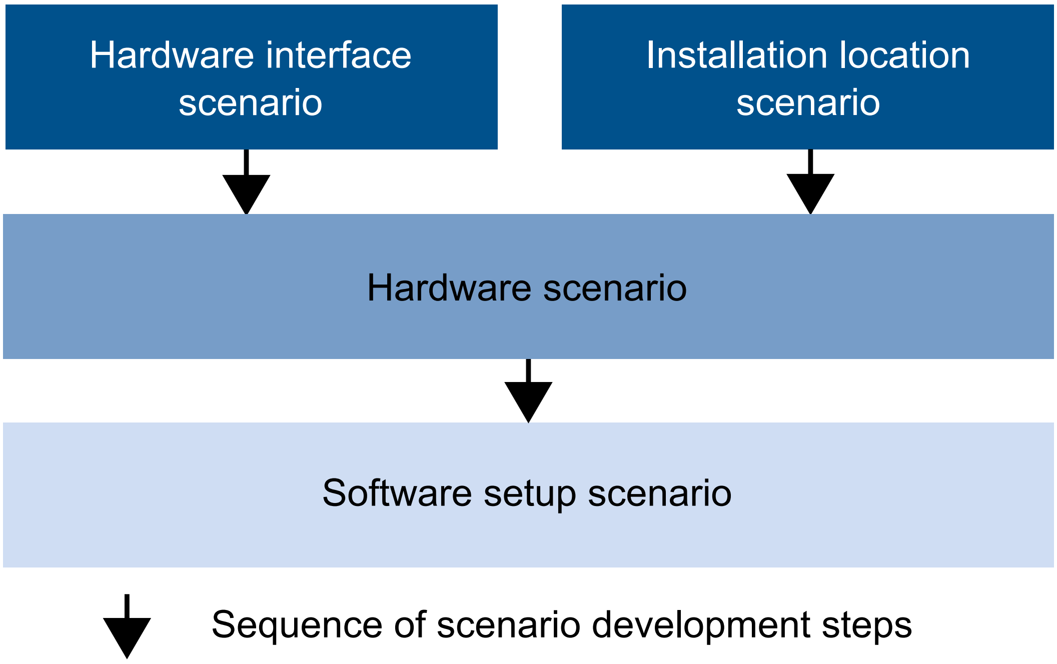
Hardware interface scenario
Installation location scenario
Hardware scenario
Software setup scenario
Sequence of scenario development steps

Figure 3: Basic scenario development steps

1.2.6 Scenario development

To develop a scenario (eventually represented by a set of hardware or software setup steps), typically a structured approach is taken. The steps of this approach are outlined in the following chapters:

- Gathering threats to compile a threat collection
- Assessing the threat risks to compile a threat profile
- Gathering mitigation measures to create a mitigation pool
- Assessing the mitigation measure efficiencies to develop a mitigation strategy
- Selecting mitigation measures for defense in depth
- Selecting mitigation measures for hardening

Consider using software tools that support you in these steps.

1.3 Compiling a threat profile

An individual threat profile for a device typically results from the specific user scenario (a collection of use cases) for the device.

The user scenario is defined by the following circumstances which are part of the threat model:
- the physical position of the device on the site
- the logical position of the device in the network
- the required functions of the device
- other functions of the device that are not required, but exist and may pose a vulnerability

When you compile the threat profile, determine the following aspects for each individual threat:
- Exploitability: How hard it is to exploit the individual threat
- Exploit severity: How significant the effects of an exploitation are

For gaining a better overview of the individual threats, you can assess the risk for an individual threat by combining exploitability and exploit severity.

1.3.1 Risk value and unit

A concrete, individual risk has a value and a unit:
- A risk can take on any positive, continuous, nonzero value.
- The unit of a risk depends on which risk you are considering. All risks include a probability (which has no unit) relating to a given time period (which has the unit of time). When combining these units, a risk has the unit of a rate, for example, a probability rate of 1% / year or 1 / 100 years.
  - Some risks can be reasonably associated with money, for example, the amount of money needed to restore lost data. Risks of this type, for example, can have the unit EUR / year, and an example value could be 10 EUR / year.
  - Other risks (for example, bodily injury or loss of reputation) cannot be assigned a straightforward amount of money. For risks of this type, it may be advisable to explicitly keep the unit of the individual risk together with the probability and the time period. For example, such a risk could have the unit "probability of light bodily injury per year" and an example value could be "probability of light bodily injury: 10 ppm / year".

Note:
The two types of risks (monetary and non-monetary) cannot be compared or combined directly because their units do not match. One possible approach to compare or combine them indirectly is to multiply the non-monetary residual risks by an explicit factor, resulting in a unit of money per time period. The factor should represent a very conservative approach to converting non-monetary risks (for example, personal injury) to monetary risks. This is a demanding ethical assessment. There is no technical solution.

1.3.2 Assess the risk of an individual threat

The risk of a threat is determined both by its exploitability and by the severity of the effects of an exploit. These aspects can be summed up in a threat risk matrix. This matrix concentrates a 2-dimensional set of 9 possible combinations into a one-dimensional index of 5 values.

Table 4: Threat risk matrix

	Exploitability		
Exploit severity	Easy	Medium-hard	Hard
High	**5**: Very high risk	4: High risk	**3**: Medium risk
Medium	**4**: High risk	**3**: Medium risk	2: Low risk
Low	**3**: Medium risk	**2**: Low risk	**1**: Very low risk

Note:
This matrix is intended to provide basic guidance on how to assess a threat’s risk. Your actual situation may require a different assessment approach.

Table 5: Examples for threat exploitability

Threat	**Exploitability**	**Remarks**
Telnet access to the device management is possible.	Easy	Telnet offers no confidentiality, no integrity, and no authenticity.
SSH access to the device management has weak password.	Medium-hard	Dictionary or brute-force attack needed for exploit.
The device LEDS on front panel are visible.	Hard	An observer can infer a small part of the device and port status.

Note:
These examples are intended to provide basic guidance and are non-exhaustive. Your actual situation may require a different classification of threat exploitability.

Table 6: Examples for threat exploit severity

Threat	**Exploit severity**	**Remarks**
Attacker has access to the device management	High	Attacker can circumvent confidentiality, integrity and authenticity of sensitive information.
Attacker abuses a loop guard on a specific segment	Medium	Attacker can execute a Denial of Service (DoS) attack on this segment.
Attacker can create arbitrary syslog messages	Low	Attacker can create false syslog entries.

Note:
These examples are intended to provide basic guidance and are non-exhaustive. Your actual situation may require a different classification of exploit severity.

1.4 Defense in depth

1.4.1 Introduction

The concept of defense in depth is presented here because it is useful and even necessary for planning the mitigation strategies that are introduced later.

The same applies to the complementary concept of hardening.

1.4.2 Purpose

Defense in depth is a strategic concept that employs various independent security (that is, mitigation) measures to guard an asset under consideration against specific threats, as summed up in a threat profile.

A system that employs defense in depth first confronts an attacker with a particular barrier. If an attacker overcomes this barrier, the system presents another barrier of a different type. This layered security approach is considered best practice. It potentially demoralizes an attacker while taking the imperfection of real-world security barriers into account.

Note:
Implementing at least 2 barriers may require additional mitigation steps than those resulting from the particular user scenario part that the threat profile is based on. These additional mitigation steps could be taken from another part of the user scenario.
If no additional mitigation measures readily exist, this may be a sign that your user scenario or your mitigation strategy needs enhancement. You may then be required to plan for additional mitigation measures.

1.4.3 Defense in depth vs. hardening

In comparison to hardening, defense in depth is a more selective and structured approach. Defense in depth employs a specific subset of all conceivable security measures.

Hardening can be characterized as defense in broad. It aims at closing as many weaknesses in any barriers as possible and reasonable. When you are planning a mitigation strategy, use the concept of defense in depth first and deduce a plan with particular mitigation measures. Then consider complementing the plan by using additional hardening measures.

Implementing hardening measures may also help to establish additional barriers in the context of defense in depth. This way, implementing hardening measures steps can also enhance the defense in depth measures. Therefore, hardening measures, although more general in nature, can be efficient.

A strategic approach to hardening may include the concepts:
- Least required privileges – for the device user accounts
- Least required functions – for the device security
- Least required device functions – for the network security support

1.4.4 Responsibilities

Defense in depth and hardening both require planning, implementation, and maintenance. The system operator is responsible for performing these steps.

To help secure your system, consider the security measures provided in this manual. Select those that are most relevant for your specific situation.

1.4.5 Defense in depth example

An attacker is supposed to be connected to a company's industrial network. The asset under consideration is an industrial Ethernet switch in a production cell. The goal of the attacker is to gain access to the device management. The following graphic shows a possible arrangement of device-level barriers in a simplified way.

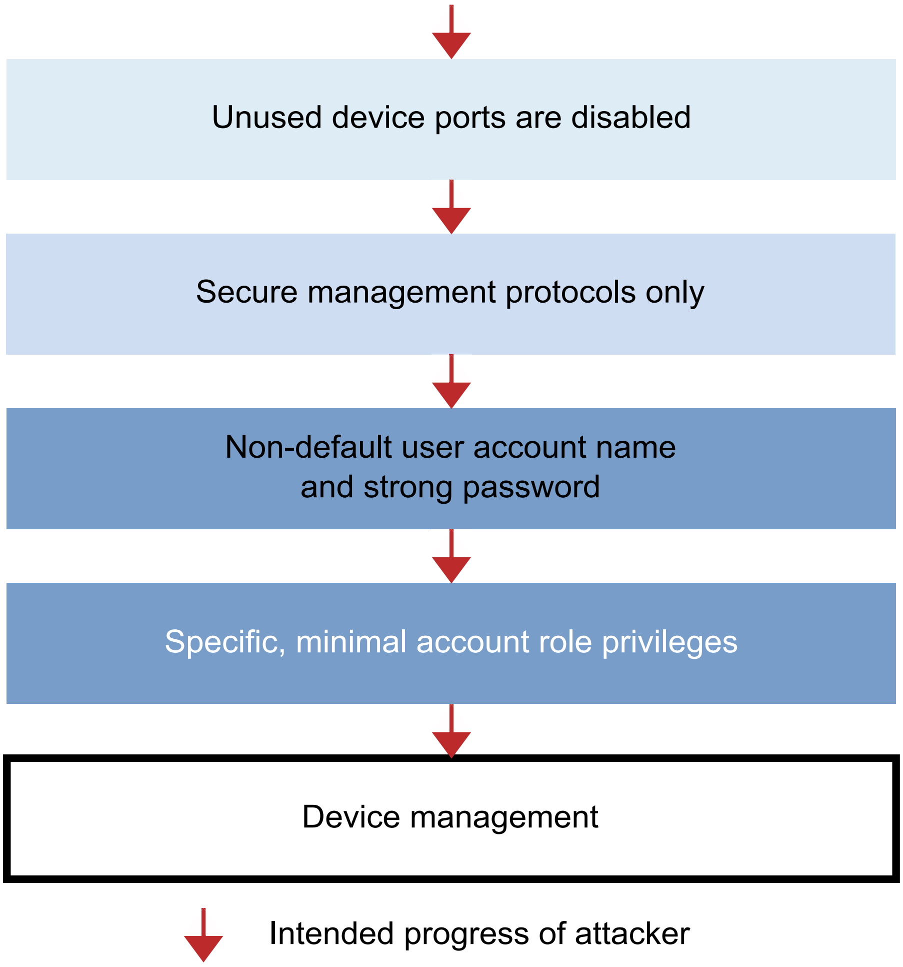
Unused device ports are disabled
Secure management protocols only
Non-default user account name and strong password
Specific, minimal account role privileges
Device management
Intended progress of attacker

Figure 4: Barrier arrangement example for defense in depth

A more detailed example

The attacker is supposed to be connected to the company’s industrial network (1). In more general cases, the attacker may instead be connected to the company Intranet (b) to the Internet (a).

Table 7: Defense in depth barriers example

ID	Barrier	Description
	System level	
a	Internet Firewall	The attacker must overcome the firewall between the Internet and the company Intranet to get access to the company Intranet.
b	Industrial Firewall	The attacker must overcome the industrial firewall to get access to the industrial network. The industrial firewall separates the industrial network from the company Intranet.
1	Dedicated device management VLAN	The attacker must overcome VLAN restrictions to snoop or inject packets.
	Device level	
2	Secure management protocols only	The attacker must overcome encryption to snoop or create packet contents.
2a	Non-default user account name[1]	The attacker must perform a brute-force attack to find the real user account name.
2b	Strong password[2]	The attacker must perform a brute-force attack to find the real password.
3	Specific, restricted account privileges	To read privileged data or manipulate device settings, the attacker must perform a dictionary or brute-force attack to find the real administrator account credentials.

[1] A dedicated user account name can be device-specific and could be intentionally chosen to be non-descriptive.

[2] A password can be specific to a certain access protocol (for example HTTPS) and can also be device-specific.

1.5 Developing a mitigation strategy

To build a mitigation strategy, first develop a pool of conceivable mitigation measures. Then assess the mitigation measures' efficiencies to develop a mitigation strategy.

When you develop a mitigation strategy, determine the following aspects for each individual mitigation measure:
- Effort: How much effort it takes to implement an individual mitigation measure
- Effectiveness: How effective the individual mitigation measure is in reducing or eliminating the threat

To gain a better overview on the individual mitigation measures, you can determine the efficiency for an individual mitigation measure by combining effort and effectiveness.

1.5.1 Mitigation efficiency value and unit

The efficiency of a concrete, individual mitigation measure can take on any positive, continuous, nonzero value <1. It has no unit, so it can be regarded as a factor. The higher the mitigation efficiency, the smaller the associated risk reduction factor.

1.5.2 Assess the efficiency of an individual mitigation measure

The efficiency of a mitigation measure is determined both by the required mitigation effort and by the mitigation's effectiveness. These aspects can be summed up in a mitigation efficiency matrix. This matrix concentrates a 2-dimensional set of 9 possible combinations into a one-dimensional index of 5 values.

Table 8: Mitigation efficiency matrix

	Effort		
Effectiveness	Small	Moderate	Big
High	**A**: Very high efficiency	**B**: High efficiency	**C**: High efficiency
Medium	**B**: High efficiency	**C**: Medium efficiency	**D**: Low efficiency
Low	**C**: Medium efficiency	**D**: Low efficiency	**E**: Very low efficiency

Note:
This matrix is intended to provide basic guidance on how to assess a mitigation measure's efficiency. Your actual situation may require a different assessment approach.

Table 9: Examples for mitigation efforts

Mitigation measure	Effort	Remarks
Disable Telnet access.	Small	Telnet access has a simple, binary, setting.
Set up restrictions to device management, by protocol and IP address range.	Moderate	The restrictions consist of a number of tabular settings and require an L3 network plan.
Create individual and CA-signed HTTPS certificates for each device.	Big	Generating private/public key pairs requires high-quality entropy and possibly dedicated hardware. Signing the individual keys by a certificate authority (CA) additionally requires a public key infrastructure (PKI).

Note:
These examples are intended to provide basic guidance and are non-exhaustive. Your actual situation may require a different classification of mitigation effort.

Table 10: Examples for mitigation effectiveness

Mitigation measure	Effectiveness	Remarks
Set the waiting period after a number of successive failed device management logins to >0.	High	The mitigated attack rate of a dictionary or a brute-force attack is significantly lowered.
Define a VLAN dedicated to device management access.	Medium	Flooded unknown unicast frames of the device management traffic are confined to the respective VLAN and cannot be intercepted from other VLANs.
Set up the CLI post-login banner with only the minimal information required.	Low	The restricted information applies to a situation when an attacker has already succeeded in logging in.

Note:
These examples are intended to provide basic guidance and are non-exhaustive. Your actual situation may require a different classification of mitigation effectiveness.

1.6 Criticality assessment and mitigation strategies

1.6.1 Mitigation calculation

Applying a concrete mitigation measure to counter an individual risk can be modeled by multiplying the risk value by the mitigation’s efficiency (a factor <1), resulting in a smaller, residual risk.

Applying more than mitigation measure to the same risk can be modeled by multiplying the intermediate residual risk from the preceding calculation with another factor <1, thereby reducing the resulting residual risk further. This is the numeric background of the general recommendation to combine mitigation measures if required or possible.

1.6.2 Combining threat risk and mitigation efficiency

The risk of an individual threat, combined with the efficiency of a specific mitigation measure, can be summed up in a criticality matrix. This matrix concentrates a 2-dimensional set of 25 possible combinations into a one-dimensional index of 9 values.

Table 11: Criticality matrix matrix (threat risk and mitigation efficiency combined)

	Threat risk				
Mitigation efficiency	**5**: Very high	**4**: High	**3**: Medium	**2**: Low	**1**: Very low
E: Very low efficiency	(1)	(2)	(3)	(4)	(5)
D: Low efficiency	(2)	(3)	(4)	(5)	(6)
C: Medium efficiency	(3)	(4)	(5)	(6)	(7)
B: High efficiency	(4)	(5)	(6)	(7)	(8)
A: Very high efficiency	(5)	(6)	(7)	(8)	(9)

Note:
This matrix is intended to provide basic guidance on how to assess the combination of a particular threat’s risk with respect to a particular mitigation measure’s efficiency. Your actual situation may require a different criticality assessment.

The criticality value is an index of the urgency of a given threat/mitigation combination. It can also be used to evaluate:

- The possible necessity for defense in depth
- Hints for possible hardening measures

1.6.3 Recommended mitigation strategies

Table 12: Criticality and recommended associated mitigation strategies

Criticality	Combination with another mitigation for the same threat
(1)	**Defense in depth required**: ≥2 other mitigation measures of same or higher efficiency
(2)	**Defense in depth required**: ≥1 other mitigation measure of same or higher efficiency
(3)	**Defense in depth required**: 1 other mitigation measure of same or higher efficiency
(4)	**Defense in depth recommended**: 1 other mitigation measure of same or higher efficiency
(5)	**Defense in depth recommended**: 1 other mitigation measure of same or higher efficiency
(6)	**Hardening recommended**: 1 other mitigation measure of same or higher efficiency
(7)	**Hardening recommended**: 1 other mitigation measure of same or higher efficiency
(8)	**Hardening optional**: 1 other mitigation measure
(9)	**Hardening optional**: 1 other mitigation measure

Note:
This table is intended to provide basic guidance on how to mitigate a given criticality (the combination of the threat risk and the mitigation efficiency). You actual situation may require a different mitigation classification for any given criticality.
In fact, when assigning a mitigation strategy to a given criticality, you have considerable leeway to create a solution tailored to your situation.

1.6.4 Residual risk

This residual risk per threat is the main outcome of the threat analysis and the applied mitigation strategy. The residual risk can take on any positive, nonzero value, that is, it is a continuous value.

Note:
For the unit of the residual risk, as well as how to combine different residual risk values (see on page 25 “Risk value and unit”)

1.6.5 Security viewpoints: binary or continuous values

The security of a system under consideration, with respect to a defined threat and defined circumstances (like operation and maintenance), can be viewed in two different ways:

- Security can be regarded as a continuous value (the residual risk can take on any value).
- Security can be regarded as a binary value (security is either given or not).

When viewed as a continuous value (derived from or identical to the residual risk), security can be improved gradually if the residual risk can be lowered.

When viewed as a binary value (security is either given or not), security is the result of comparing the residual risk to the maximum accepted risk for that given residual risk:

- Security is given if the residual risk is below or equal to the maximum accepted risk.
- Security is **not** given if the residual risk is higher than the maximum accepted risk.
- From this viewpoint, and strictly speaking, security, once given, cannot be improved.

Meaning of "improving the security"

When documents use phrases like "improving the security", this can have two meanings:

- For security as a continuous value, it means lowering the residual risk.
- For security as a binary value, it means having a secure system even after lowering the maximum accepted risk. This is typically achieved by lowering the residual risk.

In practice, a phrase like "improving the security" often has the meaning "lowering the residual risk".

1.7 Impact of the system life cycle on the device life cycle

A network device is a component of the superordinate system. Therefore, the system life cycle determines parts of the device life cycle. A system life cycle involves a planning phase. The decisions taken in the planning phase affect the device life cycle directly or indirectly.

Typical decisions during system planning include:

- The physical location of the device, for example, its installation location and the location’s environmental conditions
- The logical position of the device, for example, the security zone
- The requirements of the system for defense in depth

1.7.1 VLAN plan

[SR5.1] [CR5.1]

VLANs are a software-configurable concept to segregate a LAN (Layer 1) into separate Virtual LANs (VLANs) on Layer 2. Advantages include the separation of data packets belonging to different VLANs. The separation also applies to flooded multicast, broadcast, and unknown unicast frames. This helps confidentiality and also helps reduce the network load on Layer 1.

A VLAN plan, including a dedicated device management VLAN, is considered a prerequisite for a secure setup of the device itself, and in turn for the security and availability of your system. Create a VLAN plan that segregates your network on Layer 2. A dedicated management VLAN can be a barrier component in the strategy "Defense in depth".

For small networks with few communication relations, a VLAN plan and the setup of VLANs may be considered unnecessary from a functional perspective. However, from a security perspective, VLANs can be useful or even required.

Note:
The redundancy protocols *HIPER Ring* and *Ring/Network Coupling* employ the fixed VLAN ID 1 for their protocol packets. If you intend to use these redundancy protocols, using the VLAN ID 1 exclusively for these redundancy protocols can help enhance network availability (see on page 43 “VLAN plan considerations depending on redundancy protocols”).

Note:
For your network, additional planning and implementation steps may be required. For example, you may need an L3 network plan in addition to the VLAN plan. Both the L3 network plan and the VLAN plan are outside the scope of this manual.

1.8 Impact of device requirements on system planning

Some requirements of the device have an impact on the system life cycle phases, in particular on system planning.

Topics of this interdependence include:
- A secure installation location, including the aspects:
  - Device availability: Power supply [SR7.5], PoE power budget, and data link redundancy
  - Properties of the SD card slot
  - Properties of the USB port
  - Properties of the media module slots
  - Properties of the signal contact
  - Properties of the digital input
  - Device and port LEDs
- The detailed physical device security requirements, in particular of its hardware interfaces
- The user account policy parameters the device offers:
  - For the login policy
  - For the password policy
  - For the username and access role policy
  - For the SNMPv3 authentication and encryption type, and password policy
- Configuration encryption and the associated password
- VLAN ID restrictions arising from certain redundancy protocols: VLAN IDs ≥2 for payload traffic and device management
- Advanced user authentication measures like 802.1X, the MAC authentication bypass, a dedicated authentication policy list, LDAP or RADIUS: These measures require planning for the device and may also require planning for external system components, like a RADIUS server:
  - Plan the 802.1X setup [SR2.3] [SR2.3 RE1].
  - Plan the MAC authentication bypass setup.
  - Plan the dedicated authentication policy list.
  - Plan the LDAP server setup.
  - Plan the RADIUS server setup.

Note:
These topics are covered in more detail in the following main chapter (see on page 61 “Considering the device availability requirements”).

1.8.1 Planning a secure installation location

Select a location that in addition to its physical properties offers appropriate device security by restricting physical access to the device. For example:
- Install the device in a lockable room to which only authorized personnel have access.
- Install the device in a lockable cabinet to which only authorized personnel have access.
- Install the device in a lockable cabinet with a nontransparent door.

ℹ Refer to the "Installation" user manual for a suitable physical installation location:
- Chapter "Safety instructions" for safety and regulatory topics
- Chapter "Technical data" for the allowed device temperature ranges and climatic conditions
- Chapters "Installation > Installing and grounding the device" and "Installation > Connecting the terminal blocks" for the mechanical and electrical device installation

1.8.2 Planning for device availability

Device availability can be an important base for the security of the superordinate system. Check that the following device availability requirements are met as required in your situation:

- [SR7.5] Provide a redundant power supply
- Provide an adequate power budget for the device and for PoE
- Provide data link redundancy

1.8.3 Planning for signal contact use

If you intend to use the signal contact, consider the following security aspects:

- **To help protect the device**, connect the signal contact only to a circuit that meets the device requirements.
- **To help protect your system**, connect the signal contact only to a circuit that does not have explicit security or safety requirements.

ℹ Refer to the "Installation" user manual:

- Chapter "Safety instructions" for safety and regulatory topics
- Chapter "Technical data > Signal contact" for allowed signal contact operating conditions
- Chapter "Installation > Connecting the terminal blocks > Signal contact" for the electrical signal contact connection

1.8.4 Planning for digital input use

If you intend to use the digital input, consider the following security aspects:

- **To help protect the device**, connect the digital input only to a circuit that meets the device requirements.
- **To help protect your system**, connect the digital input only to a circuit that does not have explicit security or safety requirements.

ℹ Refer to the "Installation" user manual:

- Chapter "Safety instructions" for safety and regulatory topics
- Chapter "Technical data > Digital input" for allowed digital input operating conditions
- Chapter "Installation > Connecting the terminal blocks > Digital input" for the electrical digital input connection

1.8.5 Planning for device and port LED visibility

The device and port LEDs show important information about the device state and the port states.

If you have high security requirements, consider the following security measures as required to help prevent information leakage:

- Install the device in a cabinet with a nontransparent door.
- Cover or obstruct the LEDs with a removable cover.

ℹ Refer to the "Installation" user manual, chapter "Description > Display elements" for the device and port LEDs.

1.8.6 Planning how to check the security seal

[NDR3.13]

Plan on how the security seal on a new device shall be checked (see on page 119 “Security seal”).

1.8.7 Planning restrictions to the device hardware interfaces

The possible modifications discussed here apply exclusively to the external hardware interfaces at the device surface. The intent of these measures is to restrict physical access to particular device hardware interfaces while keeping the device closed.

Plan the restrictions, like covering or obstructing a slot or a port, according to your requirements:
- Restrict physical access to the SD card slot.
- Restrict physical access to the USB port.
- Restrict physical access to network ports or SFP slots.
- Restrict physical access to empty media module slots.
- Restrict physical access to the signal contact.
- Restrict physical access to the digital input.
- Restrict physical (visual) access to the device LEDs and port LEDs.

ⓘ Refer to the "Installation" user manual, chapter "Description > Management interfaces" for the hardware interfaces.

1.8.8 Planning a dedicated user account login policy

[SR3.8] [SR3.8 RE1] [SR3.8 RE2] [SR3.8 RE3] [CR1.11] [CR2.5] [CR3.8]

The device lets you set up a login policy for the user accounts.

The login policy applies consists of:
- Login attempts:
  - The maximum number of failed user login attempts in a row until the device locks the respective user account
- Minimum password length:
  - The minimum password length that the device enforces when changing a password or specifying a new password
- Login attempts period:
  - The waiting time before the device auto-unlocks a locked user account

The login policy applies to every user account.

The login policy applies to the following user interfaces and access protocols:
- The Command Line Interface (CLI) using SSH or Telnet
- The Graphical User Interface (GUI) using HTTPS or HTTP

Note:
For quantitative information on how to ensure a secure login policy (see on page 136 “Attack rate mitigation”). For quantitative information on how to provide for hard-to-break passwords (see on page 123 “Password strength and policy guide”).

You can plan the following requirements for the user login:

- Login attempts:
  - For security reasons, plan the value as low as possible but >0.
  - For availability reasons, plan it as high as practical. Chose a value that fits your requirements.
- Minimum password length:
  - For security reasons, plan a value as high as reasonable.
  - Consider the type of password you want to use: High-complexity passwords contain a higher level of entropy than low-complexity passwords of the same length. To achieve a given entropy, low-complexity passwords therefore should be considerably longer than high-complexity passwords.
  - Chose a minimum password length that fits your requirements.
  - For quantitative information on how to ensure hard-to-break passwords (see on page 123 “Password strength and policy guide”).
- Login attempts period:
  - For security reasons, plan the value >0 and as high as reasonable.
  - For availability reasons, plan it as low as practical but >0. Chose a value that fits your requirements.

Note:
Access to the CLI using the serial connection is exempt from the login policy. Users accessing the CLI through the serial connection have an unlimited number of login attempts. These users are also not required to wait for the next login attempt, that is, the Login attempts period does not apply. This helps ensure access to the device management in situations where availability may be critical, and for users who already have physical access to the device.
To help secure your system, develop an overarching user account login policy.

ℹ Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device login functions.

1.8.9 Planning a dedicated user account password policy

[CR1.7]

The device lets you set up a password policy for the user accounts.

For detailed information on how to ensure hard-to-break passwords (see on page 123 “Password strength and policy guide”).

Consider the type of password you want to use (see on page 130 “Quantitative password strength”):

- High-complexity passwords have the following properties (see on page 130 “High-complexity passwords”):
  - No part of the password can be found in a dictionary
  - Contains ≥1 lowercase characters, ≥1 uppercase characters, ≥1 digits, and ≥1 special characters
- Low-complexity passwords have the following properties (see on page 132 “Low-complexity passwords”):
  - Consist of several words, each of which can be found in a dictionary
  - A punctuation character typically separates the words
  - Allow but do not require uppercase characters, digits, or special characters

High-complexity passwords of a given length contain a higher level of entropy than low-complexity passwords of the same length. To achieve a given entropy, low-complexity passwords should be considerably longer than high-complexity passwords.

Note:
High-complexity passwords are more commonly used.

You can set up the following requirements for the password:
- The minimum number of uppercase characters
- The minimum number of lowercase characters
- The minimum number of digits
- The minimum number of special characters

Note:
The minimum password length belongs to the user account login policy (see on page 38 “Planning a dedicated user account login policy”).

To help secure your system, develop an overarching user account password policy. When you do, consider the following aspects to deter attackers:
- Consider using account names that are non-standard and are non-descriptive to unauthorized entities.
- Consider using different user account names on different devices.
- Consider using different passwords on different devices, even for user accounts with the same name.
- Consider using different SNMPv3 passwords on different devices.

For the user credentials in the delivery state (see on page 77 “Set up a dedicated user account login policy”).

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device password policy functions.

1.8.10 Planning a dedicated user account name and access role policy for device management

[SR2.1] [SR2.1 RE1] [SR2.1 RE2] [CR1.1 RE1] [CR1.3] [CR1.4] [CR1.5] [CR2.1 RE1] [CR2.1 RE2]

The device requires each user to identify themselves (by the user account name) and to authenticate themselves (by the associated password). The device associates a specific access role to each user account <SL-C2>.

Note:
User account names are case-sensitive.

Table 13: User account roles and privileges

User account role	Privileges
`unauthorized`	None - refuses login into the device.
`guest`	Permits reading of device management data, except the audit trail. The role refuses any write access to data.

Table 13: User account roles and privileges

User account role	Privileges
`auditor`	Permits reading of device management data, including the audit trail. The role permits writing the audit trail to a log file, but refuses any other write access.
`operator`	Permits reading and writing of device management data. The role refuses write access to security-relevant settings and the audit trail.
`administrator`	Permits reading and writing of device management data, including security-relevant settings. This role also permits the reading of the audit trail.

In the delivery state, the device has the following user account preconfigured:

Table 14: User credentials for the administrator account in the delivery state

Username	Password	User account role
`admin`	`private` (May have been changed at first login.)	`administrator`

Note:
Software releases 08.1.00 and higher in the delivery state no longer offer a user account with the name `user` and the associated password `public`. If you need a user account that has only read access, you can create a user account with the access role `guest` and assign it the username `user`, for example.

Set up dedicated user accounts as required:
- Assign the login and password policies.
- Create user accounts with:
  - Dedicated names <SL-C2>
  - Chosen access roles that offer only the least required privileges
  - The password policy check enabled
- Assign the new user accounts strong, individual passwords.
  - Plan strong SNMPv3 authentication and encryption types and strong related passwords for the new user accounts.
- Remove user accounts with standard names.

Note:
To help secure your system, develop an overarching user account and access role policy.
If you have high security requirements, consider planning different user account names and different passwords on different devices. Also consider user account names that are intentionally non-descriptive to unauthorized entities.
If you intend to use SNMPv3, also consider developing an overarching policy for SNMPv3 authentication and encryption types, and the related passwords. If you have high security requirements, consider planning different SNMPv3 passwords on different devices.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device user account name and access role functions.

1.8.11 Planning configuration encryption and the associated password

Plan a configuration encryption policy:
- Plan if you want to enable the configuration encryption.
- Plan a specific password policy for the configuration encryption password.

Note:
Configuration encryption with a password is required for a device setup compliant with SL-C2.

The default setting of the configuration encryption is disabled ⚠. If the configuration encryption is disabled, the *Security Status* function in the Web-based interface notifies the user.

Note:
The configuration encryption password can and likely should be different from the user account passwords.
The configuration encryption password is not checked against the user account password policy.

ℹ Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > Load/ Save" for the configuration encryption and the associated password.

1.8.12 Planning session timeouts <SL-C2>

Plan finite session timeouts for:
- The Graphical User Interface using HTTPS or HTTP
- The Command Line Interface through the serial connection, SSH, or Telnet

ℹ Refer to the "Graphical User Interface" reference manual:
- Chapter "Device Security > Management access > Web" for the Graphical User Interface timeout function
- Chapter "Device Security > Management access > CLI" for the SSH and serial connection timeout function

1.8.13 Planning a dedicated logging policy

[SR2.8] [SR2.8 RE1] [SR2.11] [SR2.11 RE1] [SR2.12] [SR2.12 RE1] [SR6.1] [CR2.8] [CR2.9] [CR2.10] [CR2.12] [CR3.9] [CR6.1] [CR6.2]

Set up the device logging settings:
- [CR2.11 RE1] Synchronize the device system clock to a trusted source <SL-C2>.
- Specify the severity levels of events you require to be logged.
- Specify the logging destinations you require, including possible remote logging.

To help secure your system, develop an overarching remote logging policy (see on page 48 “Logging server considerations <SL-C2>”).

Note:
The syslog (system message logging) client in the device offers unencrypted communication as well as encrypted communication. To help secure your system, use encrypted syslog, that is, syslog over TLS <SL-C2>.
The persistent logging function can be enabled or disabled. However, the audit trail created by the persistent logging function cannot be deleted once written to. Neither can the audit trail be deleted by resetting the device to the delivery state.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Diagnostics > Syslog" for the device syslog function.

1.8.14 Planning a dedicated LLDP policy <SL-C2>

When LLDP is enabled on your device:
- When the **LLDP receive function** is enabled, the device collects information about its neighbors and provides this information to a management station.
  - The prerequisite is that the other devices in the same network have their individual LLDP send function enabled.
- When the **LLDP send function** is enabled, the device sends information about itself and its respective port to its neighbors. The neighbors can collect that information and provide it to a management station.
  - The prerequisite is that the other devices in the same network have their individual LLDP receive function enabled.

LLDP can help automate a system inventory. LLDP may also help discover mismatches in port settings, like half-duplex and full-duplex settings, or VLAN settings, of ports connected to each other.

Depending on your security requirements, LLDP may need to be disabled on the device as well as on other network devices. The delivery state for LLDP is globally disabled.

1.8.15 VLAN plan considerations depending on redundancy protocols

[SR5.1] [CR5.1]

Network availability can be an important base for the security of the superordinate system. The device offers redundancy protocols for this purpose.

The redundancy protocols *HIPER Ring* and *Ring/Network Coupling* employ the fixed VLAN ID 1 for their protocol packets. Using the VLAN ID 1 exclusively for these redundancy protocols can help enhance network availability. A VLAN plan (see on page 35 “VLAN plan”) that takes this particularity into account may require the use of VLAN IDs ≥2 for payload traffic and device management. The files on the external memory

Note:
The other redundancy protocols, the Media Redundancy Protocol (MRP) and the *Redundant Coupling Protocol*, do not require a fixed VLAN ID to function. Therefore, MRP and the *Redundant Coupling Protocol* may be preferable over *HIPER Ring* and *Ring/Network Coupling*.

ⓘ Refer to the "Graphical User Interface" reference manual:
- Chapter "Switching > *HIPER Ring*" for the *HIPER Ring* function
- Chapter "Switching > *Ring/Network Coupling*" for the *Ring/Network Coupling* function

1.8.16 Advanced authentication measures <SL-C2>

If you intend to use advanced user authentication measures like 802.1X, MAC authentication bypass or a dedicated authentication policy list:
- Plan the 802.1X setup [SR2.3] [SR2.3 RE1].
- Plan the MAC authentication bypass setup.
- Plan the dedicated authentication policy list.

ⓘ Refer to the "Graphical User Interface" reference manual:
- Chapter "Network security > 802.1X" for the 802.1X function
- Chapter "Controlling the data traffic > MAC authentication bypass" for the MAC authentication bypass function
- Chapter "Device security > Authentication lists" for the dedicated authentication policy list

1.9 Impact of network aspects on system planning

1.9.1 External server considerations

To perform its functions, the device may rely on other system components. These system components are internal to the network but external to the device.

Typical examples are:
- Software update and configuration servers
- DHCP servers
- DNS servers
- Time-servers
- Authentication servers
- Syslog servers

Using these servers can provide extended functionality that is not available in a purely local system concept. Examples for extended functionality are:
- Authentication servers offer various optional parameters, like assigning a VLAN ID to a user.
- Syslog servers offer log entry redundancy and virtually unlimited storage capacity.

For some protocols, like system message logging (syslog), you can use the remote server in the normal state of operation, and have a fall-back to the local operation should the respective server become unreachable.

Note:
If your planned device configuration uses such external system components, consider developing an overarching policy for the external system components. This may include certificate and revocation management for authentication, logging and eMail servers.
If you intend to use a fall-back operation for a certain protocol, check if the protocol offers this possibility, and if it is appropriate for your situation. Then develop an overarching policy for the fall-back.

1.9.2 Software update and configuration server considerations <SL-C2>

If you intend to use servers for the update of the device software and to distribute device configuration files, plan a host key policy for these servers, possibly including server key rotation.

Policy items may include:
- Plan a secure transfer protocol, for example, SFTP or SCP
- Plan the distribution of the server public key fingerprints
- Plan for a rotation of the server keys and the associated fingerprints

Note:
For authentication, logging, and eMail logging servers, trust is managed by another concept, TLS server certificates and revocations lists (see on page 49 “Certificate and revocation management for authentication, logging and eMail servers <SL-C2>”).

Server key rotation

Server key rotation on a regular basis limits the amount of data encrypted or signed by a specific key (to be precise: by the private key of a specific key pair).

Given that the private key has a non-zero probability of being leaked, key rotation limits the amount of data encrypted or signed by that key:

- Data encrypted by that key may have also been leaked and might subsequently be exposed to decryption by the leaked private key. Therefore, key rotation limits the extend of possible decryption exposure.
- For data signed by that key, it limits the amount of data that could have signed by an attacker, thus pretending a trustworthy signature.

Server key rotation means that a specific key will only be user for a limited period and will normally replaced by another key shortly before the period of the given key runs out.

A server key rotation scheme may include the setting up of 2 or more keys per server whose validity periods overlap.

1.9.3 External DHCP server considerations

If you intend to use DHCP to obtain the device management IP address or other parameters, plan the DHCP server setup. If you intend to use external DHCP servers, consider developing an overarching DHCP server policy.

Note:
The DHCP client implicitly trusts the DHCP server. Depending on your actual situation, assigning a static (that is, locally specified) IP address to the device may be considered more secure than using the DHCP client.

ⓘ Refer to the "Graphical User Interface" reference manual:

- Chapter "Basic settings > IPv4 > BOOT/DHCP" for the device IPv4 DHCP client function
- Chapter "Basic settings > IPv6 > DHCP" for the device IPv6 DHCP client function

1.9.4 DNS server considerations

If you intend to use the device DNS client functions that require an external DNS server, plan the DNS server setup. If you intend to use external DNS servers, consider developing an overarching DNS server policy.

Note:
The device’s DNS client implicitly trusts the external DNS server. Depending on your actual situation, not using the device DNS client functions may be typically considered more secure than using an external DNS server.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Advanced > DNS > DNS client" for the device DNS client function.

1.9.5 Network time synchronization considerations <SL-C2>

[CR2.11 RE1]

Network time synchronization can be required for several reasons, including secure logging or TLS certificate validation.

The device offers SNTP and PTP for synchronizing its internal clock.

The time synchronization protocols SNTP and PTP implicitly trust their time source. To make network time synchronization more secure, consider developing an overarching network time synchronization policy.

Parameters of this policy may include:
- The choice of the network protocol for time distribution
- The choice of the primary time sources
- The choice of time synchronization paths, based on precision, availability, and security requirements
- Requirements for controlling or tuning the chosen network time protocol on the nodes that are part of the time synchronization path
- The choice of Multicast or Unicast packets on the network layer (L3)

Plan a suitable mitigation concept tailored to your threat model. For example, restrict the time sources a given device accepts. Based on your mitigation concept and your chosen policy, determine which settings are required for the individual devices.

ℹ Refer to the "Graphical User Interface" reference manual:
- Chapter "Time > SNTP" for the device SNTP client and server functions
- Chapter "Time > PTP" for the device PTP functions

1.9.6 Authentication server considerations <SL-C2>

If you intend to use authentication servers to help the device authenticate users or other system entities, plan the setup of the appropriate authentication servers:
- Plan for the dedicated local authentication policy list to use an external authentication server.
- Plan the external LDAP server setup.
- Plan the external RADIUS server setup.

Note:
Depending on your actual situation, setting up only a static, local Integrated Authentication Server (IAS) in the device may be considered more secure than using external authentication servers.
The LDAP client in the device offers encrypted communication as well as unencrypted communication. The default setting is unencrypted communication ⚠. To help secure your system, use encrypted LDAP communication. Secure LDAP establishes trust for the device (the LDAP client) towards the LDAP server by means of a TLS server certificate.
The RADIUS client in the device exclusively uses encrypted communication. The secure RADIUS protocol establishes mutual trust between the device (the RADIUS client) and the RADIUS server by means of a shared secret.
The unsecured protocol versions of LDAP and RADIUS implicitly trust their servers. If you intend to use remote authentication, consider using developing an overarching remote authentication policy and using only encrypted LDAP or RADIUS.
From a security viewpoint, encrypted LDAP is preferable over encrypted RADIUS because encrypted LDAP employs a newer and more sophisticated concept of establishing trust towards the authentication server.

ℹ Refer to the "Graphical User Interface" reference manual:

- Chapter "Device security > Authentication lists" for the dedicated authentication policy list
- Chapter "Device security > LDAP" for the device LDAP client function
- Chapter "Network security > RADIUS" for the device RADIUS client function

1.9.7 Logging server considerations <SL-C2>

[SR2.8] [SR2.8 RE1] [SR2.11] [SR2.11 RE1] [SR2.12] [SR2.12 RE1] [SR6.1] [CR2.8] [CR2.9] [CR2.10] [CR2.12] [CR3.9] [CR6.1] [CR6.2]

If you intend to use syslog (system message logging) servers to help keep a complete and persistent log of the events reported by the device, plan the setup of the appropriate external syslog servers.

Note:
The syslog client in the device offers unencrypted communication as well as encrypted communication. To help secure your system, use encrypted syslog, that is, syslog over TLS <SL-C2>. The encrypted syslog protocol establishes trust for the device (the LDAP client) towards the LDAP server by means of a TLS server certificate.
Using syslog servers offers the advantage of sending the log entries to a remote location different from the device. This helps provide redundancy. It also helps overcome local log capacity constraints on the device.
If you intend to use remote logging, consider developing an overarching remote logging policy and consider using only encrypted syslog.
The persistent logging function can be enabled or disabled. However, the audit trail created by the persistent logging function cannot be deleted once written to. Neither can the audit trail be deleted by resetting the device to the delivery state.

ℹ Refer to the "Graphical User Interface" reference manual:

- Chapter "Diagnostics > Syslog" for the device syslog function
- Chapter "Diagnostics > Report > Audit trail" for the device Audit trail

1.9.8 eMail logging server considerations <SL-C2>

If you intend to use eMail servers to as part of your logging policy, plan the setup of the appropriate external eMail (SMTP) servers.

The eMail client in the device offers unencrypted communication as well as encrypted communication (SMTP over TLS). To help secure your system, use encrypted eMail submission <SL-C2>. Encrypted eMail submission establishes trust for the device (the eMail client) towards the eMail server by means of a TLS server certificate.

If you intend to use eMail logging, consider developing an overarching eMail logging policy and using only encrypted eMail submission.

ℹ Refer to the "Graphical User Interface" reference manual, chapter "Diagnostics > Email notification" for the device eMail function.

1.9.9 Certificate and revocation management for authentication, logging and eMail servers <SL-C2>

If you intend to use TLS-based servers for one of the following functions, plan a policy for the management of the server certificates and revocation lists, possibly including server certificate rotation:

- Authentication servers (see on page 47 “Authentication server considerations <SL-C2>”)
- Logging servers (see on page 48 “Logging server considerations <SL-C2>”)
- eMail logging servers (see on page 48 “eMail logging server considerations <SL-C2>”)

Note:
For software update and configuration servers, trust is managed by another concept, SSH Known Host key fingerprints (see on page 45 “Software update and configuration server considerations <SL-C2>”).

Server certificate rotation

A TLS server certificate, issued by a Certificate Authority (CA) attests the validity and trustworthiness of a public key that was created and submitted for attestation by the server administrator. A certificate therefore implicitly attests the validity and trustworthiness of the private key associated with the signed public key.

Certificate rotation means that a specific certificate has an explicitly limited validity period and will normally be replaced by another certificate shortly before the validity period of the current certificate runs out.

Generating a new certificate includes generating a new key pair by the server administrator and attestation of the new public key by the CA. Certificate rotation therefore also requires key rotation, and the properties of the key rotation apply accordingly (see on page 46 “Server key rotation”).

A certificate rotation scheme may include:

- Setting up of 2 or more certificates per server
- The different certificates attest different public keys of the given server.
- The validity periods of these certificates overlap.

1.10 Device-related policies

1.10.1 Develop a backup policy for device-related data

[SR7.3] [SR7.3 RE1]

Consider developing a backup policy for device-related data. This minimizes your effort for replacing a device if the device becomes inoperable.

This policy may include:
- [SR7.3] [SR7.3 RE1] [CR7.3] [CR7.3 RE1] Creating a backup copy of the device configuration profiles <SL-C2>.
- Keeping the backup files separate from the device in a secure location.
  - For example, placing the backup files on a file server in a device-specific folder.
- Including other device-specific data in the same device-specific folder.
  - For example, including device-specific private keys or certificates.
- Using a file or folder numbering scheme or even a version control tool to track the device configuration history.

1.10.2 Develop a policy for replacing the device hardware

[CR7.4]

Consider developing a policy for replacing the device hardware.

Topics of this policy may include:
- Which data of the former device shall be backed up to a remote location
- [NDR3.13] How the security seal of the new device shall be checked (see on page 119 “Security seal”)
- Which data of the former device shall be restored to the new device. For example, the following data for the new device may or may not be identical to the former device’s data:
  - User account names and passwords
  - Host keys (public and private) or certificates
- Which software shall be loaded onto the new device. For example, the software on the new device may or may not be identical to the former device’s software:
  - The new device may be of a different device family.
  - The new device may be of a different device generation.
- If the hardware interfaces of the new device shall be restricted

Align the device hardware replacement policy with:
- The hardware repair policy
- The hardware decommissioning policy

1.10.3 Develop a policy for device hardware repair

Consider developing a policy for device hardware repair.

If a device needs repair, consider your actual confidentiality needs regarding the data present on the device:
- The configuration profiles and configuration scripts
- The boot parameters

- The current HTTPS certificate
- The current SSH host key pair
- The current software files
- The configuration profiles on the external memory

Furthermore, consider the following organizational steps:
- For the device hardware, specify:
  - If you expect to get the same device back (identified by the same base MAC address)
  - If you agree to receive another device of identical type (will have a different base MAC address)
  - If you agree to receive a device of another, superior type or generation (will have a different base MAC address and possibly also other properties)
- For the security seal on the device (see on page 119 “Security seal”), specify
  - How you check the security seal’s condition before sending the device to the manufacturer
  - How you check the security seal’s condition after receiving the device back from the manufacturer

1.10.4 Develop a policy for device hardware decommissioning

Consider developing a policy for device hardware decommissioning.

Specify which of the following steps to carry out, and how.

Note:
Depending on your actual environment, fewer, more or other steps than those listed below may be necessary.

Deletion of confidential data and secrets:
- Reset to the delivery state:
  - Deletes the configuration profiles and configuration scripts in the device
  - Resets the boot parameters
  - Deletes the current HTTPS certificate in the device and creates a new, self-signed HTTPS certificate
  - Deletes the current SSH host key pair in the device and creates a new, self-signed SSH host key pair
  - If the external memory is plugged in, the device also deletes the configuration profiles on the external memory.
- Possible secure wipe (instead or in addition to the reset to the delivery state):
  - Securely overwrite the data and secrets listed in the previous list item, "Reset to the delivery state".
  - If required, securely overwrite the software files in the device.
  - Securely overwrite every configuration profile on a connected external memory.

Secure physical destruction of the device and its accessories:
- Destroy the security seal on the device (see on page 119 “Security seal”).
- Physically destroy the device, including the flash memory chips. This destroys the data and secrets listed in the above list item "Reset to the delivery state".
- If required, physically destroy the external memory.

Note:
The reset to the delivery state leaves the audit trail intact.
If you intend to continue using the device, consider leaving the device and its software intact and deleting or wiping only the data on the device and on the external memory.

For the secure removal of device-related data from the administration environment, perform the following steps. This may include:

- The removal of:
  - Configuration data and its backups
  - Private cryptographic keys
  - Self-signed certificates
- The removal of references to:
  - The device MAC base address
  - The device serial number
  - The device product code

1.10.5 Develop a policy for device hardware disposal

Consider developing a policy for device hardware disposal.

If you have high security requirements, consider disposing of the device by shredding it.

1.11 Operation and maintenance policy

Develop a policy for operation and maintenance. Such a policy may include:

- Which administrative roles for operating or maintaining the device hardware are required
- Which administrative roles for operating or maintaining the device settings are required, along with specific privileges and responsibilities for each role (see on page 40 “Planning a dedicated user account name and access role policy for device management”).
- A schedule for routine operation and maintenance tasks
- A synchronization with operation or maintenance tasks for superordinate system components
- The extent of the scheduled tasks, for example:
  - Looking for a available software update and evaluating or applying it
  - Performing a check on a set of security-related settings and statuses
  - Performing a server key or certificate rotation and applying the resulting changes to the associated device settings, possibly both before and after the server key or certificate rotation
- The extent of active measures that determine the device security status, like:
  - Checking the security status variable of the device
  - Checking other, selected security-related settings in the device
  - Regular penetration tests
- Manual triggers of an out-of-schedule operation or maintenance task, for example:
  - Because of a change in the device setup
  - Because of an audit
  - Because of the results of a penetration test
  - Because of the manual evaluation of log files
- Automatic triggers of an out-of-schedule operation or maintenance task, for example:
  - Caused by the detected change of the security status variable of the device
  - Caused by the detected change in selected security-related settings and statuses
  - Caused by the automatic evaluation of log files

1.12 Document the planned policies

Document the overarching policies. These policies serve as an essential base for planning the individual device configuration and setting up the device.

Depending on your requirements and circumstances, you can plan and maintain the policies with a general software tool (for example, an office spreadsheet or a database application), or use a dedicated software tool.

2 Device security in the life cycle phases

2.1 Develop the device configuration

Based on your documented overarching policies, plan (develop) the configuration for each considered device. If you follow a whitelist approach, include the necessary function policy from your whitelist policy.

Document the planned configuration for each considered device. This helps to keep track of the system.

This planned configuration per device can be, for example:

- On a generalized level:
  - The device needs to have 2 ring ports and 1 uplink port.
- On a concrete level:
  - The device needs ports 3 and 4 as MRP ring ports with a data rate of at least 1 Gbit/s, and ports 1 and 2 for the redundant uplink with at least 100 Mbit/s.

Depending on your actual situation, you can either directly deduct the detailed device configuration from the policies, or allocate 2 steps by planning the device configuration on a generalized level first and then detailing it.

- For a small system or system zone, and if you have already decided which device types you will use, it may be appropriate to plan the concrete device configuration directly (deduct it directly from the policies).
- For a large or complex system or system zone, it may be necessary to split the steps:
  - Plan a generalized device configuration first.
  - Decide which concrete device type and variant you want to deploy.
  - Detail the device configuration.

Depending on your requirements and circumstances, you can plan and maintain the device configuration with a general software tool (for example, an office spreadsheet or a database application), or use a dedicated network planning/management tool.

2.2 Software vs. hardware measures (logical vs. physical)

This main chapter deals with software setup measures as well as hardware measures.

- The software setup measures are also referred to as logical measures.
  - For example: Disable logical access to unused ports and SFP slots.
  - For example: Disable logical access to the digital input.
- The hardware measures are also referred to as physical measures.
  - For example: Restrict or disable physical access to the USB port or the SD card slot.
  - For example: Restrict or disable physical access to the SD card slot.

2.3 Security-related vs. general device functions

The software setup measures in this main chapter deal with the security-related setup of device functions throughout the life cycle phases of the device.

The device functions can be divided into three groups:

- Security-related device functions that help secure the device itself:
  - The setup of these functions is described in this main chapter (see on page 67 “Security setup overview”).
- Security-related device functions that help secure your system and improve its availability:
  - The setup of these functions is described in the following main chapter "Network security support" (see on page 99 “Network security support”).
- General device functions: The setup of the general device functions is outside the scope of this document. If you follow a whitelist approach, include the necessary function policy from your whitelist policy. The necessary function policy may stipulate which general device functions need to be disabled although they are not directly security-related.

  ℹ For the general device functions, refer to the detailed manuals:
  - The "Configuration" user manual
  - The "Graphical User Intere" user manual
  - The "Command Line Interface" reference manual
  - The "Installation" user manual (for hardware-related setup steps)

2.4 Prerequisites for installation and setup

The prerequisite for working through this section is that you have already performed the system planning steps, including:

□ Planning a suitable physical location for the device (see on page 61 “Choosing a secure installation location”)

□ Planning restrictions to the device hardware interfaces (see on page 38 “Planning restrictions to the device hardware interfaces”)

□ If you follow a whitelist approach, develop a necessary function policy from your whitelist policy.
  – The necessary function policy may stipulate which general device functions need to be disabled although they are not directly security-related.

□ Developing a dedicated user account **login** policy (see on page 38 “Planning a dedicated user account login policy”)

□ Developing a dedicated user account **password** policy (see on page 39 “Planning a dedicated user account password policy”)

□ Developing a dedicated user account and access role policy for device management (see on page 40 “Planning a dedicated user account name and access role policy for device management”)
  – Developing a dedicated policy for SNMPv3 authentication and encryption types, and for the related passwords

□ Planning configuration encryption <SL-C2> (see on page 42 “Planning configuration encryption and the associated password”)

□ Planning session timeouts <SL-C2> (see on page 42 “Planning session timeouts <SL-C2>”)

□ Developing a dedicated logging policy, possibly including remote logging (see on page 42 “Planning a dedicated logging policy”)

□ Developing a policy for the servers that hold device software updates and configuration files <SL-C2> (see on page 45 “Software update and configuration server considerations <SL-C2>”)

□ Planning a dedicated LLDP policy <SL-C2> (see on page 43 “Planning a dedicated LLDP policy <SL-C2>”)

If required, the following organizational concepts are also part of the above planning work:

□ Network time synchronization considerations <SL-C2>

□ Certificate and revocation management for authentication, logging and eMail servers <SL-C2>

□ Authentication server considerations <SL-C2>

□ Logging server considerations <SL-C2>

□ eMail logging server considerations <SL-C2>

□ A backup policy for device-related data [SR7.3] [SR7.3 RE1]

□ A policy for device hardware replacement

2.4.1 Possible further prerequisites

Your network may require further system planning steps, including:

□ Traffic segregation on Layer 2 by a VLAN plan

□ Traffic segregation on Layer 3 by an IP subnet plan and the use of routers

□ Use of a network management system like Industrial HiVision (optional)

Note:
The details of these steps are outside the scope of this document.

2.5 Suggested installation step sequence

The steps in the device security life cycle phases in a practical order are:

□ Choose a secure installation location (see on page 61 “Choosing a secure installation location”)
□ Perform the initial software update (see on page 65 “Software update”)
□ Perform the initial security setup (see on page 67 “Security setup overview”)
□ If required, modify the hardware interfaces for security (see on page 87 “Possible restrictions to the device’s hardware interfaces”)
□ Perform the initial device installation (see on page 90 “Device installation”)
□ Operation measures (see on page 92 “Operation”)
□ Maintenance measures (see on page 93 “Maintenance”)
□ Decommissioning measures (see on page 97 “Device decommissioning”)

Note:
Depending on your requirements, you may want to perform the steps in a different sequence.

2.5.1 Reasons for the suggested installation step sequence

Performing the initial setup and the initial software update before the initial device installation can have the following benefits:

- The required resources, for example, TLS server certificates, SSH known host fingerprints, prepared device configuration files and device labels, may be more conveniently available in an office location.
- Time-consuming steps like software updates can be performed in parallel.
- Associated devices, for example, devices participating in a ring redundancy, can be set up contiguously.
- For certain hardware measures like physically blocking the SD card slot, you may need the SD card slot for the initial setup and software update before you can block the SD card slot.
- For certain hardware measures like physically blocking a USB port, you may need the USB port for the software update and initial setup before you can block the USB port.
- The remaining work steps in the field require less time.

2.5.2 Suggested preparation for installation

The following suggested steps and their sequence can help reduce the initial effort and save time:

□ Check the security seal of the device, (see on page 119 “Security seal”).
□ Check the available device software release on the Hirschmann product pages on the Internet at catalog.belden.com.
□ Decide which device software release you want to run on your devices.
□ Download the respective software files.
□ If you want to load the device configuration or update the device software from an SFTP or SCP server, determine the fingerprints of the respective configuration profile or software update servers. Verify that the fingerprints are from a trustworthy source, like the server administrator.

□ If desired, prepare the individual device configuration files based on the respective planned device configuration. If you want to enable the configuration encryption, (see on page 70 “Options to enable configuration encryption”).

□ Prepare the device labels.

Note:
To help keep your system secure, consider using the latest available release of the device software. If you want to load the device configuration or update the device software over a network, verify that you are using a secure transfer protocol, like HTTPS, SFTP or SCP. Use the insecure protocols FTP or TFTP only if you trust the servers and the transfer network or if the files (software or configuration files) are cryptographically signed.

Note:
Configuration encryption with a password is required for a device setup compliant with SL-C2.

ⓘ Refer to the "Configuration" user manual:

- Chapter "Loading software updates" for details on how to:
  - Determine the currently running software release
  - Determine the stored software release
  - Load a previous software version, if required
  - Check for a newer available software release
  - Update the device software
- Chapter "Assistance in the protection from unauthorized access > Making SSH hosts known to the device" for details on how to set up the known hosts’ public key fingerprints.

2.6 Choosing a secure installation location

Note:
The prerequisite for working through this section is that you have already performed the planning for a secure installation location (see on page 36 “Planning a secure installation location”).

Select an installation location that in addition to its physical ambient conditions offers appropriate device security by restricting physical access to the device or its hardware interfaces.

Check that the following device security requirements are fulfilled as required:

- Install the device in a room that can be locked and to which only authorized personnel have access.
- Install the device in a lockable cabinet to which only authorized personnel have access.
- Install the device in a lockable cabinet with a nontransparent door (see on page 89 “Restrict physical (visual) access to the device LEDs and port LEDs”).

ℹ Refer to the "Installation" user manual for a suitable physical installation location:

- Chapter "Safety instructions" for safety and regulatory topics
- Chapter "Technical data" for the allowed device temperature ranges and climatic conditions
- Chapters "Installation > Installing and grounding the device" and "Installation > Connecting the terminal blocks" for the mechanical and electrical device installation

2.6.1 Considering the device availability requirements

Device availability can be an important base for the security of the superordinate system. Therefore, also consider implementing measures that increase device availability.

Check that the following device availability requirements are fulfilled, if required:

- [SR7.5] Consider the power supply requirements (see on page 62 “Considering the power supply redundancy requirements”).
- Consider the power budget requirements (see on page 63 “Considering the power budget requirements”).
- Consider the data link redundancy requirements (see on page 64 “Considering the data link redundancy requirements”).

ℹ Refer to the "Installation" user manual, chapter "Technical data > Supply voltage" for the power requirements of the device.

2.7 Considering the power supply redundancy requirements

[SR7.5]

Check that the power supply redundancy requirements are fulfilled, if required:

- The device is powered by 2 redundant power sources.
- The power supply cables to the device run along different paths as far as possible.
- The power supplies themselves are powered in a redundant way, for example, by 2 separate mains cables.
- The mains cables to the redundant power supplies run along different paths as far as possible.

2.8 Considering the power budget requirements

Check that the power requirements are fulfilled as required:

- One single power supply can deliver power for every connected device.
  - Consider the worst-case power requirements of the inserted SFPs.
  - Consider the inserted media module worst-case power requirements.
- One single power supply can also deliver the worst-case set-up PoE or PoE+ power.

Note:
The condition "one single power supply" takes the possible failure of one power supply in a dual power supply configuration into account.

ⓘ Refer to the "Installation" user manual, chapter "Technical data > Supply voltage" for the power requirements of the device.

2.9 Considering the data link redundancy requirements

Check that the data link redundancy requirements are fulfilled as required:

- The device has redundant data links (typically for an upstream connection).
- The cabinet or room has redundant data links.
- The redundant data links of the cabinet or the room run along different paths as far as possible.

2.10 Software update

[CR4.3] [NDR3.10] [NDR3.14]

The following description applies to:
- The initial software update for a device out-of-the-box
- A software update as part of operation or maintenance

Check if an updated release of the device software is available. You find information and software downloads on the Hirschmann product pages on the Internet at catalog.belden.com. Then decide which software release you want to run on your device [NDR 3.10 RE1] <SL-C2>.

Note:
To update the software on the device, you need management access to the device, which requires at least a preliminary IP address setup. Hirschmann recommends using HiView to assign an IP address setup to the device. After that, HiView allows you to open the Graphical User Interface or the Command Line Interface of the device.

In the delivery state, the device has the following user account preconfigured:

Table 15: User credentials for the administrator account in the delivery state

Username	Password	User account role	Privileges
`admin`	`private` (May have been changed at first login.)	`administrator`	Permits reading and writing of device management data, including security-relevant settings. Also permits the reading of the audit trail.

Note:
Software releases 08.1.00 and higher in the delivery state no longer offer a user account with the name `user` and the associated password `public`. If you need a user account that has only read access, you can create a user account with the access role `guest` and assign it the username `user`, for example.

[CR1.10] At the first login with the delivery state password, the device asks you to change the password. Use a dedicated password according to your password policy (see on page 39 “Planning a dedicated user account password policy”).

If you want to update the device software over a network, verify that you are using a secure transfer protocol, like HTTPS, SFTP or SCP. Use the insecure protocols FTP or TFTP only if you trust the servers and the transfer network or if the software files are cryptographically signed.

If you want to perform the initial software update for a device out-of-the-box and you have the new software image on an SFTP or SCP server, first set up the SSH known host fingerprints in the device (see on page 77 “Set up the SSH Known Hosts fingerprints in the device”). Use the fingerprint of the software update server. This enables the device to decide whether the software update server it contacts is trustworthy or not.

Note:
Verify that the server fingerprints are from a trustworthy source, like the server administrator.

If you decide to upload an unsigned software image to the device, verify that the secure boot mode is disabled and that the setting *Allow upload of unsigned device software* is enabled. In the factory setting, the device allows the upload of an unsigned software image ⚠.

Note:
If you enable the secure boot mode, the device no longer offers the setting *Allow upload of unsigned device software*. The device then refuses the upload of an unsigned software image.

If you decide to update the device software:

□ Save the configuration profile in the volatile memory (*RAM*) to the non-volatile memory (*NVM*).
□ Back up the device configuration.
  – If required by your backup policy, save the backup configuration (see on page 50 “Develop a backup policy for device-related data”).
□ Update the device software.
□ Reboot the device for the new software to take effect.

Note:
To help keep your system secure, consider checking for device software updates regularly and using the latest available release. A newer release of the device software may provide you with security improvements or benefits like new functions, including new device functions that can assist in securing your network.

ℹ Refer to the "Configuration" user manual,

- Chapter "Managing configuration profiles" for the device configuration profiles
- Chapter "Loading software updates" for details on how to:
  - Determine the currently running software release
  - Determine the stored software release
  - Load a previous software version, if required
  - Check for a newer available software release
  - Update the device software
- Chapter "Assistance in the protection from unauthorized access > Making SSH hosts known to the device" for details on how to set up the known hosts’ public key fingerprints.

2.11 Security setup overview

[CR7.1] [CR7.6] [NDR 3.2] [NDR 3.10] [NDR3.14]

The following descriptions apply to:

- The initial device security setup for a device out-of-the-box
- Changes in the device security setup as part of operation or maintenance

Note:
To update the software on the device, you need management access to the device, which requires at least a preliminary IP address setup. Hirschmann recommends using HiView to assign an IP address setup to the device.
[CR7.1 RE1] After the IP address setup, HiView offers you to open the device management. For the software update (see on page 65 “Software update”).
[CR3.3] The *Security Status* function in the device GUI can help you gain a first overview of the device security status. The *Security Status* function monitors some security configuration settings that are considered basic. Depending on your requirements, additional security setup steps may be required even if the *Security Status* function reports *ok*.

ⓘ Refer to:

- The "Graphical User Interface" user manual, chapter "Diagnostics > Status Configuration > Security Status" for the *Security Status* function
- The "Configuration" user manual, chapter "Assistance in the protection from unauthorized access" for a basic device security setup

You will find more details for the security setup in the remainder of this chapter.

Note:
To conserve time and effort, you can perform the following security setup steps by loading a prepared configuration profile into the device.
[CR1.10] At the first login with the delivery state password, the device asks you to change the password. Use a dedicated password according to your password policy (see on page 39 “Planning a dedicated user account password policy”).

Note:
If you want to perform the initial security setup for a device out-of-the-box over a network, verify that you are using a secure transfer protocol, like HTTPS, SFTP or SCP. Use the insecure protocols FTP or TFTP only if you trust the servers and the transfer network or if the configuration files are encrypted.
If you want to perform the initial security setup for a device out-of-the-box and you have the configuration profile on an SFTP or SCP server, first set up the SSH known host fingerprints in the device (see on page 77 “Set up the SSH Known Hosts fingerprints in the device”). Use the fingerprint of the configuration profile server. This enables the device to decide whether the configuration profile server it contacts is trustworthy or not.
Verify that the fingerprints are from a trustworthy source, like the server administrator.

In the following list and the related chapters, "disable logical access" means disabling a feature by a logical measure (a setup in the software). In contrast, "restrict physical access" means disabling a feature or an interface by a physical measure (a hardware modification) (see on page 87 “Possible restrictions to the device’s hardware interfaces”).

Note:
For a device setup compliant with SL-C2, the secure boot mode must be enabled.

The default setting of the secure boot mode is disabled ⚠. If the secure boot mode is disabled, the *Security Status* function in the Web-based interface notifies the user.

If the secure boot mode is enabled but the support mode is also enabled ⚠ (default setting: disabled), the *Security Status* function in the Web-based interface notifies the user.

Note:
If you follow a whitelist approach, consult your necessary function policy. The necessary function policy may stipulate which device functions need to be disabled. This may include functions that are not directly security-related.

Overview of possible security setup steps, in suggested sequence:

- Assign an IP address to the device management:
  - Assign a static IP address (may be considered more secure)
  - or set up DHCP (depending on your DHCP server policy)
- Disable HiDiscovery access.
- Enable configuration encryption <SL-C2>.
- Set up a VLAN dedicated to management access.
- Disable logical access to unused ports and SFP slots.
- Disable logical access for empty media module slots.
- Disable logical access to the signal contact.
- Disable logical access to the digital input.
- Set up Power over Ethernet.
- Disable the automatic device software update from an external memory (ACA).
- Disable copying a software file into the device that lacks a valid cryptographic signature.
- Disable writing a configuration profile to an external memory (ACA).
- Disable writing an unencrypted configuration profile to an external memory (ACA) <SL-C2>.
- Disable loading an configuration profile from an external memory (ACA).
- Disable loading an unencrypted configuration profile from an external memory (ACA) <SL-C2>.
- Disable insecure management protocols.
- Enable IP access restrictions.
- Set up a dedicated HTTPS certificate for the device.
- Set up a dedicated SSH host key for the device (if not already done).
- Set up the SSH Known Hosts fingerprints in the device.
- Set up a dedicated, planned user account login policy.
- Set up a dedicated, planned user account password policy.
- Set up dedicated, planned user account names and roles <SL-C2>.
- Remove user accounts that have standard names <SL-C2>.
- Specify session timeouts <SL-C2>.
- Set up time synchronization for the device clock <SL-C2>.
- Set up logging.
- Disable SNMPv1 traps.
- Enable SNMPv3 traps.
- Set up dedicated login banners.
- Set up the DNS client functions.

You can choose to set up the following advanced device security features as required:

- Access to the system monitor through the serial interface
- Disable access to the CLI service shell.

You can also choose to set up the following advanced user authentication measures as required (see on page 85 “Set up advanced user authentication <SL-C2>”):

- Use 802.1X for user authentication.
- Use a dedicated authentication policy list.
- Use MAC authentication bypass for device authentication.
- Set up LDAP or RADIUS access instead of or in addition to the local Integrated Authentication Server (IAS).

When the device configuration is complete:

- Create a backup copy of the configuration according to your backup policy for device-related data.
- If required, include other device-related data like private keys.
- If you plan on accessing the device through a web browser and use a self-signed HTTPS certificate generated on the device, look up and write down the HTTPS certificate fingerprint.
- If you plan for accessing the device through SSH and use the self-signed SSH key generated on the device, look up and document the SSH host key fingerprint for use as an SSH Known Hosts entry on the clients.

2.11.1 Assign IP address parameters to the device management

Note:
At the first login with the delivery state password, the device asks you to change the password. Use a dedicated password according to your password policy (see on page 39 “Planning a dedicated user account password policy”).

The device offers you the following options for assigning a device management IP address: Local, DHCP (delivery state) ⚠, and BOOTP.

Note:
The setting "Local" (static) is generally considered more secure than using DHCP or BOOTP.
If you use use DHCP or BOOTP, consider loading the configuration or the operating system for the device from the local device memory. This is considered more secure than loading from a TFTP server. Load from a TFTP server only if you trust the transfer network or if the configuration files are encrypted.

ℹ Refer to the "Configuration" user manual, chapter "Specifying the IP parameters" on how to specify an IP address for the device management

2.11.2 Disable HiDiscovery access

[CR4.3]

The delivery state of HiDiscovery is enabled ⚠.

Set the HiDiscovery protocol to `Off` after its initial use. This helps make the device more immune against unauthorized discovery and manipulation.

ⓘ Refer to the "Configuration" user manual, chapter "Specifying the IP parameters using HiDiscovery" on how to:

- Specify the IP address parameters for the device management
- Disable HiDiscovery

2.11.3 Enable configuration encryption <SL-C2>

Enable the configuration encryption and set the associated password according to your configuration encryption policy (see on page 42 “Planning configuration encryption and the associated password”).

Note:
Configuration encryption with a password is required for a device setup compliant with SL-C2.

The default setting of the configuration encryption is disabled ⚠. If the configuration encryption is disabled, the *Security Status* function in the Web-based interface notifies the user.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > Load/Save" for the configuration encryption and the associated password.

Options to enable configuration encryption

You have several options to enable configuration encryption:

- If you have a precompiled, **unencrypted** configuration file:
  - Load the precompiled, unencrypted configuration file.
  - Enable the configuration encryption and set the associated password manually.
  - Save the configuration.
- If you have a precompiled, **encrypted** configuration file:
  - Enable the configuration encryption and set the associated password manually.
  - Load the precompiled, encrypted configuration file.
- If you do not have a precompiled configuration file:
  - Configure the device manually.
  - Enable the configuration encryption and set the associated password manually.
  - Save the configuration.

2.11.4 Set up a VLAN dedicated to device management access

[SR5.1] [CR5.1] [NDR1.13]

Note:
The prerequisite for working through this section is that you have already performed the planning for the general and security-related device setup (see on page 43 “VLAN plan considerations depending on redundancy protocols”).

The delivery state VLAN ID for device management access is 1.

Set up a VLAN dedicated exclusively to device management access. This helps make the device more immune to potential attacks via the network. It may also help improve the reachability of the device management when there is heavy general network traffic.

Note:
If you use the redundancy protocols *HIPER Ring* or *Ring/Network Coupling*, consider using a VLAN ID ≥2 for device management access. Else, you are free to use any VLAN ID you like.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic settings > Global > Management interface" on how to specify a VLAN for device management access.

2.11.5 Disable logical access to the signal contact

If you do not need the signal contact, disable the signal contact in the device setup. In the delivery state, the signal contact is enabled in the mode "Monitoring correct operation".

If you do need the signal contact (see on page 90 “Signal contact considerations”).

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Diagnostics > Status configuration > Signal contact" for the signal contact.

2.11.6 Disable logical access to the digital input

If you do not need the digital input, disable the digital input in the device setup. In the delivery state, the digital input is disabled.

If you do need the digital input (see on page 91 “Digital input considerations”)

2.11.7 Disable logical access to unused ports and SFP slots

In the delivery state, every port and SFP slot is enabled ⚠.

Disable network access for unused ports and empty SFP slots. Treat inserted SFPs without a data cable connected the same way as an unused port. This helps prevent potential attacks that connect a rogue network device to an unused port.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > Port" for disabling ports.

2.11.8 Disable logical access for empty or unused media modules slots

In the delivery state, every media module slot allows access to the network ⚠. With this setting, if a media module is inserted into an empty media module slot, or if ports on an unused media module are physically accessed, the ports of the media module will establish network connections.

Disable empty and unused media module slots in the device setup. This helps prevent potential attacks that connect a rogue network device to a port on a newly inserted or unused media module.

ⓘ Refer to the "Configuration" user manual, chapter "Deactivating the unused modules" for disabling unused media module slots.

2.11.9 Set up Power over Ethernet

Delivery state:

- The device-global setting `PoE Global Operation` is *`On`*.
- Port-related settings:
  - The setting `PoE Port Enable` is *`PoE enable`*.
  - The allowed classes, *`Class 0`*..*`Class 4`*, are enabled.
  - The `Power limit [W]` is `0.0` — the device will not enforce a specific power limit.
  - The power PoE `Priority` is *`low`*.

Device security aspects:

- If you do not need PoE or PoE+, disable PoE and PoE+ globally in the device.
- If you need PoE or PoE+:
  - Disable PoE or PoE+ on those ports that shall not deliver power.
  - For each port with PoE or PoE+ enabled, set up the minimal required reserved power according to the class (*`Class 0`*..*`Class 4`*) of the powered device (PD).
  - If you know the exact maximum power consumption of a PD, you can additionally set the power limit for the given port to this known value.

Network availability aspects: Assign a PoE priority (*`critical`*, *`high`*, or *`low`*) to each PoE port. This helps deliver power to the most important PDs when the device is unable to deliver nominal power to all the connected PDs.

Energy conservation aspects:

- If you set the power limit for a given port to the known power consumption of the PD, this may help in powering more PDs simultaneously in certain cases.
- If you know the power consumption requirements of a PD on a time-of-day or day-of-week basis, you can activate the *Auto-shutdown power* function and set up the associated values *Disable power at [hh:mm]* and *Re-enable power at [hh:mm]*. The prerequisite for this is that the device system clock is synchronized to a reliable, trustworthy source.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > Power over Ethernet" for setting up Power over Ethernet.

2.11.10 Disable automatic device software update from an external memory (ACA)

Disable the automatic device software update from an external memory. This helps secure the device against rogue device software placed on an external memory and the external memory being plugged into the device with the intention that the rogue device software will be copied to the device and take effect after a reboot.

In the delivery state setting, the automatic device software update from an external memory is enabled ⚠.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > External Memory" on how to disable the automatic software update from the external memory.

2.11.11 Disable copying a software file into the device that lacks a valid cryptographic signature

[NDR 3.2]

Disable copying a software file into the device that lacks a valid cryptographic signature: This helps secure the device against rogue device software without a valid cryptographic signature.

If the secure boot mode setting *Secure Boot enabled* is disabled, the device offers you the setting *Allow upload of unsigned device software*. This setting controls whether the device allows the upload of an unsigned software image into the device. If you activate *Secure Boot enabled*, the devide no longer offers the setting *Allow upload of unsigned device software*. The device then refuses the upload of an unsigned software image.

The default setting *Allow upload of unsigned device software* is enabled ⚠. The device will allow the upload a software file into the device that lacks a valid cryptographic signature.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic settings > Software > Allow upload of unsigned device software" on how to allow the upload of unsigned device software.

2.11.12 Disable writing a configuration profile to an external memory (ACA)

Disable the writing of a configuration profile to an external memory. This helps secure the device against leaking its configuration onto a rogue external memory being plugged into the device.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > External Memory" on how to disable writing a configuration profile to the external memory.

2.11.13 Disable writing an unencrypted configuration profile to an external memory (ACA)

To disable writing an unencrypted configuration file to any medium, enable the configuration encryption and set the associated password according to your configuration encryption policy (see on page 70 “Enable configuration encryption <SL-C2>”).

2.11.14 Disable loading a configuration profile from an external memory (ACA)

Disable the loading of a configuration profile from an external memory. This helps secure the device against loading a rogue configuration profile placed on an external memory and the external memory being plugged into the device with the intention that the rogue configuration profile take effect after a reboot.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > External Memory" on how to disable loading a configuration profile from the external memory.

2.11.15 Disable loading an unencrypted configuration profile from an external memory (ACA) <SL-C2>

[CR3.4 RE1]

To disable loading an unencrypted configuration file from any medium, enable the configuration encryption and set the associated password according to your configuration encryption policy (see on page 70 “Enable configuration encryption <SL-C2>”).

2.11.16 Disable insecure management protocols

[CR4.3] [NDR1.13]

Disable insecure management protocols:
□ Disable SNMPv1/v2 (delivery state: disabled).
□ Disable Telnet (delivery state: disabled).
□ Disable HTTP (delivery state: enabled ⚠ – redirects to HTTPS).

ⓘ Refer to the "Configuration" user manual, chapter "Assistance in the protection from unauthorized access" for disabling insecure management protocols.

2.11.17 Set up management IP access restrictions

[CR3.1] [CR7.7] [CR4.3] [NDR1.13]

The device allows restricting the management access to the device to a source IP address range. You specify the address range by giving an IP address and a netmask.

You can set up the management access IP restrictions individually for each protocol or for a group of protocols.

Table 16: Management access protocol overview

Protocol	Recommended setting for operation	Delivery state
HTTP	Disabled	Enabled ⚠ – redirects to HTTPS
HTTPS	Enabled	Enabled
SNMPv1/v2	Disabled	Disabled
SNMPv3	Enabled	Enabled
Telnet	Disabled	Disabled
SSHv2	Enabled	Enabled
IEC 61850-MMS	Disabled	Disabled
Modbus TCP	Disabled	Disabled
EtherNet/IP	Disabled	Disabled
OPC UA Server	Disabled	Disabled
PROFINET	Disabled	Disabled

Note:

HTTP (delivery state enabled ⚠) may be useful for the initial setup of the device. However, it is considered insecure for operation. To help secure your system, disable HTTP as soon as you no longer need it, at the latest before your system goes live.

Note:
Confirm that at least one of the set-up management access IP restrictions is active. If no restriction is active, this results in unrestricted management access for every enabled protocol.
Also confirm that for every enabled protocol, at least one of the set-up management access IP restrictions is active. Excluding a protocol from every management access IP restrictions while the protocol itself is enabled, results in unrestricted management access for the respective protocol.

ℹ Refer to the "Configuration" user manual, chapter "Assistance in the protection from unauthorized access > Activating the IP access restriction" for setting up IP access restrictions.

2.11.18 Set up a dedicated HTTPS certificate for the device

[SR3.1] [SR4.1] [SR4.1 RE1] [CR1.8] [CR4.1] [CR4.3]

In the delivery state, the device contains a self-signed HTTPS certificate ⚠.

You have the option to:

- Replace the existing HTTPS certificate with a new, self-signed HTTPS certificate on the device
  - To help increase security, use the fingerprint algorithm *sha256* (delivery state: *sha256*) for the self-signed HTTPS certificate fingerprint.
  - After generating a new, self-signed HTTPS certificate on the device, write down its fingerprint for later use when you connect with web browser to the device for the first time.
- Load a dedicated, self-signed HTTPS certificate into the device.

    - If you have control over the entropy used for certificate generation, this way of certificate generation is considered more secure.
    - This alternative is also considered more secure because after generating the HTTPS certificate, you have the certificate and its fingerprint available on your external system. This can help you verify the device HTTPS certificate fingerprint when you connect with a web browser to the device for the first time.
- Load a dedicated, CA-signed HTTPS certificate into the device <SL-C2>
    - If you have an established public key Infrastructure (PKI), this option is considered more secure and also more convenient: A CA-signed HTTPS certificate on the device helps you solve the problem "Trust On First Use" when you connect a web browser to the device for the first time. <SL-C2>

Choose the option that best suits your requirements.

Note:
If you have an established public key infrastructure (PKI), then loading a dedicated HTTPS certificate onto the device is generally considered more secure and also more convenient. <SL-C2>
You can find possible popular certificate generation tools on the Internet, for example, by searching for the keywords "HTTPS certificate generation".
To help increase security when you create a new, self-signed HTTPS certificate on the device, use the HTTPS certificate fingerprint algorithm `sha256` (delivery state: `sha256`).

ⓘ Refer to the "Configuration" user manual, appendix "Setting up the configuration environment > HTTPS certificate" for an example of setting up your own HTTPS certificate.

2.11.19 Set up a dedicated SSH host key for the device

[CR1.8] [SR3.1] [SR4.1] [SR4.1 RE1] [CR4.1] [CR4.3]

In the delivery state, the device contains a self-signed SSH host key ⚠.

You have the following options:

- Replace the existing SSH host key with a new, self-signed SSH host key by generating a new SSH host key on the device.
    - To help increase security, use the fingerprint algorithm `sha256` (delivery state: `sha256`) for the SSH host key fingerprint.
    - After generating a new SSH host key on the device, write down its fingerprint for later use when you connect an SSH client to the device for the first time.
- Generate a dedicated SSH host key pair on an external system, self-sign the public key and load the key onto the device.
    - If you have control over the entropy used for key generation, this way of key generation is considered more secure.
    - This alternative is also considered more secure because after generating the SSH host keys, you have the keys and their fingerprints available on your external system. This can help you verify the device SSH host key fingerprint when you connect an SSH client to the device for the first time. <SL-C2>
- Generate a dedicated SSH host key pair, sign the public host key with your Certificate Authority (CA) key and load the CA-signed public host key onto the device.
    - If you have an established public key Infrastructure (PKI), this option is considered more secure and also more convenient: A CA-signed SSH host key on the device helps you solve the problem "Trust On First Use" when you connect an SSH client to the device for the first time. <SL-C2>

Choose the option that best suits your requirements.

Note:
You can find possible popular key generation and signing tools on the Internet, for example, by searching for the keywords "SSH key generation tool".

ⓘ Refer to the "Configuration" user manual, appendix "Setting up the configuration environment > Preparing access using SSH > Loading your own key onto the device" for an example of setting up your own SSH key pair.

2.11.20 Set up the SSH Known Hosts fingerprints in the device

If you want to load the device configuration or update the device software from an SFTP or SCP server, set up the SSH known host fingerprints for these servers in the device. Use the fingerprints of the respective configuration profile or software update servers. This enables the device to decide whether the SFTP or SCP server it contacts is trustworthy or not.

Note:
Verify that the fingerprints are from a trustworthy source, like the server administrator.
If you want to load the device configuration or update the device software over a network, verify that you are using a secure transfer protocol, like HTTPS, SFTP or SCP. Use the insecure protocols FTP or TFTP only if you trust the servers and the transfer network or if the configuration files are encrypted.

Note:
For authentication, logging, and eMail logging servers, trust is managed by another concept, TLS certificates and revocations lists (see on page 49 “Certificate and revocation management for authentication, logging and eMail servers <SL-C2>”).

ⓘ Refer to the "Configuration" user manual, chapter "Assistance in the protection from unauthorized access > Making SSH hosts known to the device" for details on how to set up the known hosts’ public key fingerprints.

2.11.21 Set up a dedicated user account login policy

[SR3.8] [SR3.8 RE1] [SR3.8 RE2] [SR3.8 RE3] [CR1.11] [CR2.5] [CR3.8]

Note:
The prerequisite for working through this section is that you have already planned a dedicated user account login policy (see on page 38 “Planning a dedicated user account login policy”).
For quantitative information on how to ensure a secure login policy (see on page 136 “Attack rate mitigation”). For quantitative information on how to ensure hard-to-break passwords (see on page 123 “Password strength and policy guide”).

The login policy applies to the following user interfaces and access protocols:
- The Command Line Interface (CLI) using SSH or Telnet
- The Graphical User Interface (GUI) using HTTPS or HTTP

Apply your planned user account login policy. This helps ensure that the device will lock out a user after the specified maximum number of failed user logins in a row, require a password with minimum length, and enforces the specified waiting period after a failed login.

Set up a dedicated user account login policy as required:

□ Login attempts:
  – Specify the maximum number of failed user logins in a row until the device locks the respective user account (delivery state: 0 – no limit ⚠).

□ Minimum password length:
  – Specify the minimum password length (delivery state: 6 ⚠).

□ Login attempts period:
  – Specify the waiting time (Login attempts period in minutes) before the device auto-unlocks a locked user account (delivery state: 0 – no waiting time ⚠).

Note:
Access to the CLI using the serial connection is exempt from the login policy. Users accessing the CLI through the serial connection have an unlimited number of login attempts. They are also not required to wait for the next login attempt, that is, the Login attempts period does not apply. This helps ensure access to the device management in situations where availability may be critical, and for users who already have physical access to the device.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device login functions.

2.11.22 Set up a dedicated user account password policy

[CR1.7]

Note:
The prerequisite for working through this section is that you have already planned a dedicated user account password policy (see on page 39 “Planning a dedicated user account password policy”). For quantitative information on how to ensure hard-to-break passwords (see on page 123 “Password strength and policy guide”).

Set up a dedicated user account password policy as required:

□ Minimum required number of uppercase characters (delivery state: 1)
□ Minimum required number of lowercase characters (delivery state: 1)
□ Minimum required number of digits in a password (delivery state: 1)
□ Minimum required number of special characters (delivery state: 1)

Note:
The minimum password length belongs to the user account login policy (see on page 77 “Set up a dedicated user account login policy”).

In the delivery state, the device has the following user account preconfigured:

Table 17: User credentials for the administrator account in the delivery state

Username	Password	User account role	Privileges
admin	private (May have been changed at first login.)	administrator	Permits reading and writing of device management data, including security-relevant settings. Also permits the reading of the audit trail.

Note:
Software releases 08.1.00 and higher in the delivery state no longer offer a user account with the name user and the associated password public. If you need a user account that has only read access, you can create a user account with the access role guest and assign it the username user, for example.

Note:
The device asks you to change the delivery state password on the first login. Use a password different from the delivery state password.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device password policy functions.

2.11.23 Set up dedicated user account names and access roles for device management <SL-C2>

[SR2.1] [SR2.1 RE1] [SR2.1 RE2] [CR1.1 RE1] [CR1.3] [CR1.4] [CR1.5] [CR2.1 RE1] [CR2.1 RE2]

Note:
The prerequisite for working through this section is that you have already planned a dedicated user account name and access role policy (see on page 40 “Planning a dedicated user account name and access role policy for device management”), and that you have planned a dedicated policy for SNMPv3 authentication and encryption types, and for the related SNMPv3 passwords.

In the delivery state, the device has the following user account preconfigured:

Table 18: User credentials for the administrator account in the delivery state

Username	Password	User account role	Privileges
admin	private (May have been changed at first login.)	administrator	Permits reading and writing of device management data, including security-relevant settings. Also permits the reading of the audit trail.

Note:
Software releases 08.1.00 and higher in the delivery state no longer offer a user account with the name user and the associated password public. If you need a user account that has only read access, you can create a user account with the access role guest and assign it the username user, for example.

Set up dedicated user accounts as required:

- □ Assign the device login policy.
- □ Assign the device password policy.
- □ <SL-C2> Create user accounts. For each new user account, perform the following steps:
  - – Create a user account with a dedicated name.
    Note that user account names are case-sensitive.
  - – Assign the new user account an access role that offers only the least required privileges.
  - – Assign the new user account a strong password.
  - – Apply the password policy check to the new user account.
  - – Avoid standard passwords like "private" or "public", even for accounts with non-descriptive names.
- □ For each new user account, set up an SNMPv3 policy if required:
  - – To help increase security, set the SNMPv3 authentication type to `hmacsha` (considered more secure than the delivery state`hmacmd5` ⚠).
  - – Set an SNMPv3 authentication password according to your policy.
  - – To help increase security, set the SNMPv3 encryption type to `aesCfb128` (considered more secure than the delivery state `des` ⚠).
  - – Set an SNMPv3 encryption password according to your policy.
- □ <SL-C2> Remove user accounts that have standard names:
  - – To remove a user account, first log out of the respective user account and log in with an administrator-role account. Then remove the respective user account.
  - – The device requires you to have at least 1 administrator-role account. To remove the standard administrator-role account "admin", you need another account with the administrator role. If you haven’t, create a new administrator-role account first.

ℹ Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device user account name and access role functions.

2.11.24 Specify finite session timeouts <SL-C2>

[CR2.6]

Apply your planned sessions timeout policy. This helps ensure that the device terminates the respective session automatically when idle.

Specify finite session timeouts:

- □ Graphical User Interface using HTTPS or HTTP ⚠ (delivery state: 160 min. ⚠)
- □ For the Command Line Interface through the serial connection, SSH, or Telnet ⚠ (delivery state: 160 min. ⚠)

ℹ Refer to the "Graphical User Interface" reference manual:

- Chapter "Device Security > Management access > Web" for the Graphical User Interface timeout function
- Chapter "Device Security > Management access > CLI" for the SSH and serial connection timeout function

2.11.25 Set up time synchronization for the device clock <SL-C2>

[CR2.11 RE1]

The device offers SNTP and PTP.

The time synchronization protocols SNTP and PTP implicitly trust their time source. Set up the network time synchronization protocol according to the requirements from your overarching network time synchronization policy (see on page 47 “Network time synchronization considerations <SL-C2>”).

To receive time information from an upstream time-server, the device has the role of a time synchronization client. To redistribute its time information to other devices, the device has the role of a time synchronization server. Thus, the client role is normally required, for example, for synchronizing the device system clock, whereas the requirement of the server role depends on your network time synchronization policy.

Parameters to be set up may include:
- Enable only the client functions for the time synchronization network protocols allowed by the policy.
- Specify only trusted next-hop upstream time-servers.
- Tune the client functions of the chosen network time synchronization protocol on the device.
- Enable the time synchronization server functions of the device only if required.
- Tune the time synchronization server functions of the chosen network time protocol on the device.

ℹ Refer to the "Graphical User Interface" reference manual:
- Chapter "Time > SNTP" for the device SNTP client and server functions
- Chapter "Time > PTP" for the device PTP functions

2.11.26 Set up certificates and possible revocation lists for authentication, logging and eMail servers

If you intend to use TLS-based servers for one of the following functions, set up the server certificates and possible revocation lists in the device:
- Authentication servers
- Logging servers
- eMail logging servers

This enables the device to decide whether a TLS-based server it contacts is trustworthy or not.

Note:
For software update and configuration servers, trust is managed by another concept, SSH Known Host key fingerprints (see on page 45 “Software update and configuration server considerations <SL-C2>”).

ℹ Refer to the "Graphical User Interface" reference manual:
- Chapter "Diagnostics > LDAP > Configuration" for managing the certificates for the LDAP client function.
- Chapter "Diagnostics > eMail Notification > Global" for managing the certificates for the email submission function.
- Chapter "Diagnostics > Syslog" for managing the certificates for the Syslog over TLS function.

2.11.27 Set up logging

[SR2.8] [SR2.8 RE1] [SR2.11] [SR2.11 RE1] [SR2.12] [SR2.12 RE1] [SR6.1] [CR1.2] [CR1.8] [CR2.8] [CR2.9] [CR2.10] [CR2.11] [CR2.12] [CR3.1] [CR3.9] [CR6.1] [CR6.2]

Set up logging:

□ [CR2.11 RE1] Consider setting up the device to synchronize its system clock to a trusted source <SL-C2>.

□ Set up the minimum severity level to be logged.
  - The setting depends on our functional and security requirements.

□ Set up logging destinations:
  - The required settings depend on our security requirements.
  - For log availability reasons, a remote destination, different from the location of the device, may be preferable. This is typically a syslog server.
  - For log confidentiality reasons (logs as data in transit), an encrypted logging protocol may be preferable.
  - For log confidentiality reasons (logs as data at rest), an appropriately secured remote destination may be preferable.

Note:
The syslog client in the device offers unencrypted communication as well as encrypted communication. The delivery state is unencrypted communication ⚠. To help secure your system, use encrypted syslog, that is, syslog over TLS <SL-C2>.

Note:
The persistent logging function can be enabled or disabled. However, the audit trail created by the persistent logging function cannot be deleted once written to. Neither can the audit trail be deleted by resetting the device to the delivery state.

ⓘ Refer to the "Graphical User Interface" reference manual:

- Chapter "Diagnostics > Syslog" for the device syslog function
- Chapter "Time > SNTP > SNTP Client" on how to synchronize the device clock through SNTP
- Chapter "Time > PTP" on how to synchronize the device clock through PTP

2.11.28 Disable SNMPv1/v2 write access

[CR6.2]

Note:
If you cannot or do not want to disable SNMPv1 (delivery state: disabled) or SNMPv2 (delivery state: disabled) for some reason, consider at least disabling SNMPv1/v2 write access.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Device Security > Server > SNMP > Configuration".

2.11.29 Disable SNMPv1 traps

[CR6.2]

The device can send SNMPv1 traps. SNMPv1 traps are unencrypted. From a security perspective, this may be considered insecure.

Disable SNMPv1 traps if you do not need them (delivery state: disabled).

ℹ Refer to the "Graphical User Interface" reference manual, chapter "Diagnostics > Status Configuration > Alarms (Traps)" for the device SNMPv1 trap send function.

2.11.30 Enable SNMPv3 traps

[CR6.2]

The device can send SNMPv3 traps. SNMPv3 traps can be signed (authenticated) and additionally encrypted. From a security perspective, authenticated and encrypted SNMPv3 traps are preferable over SNMPv1 traps.

Set up authenticated (and possibly also encrypted) SNMPv3 traps if you require them (delivery state: no SNMPv3 traps configured).

ℹ Refer to the "Graphical User Interface" reference manual, chapter "Diagnostics > Status Configuration > Alarms (Traps)" for the device SNMPv3 trap send function.

2.11.31 Set up dedicated login banners

[CR1.12]

Set up dedicated login banners:

- □ Set up the GUI pre-login banner with only the minimal information required. Avoid any additional information that may help an attacker.
- □ Set up the CLI pre-login banner with only the minimal information required. Avoid any additional information that may help an attacker.
- □ Set up the CLI (post-) login banner with only the minimal information required.

ℹ Refer to the "Graphical User Interface" reference manual:

- Chapter "Device Security > Pre-login Banner" for setting up the GUI and CLI pre-login banner
- Chapter "Device Security > Management Access > Command Line Interface" for setting up the CLI post-login banner

2.11.32 Set up the DNS client functions

Consider the possibilities to set up the device’s DNS **client**:

- Disable the DNS client if you do not use it (delivery state: disabled).
- Set up the DNS client to use only the local, static, hostname table.
- Set up the DNS client to use only specified, trusted, external DNS servers according to your DNS server policy.

Note:
If you do not use the DNS client, disabling it is typically considered more secure.
Using only the local, static, hostname table for the DNS client can be considered more secure than using an external DNS server.

ℹ Refer to the "Graphical User Interface" reference manual, chapter "Advanced > DNS" for the device’s DNS functions.

2.11.33 Advanced: Access to the system monitor through the serial interface

You can enable the access to the system monitor via the serial interface (V.24/RS-232).

Table 19: Serial port by device type

Device type	Connector type	Connector labeling	Function
EAGLE40-03	RJ45 socket	-	Console access to the device management
EAGLE40-07	DB9 socket	CONSOLE	Console access to the device management
	DB9 socket	COM	None (reserved for future use)

ℹ Refer to the "Graphical User Interface" reference manual, chapter "Operation diagnosis > Self-test" on how to enable access to the system monitor via V.24/RS-232.

2.11.34 Advanced: disable access to the CLI service shell

You can disable access to the CLI service shell (delivery state: enabled).

Note:
The CLI service shell can be accessed only by users with the administrator access role.

NOTICE

INOPERABLE DEVICE

Disabling the CLI service shell may impair service access. A possible use case when the CLI service shell is needed, is on-site staff needing to issue service shell commands as instructed by the manufacturer support.

Disabling the CLI service shell can result in an inadvertently inoperable device. Disabling the CLI service shell is permanent. To re-enable the CLI service shell, you have to send the device to the manufacturer.

ⓘ Refer to the "Configuration" user manual, chapter "User Interfaces > Command Line Interface > Service Shell > Deactivate the Service Shell permanently in the device" on how to disable access to the CLI service shell.

2.11.35 Set up advanced user authentication <SL-C2>

[CR1.2]

Set up the following advanced user authentication measures as required:
- Use 802.1X for user authentication [SR2.3] [SR2.3 RE1] [NDR1.13].
- Use a dedicated authentication policy list.
- Use the MAC authentication bypass for device authentication.
- Set up LDAP or RADIUS access instead of or in addition to the local Integrated Authentication Server (IAS).

Note:
The LDAP client in the device offers encrypted communication as well as unencrypted communication (delivery state: unencrypted communication ⚠). To help secure your system, use encrypted LDAP communication.

Note:
The RADIUS client in the device exclusively uses encrypted communication.

Note:
If you use external servers, like LDAP or RADIUS servers, this requires setup or maintenance of the external servers. The system operator is responsible to plan and implement these steps.

ⓘ Refer to:
- The "Graphical User Interface" reference manual:
  - Chapter "Network Security > 802.1X" on how to set up 802.1X port security
  - Chapter "Device Security > Authentication List" on how to set up the authentication policy list of the device’s local IAS
- The "Configuration" user manual chapter "Controlling the data traffic > MAC authentication bypass" on how to set up the MAC authentication bypass
- The "Graphical User Interface" reference manual:
  - Chapters "Device Security > Authentication List" and "Device Security > LDAP" on how to set up the LDAP client in the device
  - Chapter "Network Security > RADIUS" on how to set up the RADIUS client in the device

2.11.36 Create a backup of the device-related data

[SR7.3] [SR7.3 RE1]

Create a backup of the device-related data according to your backup policy. This minimizes the effort to replace the device if the device becomes inoperable.

- □ [SR7.3] [SR7.3 RE1] [CR7.3] [CR7.3 RE1] Consider creating a backup copy of the device configuration profile <SL-C2>.
- □ Keep the backup files separate from the device in a secure location.
  - For example, place the backup files on a file server in a device-specific folder.
- □ If required and useful, include other device-specific data in the same device-specific folder.
  - For example, include device-specific private keys or certificates.
  - If you plan on accessing the device through a web browser and use a self-signed HTTPS certificate generated on the device, look up and document the HTTPS certificate fingerprint.
  - If you plan for accessing the device through SSH and use a self-signed SSH key generated on the device, look up and document the SSH host key fingerprint for use as an SSH Known Hosts entry on the clients.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > Load/Save" on how to save the device configuration.

2.12 Possible restrictions to the device’s hardware interfaces

Note:
The prerequisite for working through this section is that you have already performed planning possible restrictions to the device’s hardware interfaces (see on page 38 “Planning restrictions to the device hardware interfaces”).

The following possible modifications to the device hardware apply exclusively to the device hardware interfaces that are reachable from the device surface. The purpose of these measures is to restrict physical access to particular device interfaces while keeping the device closed.

⚠ WARNING

ELECTRIC SHOCK

To avoid electric shock, do not open the device.

Failure to follow these instructions can result in death or serious injury.

Note:
In the following list and the related chapters, "restrict physical access" means disabling a feature or an interface by a physical measure (a hardware modification). In contrast, "disable logical access" a feature by a logical measure (a software setup) (see on page 67 “Security setup overview”).

The following descriptions apply to possible hardware modifications in the following cases:
- For a device out-of-the-box before installation
- After initial installation
- As part of operation or maintenance

Perform the following modification steps to restrict access to the device hardware interfaces, like covering or obstructing a slot or a port, as required. Restrict physical access:
- To the SD card slot
- To the USB port
- To network ports or SFP slots
- To empty media module slots
- To the signal contact
- To the digital input
- Restrict physical (visual) access to the device LEDs and port LEDs.

2.12.1 Restrict physical access to the SD card slot

If you have high security requirements, and you are sure you will not need the SD card slot after commissioning, consider covering or obstructing the SD card slot.

ℹ Refer to the "Installation" user manual, chapter "Description > Management interfaces" for the SD card slot.

2.12.2 Restrict physical access to the USB port

If you have high security requirements, and you are sure you will not need the USB port after commissioning, consider covering or obstructing the USB port.

ⓘ Refer to the "Installation" user manual, chapter "Description > Management interfaces" for the USB port.

2.12.3 Restrict physical access to network ports or SFP slots

If you have high security requirements, and you are sure you will not need certain network ports or SFP slots after commissioning, consider covering or obstructing these network ports and SFP slots.

ⓘ Refer to the "Installation" user manual, chapter "Description > Ethernet ports" for the network ports and SFP slots.

2.12.4 Restrict physical access to empty media module slots

If you have high security requirements, and you are sure you will not need certain empty media module slots after commissioning, consider covering or obstructing the empty media module slots.

ⓘ Refer to the "Installation" user manual:
- Chapter "Installation > Installing media modules" for installing a media module into a slot
- Chapter "Disassembly > Removing a media module" for removing a media module from a slot

2.12.5 Restrict physical access to the signal contact

If you do not need the signal contact and have high security requirements, consider covering or obstructing the signal contact terminals.

If you use the signal contact (see on page 90 “Signal contact considerations”).

ⓘ Refer to the "Installation" user manual:
- Chapter "Description > Management interfaces > Signal contact" for the signal contact location
- Chapter "Technical data > Signal contact" for the allowed signal contact operating conditions

2.12.6 Restrict physical access to the digital input

If you do not need the digital input and have high security requirements, consider covering or obstructing the digital input terminals.

If you use the digital input (see on page 91 “Digital input considerations”).

ℹ Refer to the "Installation" user manual:

- Chapter "Description > Management interfaces > Digital input" for the digital input location
- Chapter "Technical data > Digital input" for the allowed digital input operating conditions

2.12.7 Restrict physical (visual) access to the device LEDs and port LEDs

If you have high security requirements, consider performing the following steps:

- Install the device in a cabinet with a nontransparent door.
- Cover or obstruct the device LEDs and the port LEDs with a removable cover.

ℹ Refer to the "Installation" user manual, chapter "Description > Display elements" for the device and port LEDs.

2.13 Device installation

The following description applies to:
- The installation of a device in a new system or system zone
- Changes to the device as part of operation or maintenance

ℹ Refer to the "Installation" user manual for a suitable physical installation location:
- Chapter "Safety instructions" for safety and regulatory topics
- Chapter "Technical data" for the allowed device temperature ranges and climatic conditions
- Chapters "Installation > Installing and grounding the device" and "Installation > Connecting the terminal blocks" for the mechanical and electrical device installation

2.13.1 Checking the security seal

[NDR 3.13]

On the new device, check the security seal, (see on page 119 “Security seal”).

2.13.2 Data connections

If you have high device availability requirements, use redundant data connections, for example, for an upstream connection.

ℹ Refer to the "Installation" user manual:
- Chapter "Installation > Installing an SFP transceiver" for the SFP slots
- Chapter "Description > Ethernet ports" for the network ports
- Chapter "Installation > Connecting data cables" on details how to make data connections

2.13.3 Signal contact considerations

If you use the signal contact, consider the following security and safety aspects:
- **To help protect the device**, connect the signal contact only to a circuit that meets the device requirements.
- **To help protect your system**, connect the signal contact only to circuits that do not have explicit security or safety requirements. This means:
  - The circuit controlled by the signal contact does not have any security or safety function.
  - The controlled circuit does not rely on the secure or safe operation of the signal contact.

ℹ Refer to the "Installation" user manual for the signal contact:
- Chapter "Technical data > Signal contact" for the allowed signal contact operating conditions
- Chapter "Installation > Connecting the terminal blocks > Signal contact" for the electrical signal contact connection

2.13.4 Digital input considerations

If you use the digital input, consider the following security and safety aspects:

- **To help protect the device**, connect the digital input only to a circuit that meets the device requirements.
- **To help protect your system**, connect the digital input only to circuits that do not have explicit security or safety requirements. This means:
  - The circuit that controls the digital input does not have any security or safety function.
  - The controlling circuit does not rely on the secure or safe operation of the digital input.

ℹ Refer to the "Installation" user manual for the digital input:

- Chapter "Technical data > Digital input" for the allowed digital input operating conditions
- Chapter "Installation > Connecting the terminal blocks > Digital input" for the electrical digital input connection

2.14 Operation

The prerequisite for the operation life cycle phase is that you have taken the appropriate physical and logical steps to set up the device, both regarding functionality and security. This essentially reduces the required security steps during the operation phase to the considerations already described in this security manual, the "Installation" and "Configuration" user manuals, and the "Graphical User Interface" and "Command Line Interface" reference manuals.

As a minimal overview, the essential parts of how to operate the device properly are:

- Environmental conditions (see on page 90 “Device installation”)
- Device availability requirements (see on page 61 “Considering the device availability requirements”)
- Data connections (see on page 90 “Data connections”)

For the privileges and responsibilities of the administrative user roles for both the device hardware and software settings, as well as for the scheduled or event-driven operation and maintenance parts, follow your policy, (see on page 53 “Operation and maintenance policy”).

2.15 Maintenance

For the privileges and responsibilities of the administrative device user roles as well as for the scheduled or event-driven operation and maintenance parts, follow your policy, (see on page 53 “Operation and maintenance policy”).

2.15.1 Check the security seal (regularly or triggered by an event)

[NDR 3.11]

On the device, check the security seal, (see on page 119 “Security seal”).

2.15.2 Software update

[NDR 3.10]

If required, perform a device software update.

For the security aspects of the software update (see on page 65 “Software update”).

ℹ Refer to the "Configuration" user manual, chapter "Loading software updates" for details on how to:
- Determine the currently running software release
- Determine the stored software release
- Load a previous software version, if required
- Check for a newer available software release
- Update the device software

2.15.3 Hardware changes

⚠ WARNING
ELECTRIC SHOCK To avoid electric shock, do not open the device. **Failure to follow these instructions can result in death or serious injury.**

Typical application cases include:
- Connecting or removing an external device on an Ethernet port
- Inserting, removing or replacing an SFP
- Inserting, removing or replacing a media module on a media module slot

- Connecting, removing or replacing a power supply
- Connecting, removing or replacing a PoE-/PoE+-powered device (PD) on a port

Note:
Depending on your system availability requirements, provide a redundant data upstream connection.
Consider the worst-case power requirements of the inserted SFPs.
Consider the worst-case power requirements of the inserted media modules.
[SR7.5] Connecting an additional power supply to a device with an existing power supply forms a redundant power supply that helps the device availability. Consider the worst-case device power budget for every power supply, in case one of the redundant power supplies becomes inoperable.
Consider the new PoE/PoE+ power budget. Take the worst-case PoE/PoE+ power budget into account. If required, adapt the PoE/PoE+ parameters.

ⓘ Refer to:

- The "Installation" user manual:
  - Chapter "Description > Ethernet ports" for the network ports and SFP slots
  - Chapter "Connecting data cables" on details how to make data connections
  - Chapter "Installation > Installing an SFP transceiver" for installing an SFP
  - Chapter "Disassembly > Removing an SFP transceiver" for removing an SFP
  - Chapter "Installation > Installing media modules" for inserting a media module into an empty media module slot
  - Chapter "Disassembly > Removing a media module" for removing a media module
- The "Configuration" user manual:
  - Chapter "Configuring the ports > Enabling/disabling the port" for enabling or disabling a port
  - Chapter "Assistance in the protection from unauthorized access > Deactivating the unused modules" for enabling or disabling a media module slot
  - Chapter "Basic Settings > Power over Ethernet" for setting up PoE/PoE+

2.15.4 Device hardware replacement

⚠ WARNING

ELECTRIC SHOCK

To avoid electric shock, do not open the device.

Failure to follow these instructions can result in death or serious injury.

[CR7.4]

Perform the following steps:

- According to your backup policy (see on page 50 “Develop a backup policy for device-related data”)
- According to your hardware replacement policy (see on page 50 “Develop a policy for replacing the device hardware”)

Device hardware replacement steps:

□ On the former device, back up the configuration if required and possible.
  - If you have enabled configuration encryption, document the encryption password.

□ Remove the former device from its environment.

□ [NDR 3.11] On the new device, check the security seal, (see on page 119 “Security seal”).

□ On the new device, perform an initial software update (see on page 65 “Software update”).

□ On the new device, set up the device software, for example, by transferring the existing configuration profiles of the former device to the new device (see on page 67 “Security setup overview”).
  – If you have enabled configuration encryption (see on page 70 “Options to enable configuration encryption”).

□ On the new device, restrict the hardware interfaces if required (see on page 87 “Possible restrictions to the device’s hardware interfaces”).

□ Install and connect the new device in its environment.

□ For the former device:
  – If you want the device repaired, follow your hardware repair policy (see on page 95 “Device hardware repair”).
  – If you want to decommission the device, follow your hardware decommissioning policy (see on page 97 “Device decommissioning”).

ⓘ Refer to:

- The "Graphical User Interface" reference manual, chapter "Basic Settings > Load/Save" on:
  – How to save the former device’s configuration
  – How to load the configuration into the new device
- The "Configuration" user manual, chapter "Loading software updates" for the new device on how to:
  – Determine the currently running software release
  – Determine the stored software release
  – Load a previous software version, if required
  – Check for a newer available software release
  – Update the device software
- The "Installation" user manual:
  – Chapter "Disassembly > Removing the device" for mechanically removing the former device from its environment
  – Chapters "Installation > Installing and grounding the device" and "Installation > Connecting the terminal blocks" for the mechanical and electrical installation of the new device

2.15.5 Device hardware repair

⚠ **WARNING**

ELECTRIC SHOCK

To avoid electric shock, do not open the device.

Failure to follow these instructions can result in death or serious injury.

Should your device need repair, follow your device hardware repair policy (see on page 50 “Develop a policy for device hardware repair”).

Consider the following steps:

□ Keep a backup copy of the device configuration (see on page 86 “Create a backup of the device-related data”).
  – If you have enabled configuration encryption, document the encryption password.

□ Make a note of the device base MAC address (read it from the label on the front panel or look it up in the device management).

□ If required and possible, wipe or delete the configuration and other data you consider confidential (see on page 97 “Deletion of confidential data and secrets”).

□ Record the condition of the security seal on the device (see on page 119 “Security seal”).

□ Send the device to the manufacturer for repair.

□ When the device is back from repair:
  - Check according to your device hardware repair policy if the device you received back is acceptable (is either identical to the device you sent in, is a different device of the same type, or is a different device of a superior type).
  - Check the security seal of the repaired device, (see on page 119 “Security seal”). The security seal on the identical device received back should either be a new security seal or the old security seal shall be approximately in the same condition as when you sent the device in. If the device you received back is a different device of the same type or a different device of a superior type, it should have a new security seal.
  - If you have enabled configuration encryption (see on page 70 “Options to enable configuration encryption”).
  - Restore the files on the repaired device from the backup.
  - If required by your policy, compare the repaired device’s actual base MAC address with the address you noted earlier. This helps ensure you have the same device back that you sent in.
  - If required, update the software on the repaired device.

ⓘ Refer to the "Installation" user manual:
- Chapter "Disassembly > Removing the device" for mechanically removing the device from its environment
- Chapters "Installation > Installing and grounding the device" and "Installation > Connecting the terminal blocks" for the mechanical and electrical installation of the repaired device

2.16 Device decommissioning

When decommissioning a device, follow your device hardware decommissioning policy (see on page 51 “Develop a policy for device hardware decommissioning”).

⚠ WARNING
ELECTRIC SHOCK To avoid electric shock, do not open the device. **Failure to follow these instructions can result in death or serious injury.**

Note:
If you have high security requirements, consider physical destruction of the device and the external memory (ACA)(see on page 98 “Secure physical destruction of the device and its accessories”).
Secure physical destruction addresses the possible reading-out of memory blocks from the flash memory and makes deletion and wiping unnecessary (see on page 97 “Deletion of confidential data and secrets”).
If you plan to continue using the device, consider leaving the device and its software intact and deleting or wiping only the data on the device and on the external memory.

ℹ Refer to the "Installation" user manual, Chapter "Disassembly > Removing the device" for mechanically removing the device from its environment.

2.16.1 Deletion of confidential data and secrets

Note:
Resetting the device to the delivery state performs normal file deletion operations on the device, and on the external memory (ACA), which may leave parts of the file contents or memory blocks in the flash memory intact [CR4.2]. Furthermore, the audit trail persists after a reset to the delivery state.
If you have high security requirements, consider the physical destruction of the device and the external memory.

2.16.2 Reset to the delivery state

For the deletion of data, perform the following steps as required:

- Reset the device to the delivery state. This performs the following operations:
  - Deletes the configuration profiles and configuration scripts in the device.
  - Resets the boot parameters.
  - Deletes the current HTTPS certificate in the device and creates a new, self-signed HTTPS certificate.

  - Deletes the current SSH host key pair in the device and creates a new, self-signed SSH host key pair.
  - If the external memory (ACA) is plugged in, the device also deletes the configuration profiles on the external memory.
- If required, manually delete other files on the external memory.

Note:
The audit trail persists in the device even after a reset to the delivery state.

ⓘ Refer to the "Configuration" user manual, chapter "Managing configuration profiles > Reset the device to the factory defaults" on how to reset the device to the delivery state.

2.16.3 Secure physical destruction of the device and its accessories

For the secure physical destruction of physical components, perform the following steps as required by your decommissioning policy:

□ Destroy the security seal on the device, (see on page 119 “Security seal”).
□ Physically destroy the device, including the flash memory chips. This addresses:
  - The HTTPS certificate in the device
  - The SSH host key pair in the device
  - The configuration profiles in the device
  - Any other files in the device

□ If required, physically destroy the external memory (ACA). This addresses:
  - The configuration profiles on the external memory
  - The software files on the external memory
  - Any other files on the external memory

2.16.4 Secure removal of device-related data from the administration environment

For the secure removal of device-related data from the administration environment, perform the following steps as required by your decommissioning policy.This may include:

□ The removal of configuration data and its backups
□ The removal of private cryptographic keys
□ The removal of self-signed certificates
□ The removal of references to:
  - The device MAC base address
  - The device serial number
  - The device product code

2.16.5 Secure disposal of the device hardware

For the secure disposal of the device hardware, follow your disposal policy.

Note:
If you have high security requirements, consider disposing of the device by shredding it.

3 Network security support

This main chapter describes how the device can assist in:
- securing your system
- improving the availability of your system

This chapter deals with specific device functionality in the operation and maintenance life cycle phases that can help improve the security or availability of your network.

3.1 Introduction

Aside from the basic task of forwarding and processing data packets in your network, the device can also help:
- Deploy defense in depth for your network
- Harden your network
- Enhance and maintain the availability of your network

3.1.1 Prerequisites for setting up network security

Only a device that is itself already secured can help reasonably improve the security and availability of your network. The prerequisite for working through this section is that you have taken the required steps to securing the device itself (see on page 55 “Device security in the life cycle phases”).

To determine which device functions are suitable for providing or enhancing the security of your network, apply the process of assessing threat risks, mitigation efficiency and the criticality of the individual threat risk/mitigation efficiency combinations analogous to the device-centered process:
- Compile a network threat profile (see on page 25 “Compiling a threat profile”):
  - Develop a network threat model.
  - Collect the perceivable threats to the network.
  - Assess the network threat risks.
- Develop a general network defense strategy (see on page 27 “Defense in depth vs. hardening”).
- Develop a general network mitigation strategy (see on page 30 “Developing a mitigation strategy”):
  - Collect the perceivable network mitigations.
  - Assess the network mitigation efficiency.
- Develop an individual mitigation strategy (see on page 32 “Criticality assessment and mitigation strategies”):
  - Asses the criticality of the individual network threat/mitigation combinations.
  - Develop a mitigation strategy based on the individual criticality values.

3.1.2 Deploying defense in depth for your network

Defense in depth creates several barriers that a potential attacker must overcome one after the other. The prerequisite for working through this section is that you have already set up a dedicated plan for defending your network in depth (see on page 27 “Defense in depth”).

From a system view, there are 2 complementary ways to implement defense in depth for a network:

- The device-related way:
  - The device-related way deploys measures to help secure the device itself. This in turn helps secure the network. These measures are described in the preceding main chapter (see on page 67 “Security setup overview”).
- The network-related way:
  - The network-related way deploys specific device functions as measures to help secure the network. These measures are described in the remainder of this main chapter.

The suggested network-related mitigation measures are collected in the following chapter (see on page 101 “Measures to help secure the network”).

Note:
First pick the mitigation measures suitable for defense in depth. Then consider hardening by selecting additional measures from the remaining options.

3.1.3 Harden your network

The suggested network-related mitigation measures are collected in the following chapter (see on page 101 “Measures to help secure the network”).

Note:
Pick the mitigation measures suitable for defense in depth first. Then pick hardening measures from the remaining options.

3.2 Measures to help secure the network

The below collection of network-related mitigation measures can be used for defense in depth as well as for hardening. First pick the measures suitable for defense in depth. Then consider hardening by selecting additional measures from the remaining options.

To help you secure your network, perform the following steps on the device according to your requirements, threat and mitigation assessment results, and policies:

- Restrict logical access to your network:
  - Set up VLANs for traffic segregation.
  - Disable GVRP and MVRP.
  - Set up Port Security.
  - Set up *DHCP Snooping*
  - Set up *IP Source Guard*
  - Set up *Dynamic ARP Inspection*
  - Set up the MAC authentication bypass.
- Help secure the network protocols used.
  - Disable GMRP and MMRP.
- Help secure the redundancy protocols used:
  - Set up RSTP guards and helper protocols.
  - Set up the *MRP* (MRP VLAN ID ≥2, tagged packets) parameters.
  - Set up MRP over LAG (MRP VLAN ID ≥2, tagged packets)]
  - Set up Sub Ring with LAG (MRP VLAN ID ≥2, tagged packets)
  - Set up the *HIPER Ring* parameters.
  - Set up HIPER Ring over LAG (VLAN ID 1: tagged packets)
  - Set up the *Redundant Coupling Protocol* parameters.
  - Set up *Ring/Network Coupling* parameters.
- Set up the attack protection support functions:
  - Set up the Denial of Service (DoS) parameters.
  - Set up the Access Control Lists (ACLs).
  - Set up the rate limiter.
  - Set up the Management MAC address conflict detection
- Set up the network time synchronization parameters.
- Set up the logging parameters.
- Set up the LLDP parameters.

Note:
Securing the redundancy protocols used can also help enhance and maintain the availability of your network.
Routing protocols like HiVRRP, VRRP, OSPF or RIP are outside the scope of this document.

3.3 Restrict logical access to your network

3.3.1 Set up VLANs for traffic segregation

[SR5.1] [CR5.1]

The essential prerequisite for setting up VLANs in the device is that you have created a VLAN plan for your network (see on page 35 “VLAN plan”).

Set up the VLANs, the port memberships and the properties of the port memberships according to your VLAN plan.

Note:
If you use certain redundancy protocols, consider using only VLAN IDs ≥2 for payload traffic and device management (see on page 43 “VLAN plan considerations depending on redundancy protocols”).

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Switching > VLAN" on how to set up VLANs for traffic segregation.

3.3.2 Disable GVRP and MVRP

The GARP VLAN Registration Protocol (GVRP) and its successor, the Multiple VLAN Registration Protocol (MVRP or MRP-IEEE Multiple VLAN Registration Protocol) can be used to dynamically set up VLANs in a device. However, using these protocols can also pose a vulnerability if an attacker can snoop GVRP or MVRP frames or inject deliberately crafted GVRP or MVRP frames.

It is generally considered more secure to disable GVRP and MVRP.

Note:
The delivery state for both GVRP and MVRP is globally disabled.

ⓘ Refer to the "Graphical User Interface" reference manual:

- Chapter "Switching > GARP > GVRP" on how to set up GVRP
- Chapter "Switching > MRP-IEEE > MRP-IEEE Multiple VLAN Registration Protocol" on how to set up MVRP

3.3.3 Set up the Port Security

[NDR 1.13]

Port Security is a concept to restrict which frames the network device accepts that have been received on a specific port or VLAN. This can help secure your network.

Port Security distinguishes frames by their MAC source address and their VLAN tag. These values identify frames sent by another device in the L2 network. The device drops frames with a disallowed MAC source address or VLAN ID.

To set up Port Security, create a list of allowed MAC source addresses and VLAN IDs. If the device receives a frame with a MAC source address that is not on the allow list, the device can take a configurable action like sending an SNMP trap to the network management station or disabling the port.

Note:
The delivery state for the Port Security operation is globally disabled. The sub-function "Auto-disable" is also disabled.
Activating Port Security can help protect your network against injection of frames from unknown network nodes. However, if the Port security function is configured to auto-disable a given port when the function detects undesired frames, this can lead to a Denial of Service (DoS) situation.
An attacker may even deliberately send deliberately crafted frames to cause a DoS.
Configure the Port Security function according to what best matches your situation.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Network Security > Port Security" on how to set up Port Security.

3.3.4 Set up DHCP Snooping

DHCP Snooping is a function that supports the network security. It monitors DHCP packets between the DHCP clients and the DHCP server and acts like a specialized firewall between the untrusted DHCP clients and the trusted DHCP servers. *DHCP Snooping* supports you in protecting the network against attacks through rogue or mis-configured devices on untrusted ports or in untrusted VLANs, by filtering or rate-limiting DHCP client packets.

Note:
The delivery state for the *DHCP Snooping* sub-functions "Verify MAC" and "Auto-disable" is disabled.
Activating *DHCP Snooping* can help protect your network against rogue network nodes requesting a legitimate IP address. However, if the*DHCP Snooping* function is configured to auto-disable a given port when the function detects a rogue node, this can lead to a Denial of Service (DoS) situation.
An attacker may even deliberately send deliberately crafted frames to cause a DoS.
Configure the *DHCP Snooping* function according to what best matches your situation.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Network Security > DHCP Snooping" on how to set up DHCP Snooping.

3.3.5 Set up IP Source Guard

IP Source Guard is a function that supports the network security. It filters IP data packets received from another device (called the subscriber), based on the source ID (source IP address or source MAC address). *IP Source Guard* supports you in protecting the network against attacks through IP/MAC address spoofing.

IP Source Guard relies on the *DHCP Snooping* function (see on page 103 “Set up DHCP Snooping”) for determining trusted source IDs, VLANs, and ports for known subscribers, so you have to set up the *DHCP Snooping* function before you can use the *IP Source Guard* function.

IP Source Guard uses the *Port Security* function (see on page 102 “Set up the Port Security”) for controlling the actual data packets, so you have to also set up the *Port Security* function before you can use the *IP Source Guard* function.

Note:
Activating the *IP Source Guard* function can help protect your network against rogue network nodes requesting a legitimate IP address. However, if the *DHCP Snooping* function or the Port security is configured to auto-disable a given port when the respective function is triggered, this can lead to a Denial of Service (DoS) situation. An attacker may even send deliberately crafted frames to cause a DoS.
Configure the *IP Source Guard* function according to what best matches your situation.

ℹ Refer to the "Graphical User Interface" reference manual, chapter "Network Security > IP Source Guard" on how to set up IP Source Guard.

3.3.6 Set up Dynamic ARP Inspection

Dynamic ARP Inspection is a function that supports the network security. This function analyzes ARP packets originating from an untrusted port or destined to an untrusted port, and can rate-limit ARP packets as well as log and discard invalid ARP packets.

Note:
The delivery state for the *Dynamic ARP Inspection* sub-functions "Verify source MAC", "Verify destination MAC", "Verify IP address", and "Auto-disable" is disabled.
Activating *Dynamic ARP Inspection* can help protect your network against rogue network nodes trying to diverting and snoop or manipulate legitimate traffic. However, if the *Dynamic ARP Inspection* function is configured to auto-disable a given port when the function is triggered, this can lead to a Denial of Service (DoS) situation. An attacker may even send deliberately crafted frames to cause a DoS.
Configure the *Dynamic ARP Inspection* function according to what best matches your situation.

ℹ Refer to the "Graphical User Interface" reference manual, chapter "Network Security > Dynamic ARP Inspection" on how to set up Dynamic ARP Inspection.

3.3.7 Set up the MAC authentication bypass

If required, set up the MAC authentication bypass for device authentication.

The MAC authentication bypass can authenticate a particular user of another device, for example the laptop of maintenance personnel, without the need to set up the Port Security of the local network device to allow the MAC source address of the other device.

The advantages are:

- The MAC source addresses of the allowed external devices need not be locally set up in the network device.
  - Consequently, you are spared the local administration effort if the MAC source address changes (for example, because a maintenance laptop has been replaced).
- The external device is not restricted to authentication on a specific network device port.

Note:
The MAC authentication bypass function requires an external authentication server.
If you have high security requirements, disabling the MAC authentication bypass and instead temporarily setting up the maintenance laptop's MAC address locally on the device may be considered more secure.

ⓘ Refer to:

- The "Configuration" user manual, chapter "Controlling the data traffic > MAC authentication bypass" on how to set up the MAC authentication bypass
- The "Graphical User Interface" reference manual, chapter "Network Security > 802.1X > 802.1X Global > MAC authentication bypass format options" on the MAC authentication bypass format

3.4 Help secure the network protocols used

3.4.1 Disable GMRP and MMRP (MRP-IEEE Multiple MAC Registration Protocol)

The GARP Multicast Registration Protocol (GMRP) and its successor, the Multiple MAC Registration Protocol (MMRP or MRP-IEEE Multiple MAC Registration Protocol), can be used to register group (that is, Multicast) MAC addresses dynamically and to automatically setup Multicast forwarding in a device. However, using these protocols can also pose a vulnerability if an attacker can snoop GMRP or MMRP frames or inject deliberately crafted GMRP or MMRP frames.

It is generally considered more secure to disable GMRP and MMRP.

Note:
The delivery state for both GMRP and MMRP is globally disabled.

ℹ Refer to the "Graphical User Interface" reference manual:

- Chapter "Switching > GARP > GMRP" on how to set up GMRP
- Chapter "Switching > MRP-IEEE > MRP-IEEE Multiple MAC Registration Protocol" on how to set up MMRP

3.5 Help secure the redundancy protocols used

Note:
Securing the redundancy protocols used can also help enhance and maintain the availability of your network.

3.5.1 Set up RSTP guards and helper protocols

[CR3.1]

If you use RSTP, consider securing the RSTP guards:

- Consider enabling the BPDU guard function on Edge ports (delivery state: disabled).
- Consider enabling the BPDU filter function on Admin Edge ports (delivery state: disabled).
- Consider disabling the BPDU flood function on ports that have RSTP disabled (delivery state: disabled).

Help secure RSTP helper protocols:

- Consider disabling the L2 loop protection (delivery state: disabled). This helps protecting against a possible DoS attack, where an attacker sends malicious loop protection frames to the device, intending to trick it into disabling its respective port.

Note:
Enabling RSTP guards and helper protocols can help protect your network against rogue network nodes trying to diverting, snoop or manipulate legitimate traffic. However, if a function is configured to auto-disable a given port when the respective function is triggered, this can lead to a Denial of Service (DoS) situation. An attacker may even send deliberately crafted frames to cause a DoS. Configure the RSTP guards and helper protocols according to what best matches your situation.

ℹ Refer to the "Graphical User Interface" reference manual:

- Chapter "Switching > L2-Redundancy > Spanning Tree > Spanning Tree Global" on how to set up the BPDU guard and BPDU filter in the device
- Chapter "Switching > L2-Redundancy > Spanning Tree > Spanning Tree Port" on how to set up the Root guard, TCN guard, the port-related BPDU filter and the BPDU flood functions
- Chapter "Diagnostics > Loop Protection" on the device L2 loop protection function.

3.5.2 Set up the MRP (Media Redundancy Protocol) parameters.

[SR5.1] [CR5.1] [CR3.1]

If you use MRP, consider:

- Using tagged packets for the MRP VLAN
  - This helps MRP availability by prioritizing MRP control packets.
- Specifying a MRP VLAN ID ≥1
  - This causes MRP to use a standard VLAN tag in MRP control packets. This may require an existing VLAN plan.

Note:
The delivery state for MRP is disabled in the device, the MRP VLAN ID is 0.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Switching > L2 Redundancy > MRP" on how to set up MRP.

3.5.3 Set Up MRP over LAG

Set Up MRP over LAG (MRP VLAN ID ≥1, tagged packets). This may require an existing VLAN plan.

Note:
The delivery state for MRP is disabled in the device, the MRP VLAN ID is 0.

ⓘ Refer to the "Configuration" user manual, chapter "Redundancy > Media Redundancy Protocol (MRP) > MRP over LAG" on how to set up MRP over LAG.

3.5.4 Set up Sub Ring with LAG

Set up the Sub Ring with LAG function with an MRP VLAN ID ≥2 and tagged packets. This may require an existing VLAN plan.

Note:
The delivery state for the Sub Ring is disabled in the device, the MRP VLAN ID is 0.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Redundancy > Sub Ring with LAG" on how to set up Sub Ring with LAG.

3.5.5 Set up the HIPER Ring parameters

[SR5.1] [CR5.1] [CR3.1]

If you use the *HIPER Ring* function, consider setting up tagged packets for the fixed VLAN ID 1. This helps the availability of the *HIPER Ring* by prioritizing *HIPER Ring* control packets.

This may require an existing VLAN plan with a device management VLAN ID ≥2.

Note:
The delivery state for the *HIPER Ring* is globally disabled.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Switching > L2 Redundancy > *HIPER Ring*" on the device *HIPER Ring* function.

3.5.6 Set Up HIPER Ring over LAG

Set Up HIPER Ring over LAG with the fixed VLAN ID 1 and tagged packets. This may require an existing VLAN plan with a device management VLAN ID ≥2.

Note:
The delivery state for the *HIPER Ring* is globally disabled.

ⓘ Refer to the "Configuration" user manual, chapter "Redundancy > HIPER Ring client > HIPER Ring over LAG" on how to set up HIPER Ring over LAG.

3.5.7 Set up the Redundant Coupling Protocol parameters

[CR3.1]

If you use the *Redundant Coupling Protocol*, consider helping secure the *Redundant Coupling Protocol*, for example, by setting up VLANs according to your VLAN plan.

Note:
The delivery state for the *Redundant Coupling Protocol* is globally disabled.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Switching > L2 Redundancy > *Redundant Coupling Protocol*" on the device *Redundant Coupling Protocol*.

3.5.8 Set up Ring/Network Coupling parameters

[SR5.1] [CR5.1] [CR3.1]

If you use *Ring/Network Coupling*, consider setting up tagged packets for the fixed VLAN ID 1 (delivery state: untagged). This helps harden the *Ring/Network Coupling* by prioritizing *Ring/Network Coupling* control packets.

This may require an existing VLAN plan with a device management VLAN ID ≥2.

Note:
The delivery state for the *Ring/Network Coupling* is globally disabled.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Switching > L2 Redundancy > *Ring/Network Coupling*" on the device *Ring/Network Coupling* function.

3.6 Set up the attack protection support functions

3.6.1 Set up the Denial of Service (DoS) parameters

[CR7.2]

Consider setting up DoS filters.

Note:
The delivery state for the DoS filters is globally disabled.

ℹ Refer to the "Graphical User Interface" reference manual, chapter "Network Security > DoS > DoS Global" on the device DoS filter functions.

3.6.2 Set up the rate limiter

[CR7.2]

Consider setting up the rate limiter for broadcast, Multicast or Unknown Unicast frames.

Note:
The delivery state for the broadcast, Multicast or Unknown Unicast rate limiters is disabled.

ℹ Refer to the "Graphical User Interface" reference manual, chapter "Switching > Rate Limiter" on the device Rate Limiter functions.

3.6.3 Set up the Management MAC address conflict detection

[NDR1.13]

Consider activating the Management MAC address conflict detection for the device management address. If the function is active and the device detects a conflict, the device will send a trap.

Note:
The delivery state for the Management MAC address conflict detection is disabled.

ℹ Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > Network > Global > Management interface" on the device’s Management MAC address conflict detection function.

3.7 Set up Access Control Lists (ACLs)

[CR7.2] [NDR 1.13] [NDR5.2] [NDR5.2 RE1] [NDR5.3]

This chapter deals with ACLs, their function and the suggested setup steps. It describes the basic ACL functions. Extended ACL functions are outside the scope of this chapter.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Network Security > ACL" for the device ACL function.

3.7.1 Introduction

Access Control lists (ACLs) offer extensive and fine-grained control over the forwarding or dropping of data packets received or transmitted by the device. ACLs can therefore be useful to mitigate security threats in a straightforward yet detailed way.

Note:
In the GUI, an ACL is referred to as a "Group" (a rule group) that has a name and contains one or more rules.

A rule consists of:
- One or more criteria that have to match simultaneously (like a device port number, or an L3 protocol field) and
- One or more actions (mainly `permit` or `deny`) that the device takes when a data packet matches the rule’s criterion

The following rule features are outside the scope of this chapter:
- A rule can have the following extended criteria:
  - The operators `not equal to`, `less than`, and *greater than* for Layer 4 port numbers (source or destination).
  - The operator `fragmented IPv4 packets`
  - The operator `IGMP type`
  - The operator `ICMP type and code`
  - Operators for the TCP flags `ACK`, `RST`, `FIN`, `PSH`, `SYN`, `URG`, and established (`ACK` or `RST`)
- A rule can have the following actions:
  - Creating a log entry
  - Limiting the data rate
- A rule can have the following extended actions:
  - Redirection to a specific port
  - Mirroring to a specific port
  - Assigning a specific queue ID
- A rule can be time-based. That is, the device activates or deactivates a time-based rule, based on the device system time. A time range can be an absolute or periodic time and date. A time range is identified by a name that is referenced in the ACL rule.

Each rule belongs to an ACL with a specific name and has the same type (IPv4-based) as the ACL and its sibling rules. Rules belonging to the same ACL are processed in ascending order of the individual rule index.

Every ACL has an implicit, invisible `deny` rule as the last rule <SL-C2>. As a result, if no explicit rule of an ACL matches a data packet, the device drops the data packet.

Note:
The IPv4-based numerical range starts with 1000.

For an ACL to take effect, assign the ACL: Choose a device port (source or destination port) or a VLAN. Assign a priority to this association, choose the desired direction of the data flow the ACL association shall apply to, and finally select an existing ACL name (followed by the ACL's internal number).

Properties of ACL assignments:

- On a device, 2 or more ACLs can be active simultaneously.
- Each assignment has a priority.
- If there are 2 or more ACLs of the same type assigned to the same device port or VLAN, the device processes the ACL with the higher priority first.
- If the same ACL is assigned to both a port and a VLAN, the device processes the port-related assignment first.
- A particular ACL can be assigned to more than one device port or VLAN, for example, to allow for bidirectional packet flow.

Note:
The device can apply ACLs only to received data packets.

Note:
To help ensure a defined processing order, specify for each assignment a priority that is unique in the scope of the device.

Because ACLs have a potentially heavy impact on the forwarding of data packets, ACLs should be planned accurately and generally need to be tested. If possible, test your planned and set-up ACLs in a test environment before applying the ACLs in a production environment. This allows for the modification, addition, or deletion of rules, ACLs, or ACL assignments that may have been overlooked during planning.

3.7.2 Resolving potential conflicts of aims for an ACL

When creating or modifying an ACL, there can be a conflict of aims between the security aspects of the network and the desire for the smooth functioning of the network:

- **Security aspects of the network** require the ACLs to be as restrictive as possible and to set up only the smallest possible set of `permit` rules. These ACLs are preferably applied to incoming data packets to drop unwanted data packets at the earliest possibility, and also to minimize the traffic within the device.
- **Smooth functioning of the network** desires the ACLs to be as permissive as possible and to set up only the smallest possible set of `deny` rules. The ACLs can be applied to outgoing data packets to maximize possible data packet processing in the device and to drop only the explicitly undesired data packets.

One possible way to address this conflict of aims is to put security first. That is, you plan and set up only the explicitly required `permit` rules. If the test results indicate that ACLs or their assignments are too restrictive, you can modify the ACLs (for example, add new `permit` rules) or their assignments appropriately.

3.7.3 Creating ACLs and associations

The following section describes one possible way of planning, setting up, testing, and administering ACLs for a device. Adapt these steps to suit your specific situation. Some steps may need to be applied iteratively.

Note:
You can plan the ACLs by setting up the ACLs directly on the device, or by using an off-line process and uploading the resulting ACLs to the device later.

Planning

□ Make a list of packet types that explicitly need to be forwarded by the device.
□ Common criteria for packets are (not exhaustive):
  – For an IPv4-based ACL: Source IP address, destination IP address, protocol, source TCP/UDP port, and destination TCP/UDP port
□ As data traffic is typically bidirectional, plan 2 ACLs to consider the data packets for both directions. If the ACLs for different data directions are identical, consider creating only one ACL and assign it separately to each data direction, if possible.
□ Determine to which device port or VLAN you assign the planned ACLs.
□ Consider if it is advantageous to split up the set of packet types into subsets, so each subset can be processed by a particular ACL of a given type, assignment, and data packet direction.
  – Name the individual ACLs (groups) to reflect the ACL's purpose, and, for example, by using a common name prefix for related ACLs.
□ For each ACL, order its rules, using the following criteria:
  – Put the `permit` rule with the most general criteria first (for example, every packet with a certain VLAN tag). Give this rule the lowest index within the ACL. This takes care of the ACL function aspect.
    In the simplest case, this rule is general and has no exceptions. If exceptions are required, deal with them in the next planning step, "Refine the rule list…".
  – Put the `permit` rule with the second-most general criteria next (after the previous rule) by giving it a higher index than the first rule.
  – Proceed with the remaining `permit` rules in this order.
□ Refine the ACL by planning exceptions:
  – For required exceptions to an `permit` rule, put a specific `deny` rule before the respective `permit` rule by giving it a lower index than the existing `permit` rule. This takes care of the ACL security aspect.
  – If further exceptions are required, insert the respective new `deny` rules before the respective existing `permit` rule (give it a lower index). This takes care of the ACL security aspect.
  – Put the rule with the most general exception first (give it the lowest index), followed by the rule with the second-most general exception (give it the second-lowest index), and so on.
  – Repeat these steps for every required exception in the given ACL.
  – A new `deny` rule may turn out to be too general and may therefore require further exceptions in the form of one or more additional preceding `permit` rules. This takes care of the ACL function aspect.

Note:
ACLs and their assignments can become complex. Consider testing the ACLs before you deploy them.

Setup

□ Use the GUI, CLI, or network management software to set up the planned ACLs on the device, or
□ Upload a configuration script (for example, generated by an offline configuration tool) to the device.

Test

□ Activate and assign the ACLs on the device in a test setup.

□ Generate test traffic that represents the expected traffic, that is, consisting of desired as well as of undesired data packets.

□ Evaluate the packets received on the test end devices:
  - Look for unexpected packets. If unexpected undesired packets are transmitted by the test device, add a matching `deny` rule to the ACL plan and subsequently to the respective ACL. Note that the unexpected, undesired packets may include packets targeted at the device-under-test’s management.
  - Look for missing packets. If expected desired packets are not received on the test end devices, consider adding a matching `permit` rule to the ACL plan and subsequently to the respective ACL.
    Note that the expected desired packets may include packets sent by the device-under-test’s management.

□ Evaluate the log entries created by the device:
  - If you have configured your ACL rules to create log entries, inspect the log entries. This can be useful to determine, for example, why the device has dropped a packet.

Administration

- Give the ACLs descriptive names, for example, showing their purpose, possibly including the assignment to a port or VLAN, and the data direction.
- Consider:
  - Saving the ACLs separately from the device configuration or in addition to the device configuration, for example, as script files
  - Assigning the ACL a version number, if you have separate script files for each ACL
  - Using version control to track the ACL history

3.8 Set up the network time synchronization parameters <SL-C2>

[CR2.11 RE1]

The prerequisite for working through this section is that you have taken the required steps to help secure the device itself (see on page 81 “Set up time synchronization for the device clock <SL-C2>”).

To synchronize its system clock, the device acts as a network time client. To help synchronize the time in the network, the device can also act as a network time-server.

Set up the time functions of the device:
- Enable the client function of the device, if required.
  - Enable only the client functions for the network time protocol allowed by your policy.
  - Tune the client functions of the chosen network time protocol on the device.
- Enable the server function of the device only if required.
  - Enable only the server functions for the network time protocol allowed by your policy.
  - Tune the server functions of the chosen network time protocol on the device.

Note:
The delivery state for the time functions is globally disabled.

ℹ Refer to the "Graphical User Interface" reference manual:
- Chapter "Time > SNTP" for the device SNTP client and server functions
- Chapter "Time > PTP" for the device PTP functions

3.9 Set up the logging parameters

[CR1.2] [CR1.8] [CR2.11] [CR3.1]

Set up logging severity levels and destinations. The required settings depend:

- on your device logging policy
- on your remote logging policy

Note:
In the delivery state, the syslog function is globally disabled.
The syslog client in the device offers unencrypted communication as well as encrypted communication (that is, syslog over TLS). The delivery state is unencrypted communication ⚠.
To help secure your system, use encrypted syslog <SL-C2>.
[CR2.11 RE1] Secure logging also relies on the synchronization of the device system clock to a trustworthy source (see on page 81 “Set up time synchronization for the device clock <SL-C2>”).
The persistent logging function, which writes logged events to a device-internal log, can be enabled or disabled. However, the audit trail created by the persistent logging function cannot be deleted once created and written to. Neither can the audit trail be deleted by resetting the device to the delivery state.

ℹ Refer to the "Graphical User Interface" reference manual, chapter "Diagnostics > Syslog" for the device syslog function.

3.9.1 Audit trail (created by persistent logging)

[CR2.11]

The persistent logging function itself can be enabled or disabled. However, existing audit trail entries persist even after the persistent logging function has been disabled.

Note:
The audit trail cannot be deleted by resetting the device to the delivery state.

3.10 Set up the LLDP parameters <SL-C2>

The LLDP global operation setting can be *On* or *Off*. The delivery state is *Off* (disabled).

The device also offers the following basic port-related LLDP operating modes:

- *transmit*
  - The port transmits information about the device and the port itself to its neighbors.
  - The neighbors can collect that information, provide it to a management station, or process it themselves. The prerequisite is that the other devices in the same network have their individual *receive* function enabled.
- *receive*
  - The device collects information about its neighbors that it receives at the given port.
  - The device can provide this information to a management station or process the information itself. The prerequisite is that the other devices in the same network have their individual *transmit* function enabled.
- *receive and transmit* (delivery state ⚠)
  - The port transmits information about the device and the port itself to its neighbors.
  - The device also collects information about its neighbors that it receives at the given port.
- *disabled*
  - The port neither transmits any information about the device or the port itself, nor does it collect information received from other devices.

Enabling LLDP on the device has the following possible advantages and drawbacks:

- Security aspects:
  - Drawback: The device sends information about itself to its immediate neighbors. This might pose an attack surface.
  - Drawback: LLDP-unaware neighbors (for example, a hub) may distribute the device information beyond the immediate neighbors, possibly to the entire L2 network, which might pose an additional attack surface.
  - Advantage: The device can indirectly detect the addition, removal, or reconfiguration of an LLDP-enabled neighbor and report that event to a management station.
- Functional aspects:
  - Advantage: Topology discovery: The device can help perform a system inventory by collecting information about its neighbors and providing this information to a management station.
  - Advantage: The device can use the received information, for example, to automatically detect a duplex mismatch between one of its ports and the given port’s immediate neighbor without the need to set up the Port Monitor function.

Disabling LLDP on the device has the following possible advantages and drawbacks:

- Security aspects:
  - Advantage: The device does not send out any explicit information about itself. This reduces the attack surface.
  - Drawback: The device cannot detect the addition, removal, or reconfiguration of an LLDP-enabled neighbor.
- Functional aspects:
  - Drawback: No Topology discovery: The device cannot help perform a system inventory.
  - Drawback: The device cannot automatically detect, for example, a duplex mismatch. For that, the Port Monitor function needs to be set up.

The above lists are not exhaustive. Evaluate the possible LLDP settings on the device according to your planned LLDP policy.

Enable or disable LLDP globally and choose the port-related operation modes according to your planned LLDP policy. Setting up LLDP on the device may require that other network devices have their own LLDP function appropriately enabled.

ℹ Refer to:

- The "Graphical User Interface" reference manual, chapter "Diagnostics > LLDP > LLDP Configuration" for the device LLDP function
- The "Configuration" user manual, chapter "Operation diagnosis > Topology discovery" for an explanation of LLDP use cases

A Security seal

A.1 Overview

Some devices are equipped with mechanical components that have the function of a security seal. The purpose of the security seal is to establish a barrier that thwarts or impedes possible attempts to manipulate the internal hardware of the device. The security seal can be of different several types. The exact type of security seal depends on the device hardware type.

Table 20: Security seal by device type

Device type	Seal type	Seal location
BRS	-	-
BXS	-	-
OS2	-	-
OS8TX	Device is encapsulated with casting compound.	-
RSP, RSPE	Sealed front panel	-

A.2 Details

The following chapters describe the properties and procedures for the mechanical security components, also called security seals.

Note:
The decommissioning procedures describe only the minimum steps to mark the security seals as decommissioned. Depending on your situation, additional decommissioning steps may be required.

A.2.1 Sealed front panel

Security properties:

- The front panel completely covers the screws that are needed to open the device.
- There are no other screws that permit opening the device.

Tampering evidence:

- The front panel has exposed screws.
- The front panel has cutaways, cuts, scratches, wrinkles or folds, especially in the corners where the screws are located.

Check procedures:

- New device:
  - Check that the front panel is new and has no exposed screws, cutaways, cuts, scratches, wrinkles, or folds in the corners.
- Device before sending it back to the manufacturer for repair or replacement:
  - Check and record the condition of the front panel.
    The front panel shall have no exposed screws, and no cutaways, cuts, scratches, wrinkles, or folds in the corners.
- Repaired device back from manufacturer:
  - If the device and the front panel are both the same:
    Check the condition of the front panel against the recorded condition. The front panel shall be approximately in the same condition as before.
    The front panel shall have no exposed screws, and no cutaways, cuts, scratches, wrinkles, or folds in the corners.
  - If the device is the same but the front panel is new:
    The front panel is new and shall have no exposed screws, and no cutaways, cuts, scratches, wrinkles, or folds in the corners.
  - If the device has been replaced (same device type):
    Check that the front panel is new and has no exposed screws, and no cutaways, cuts, scratches, wrinkles, or folds in the corners.
  - If the device has been replaced (other device type):
    Check according to the new device type’s security seal.

Decommissioning procedure:

- Cut off the front panel corners to expose the screws.
- Scratch the front panel, for example, with a screwdriver.

A.2.2 Encapsulated device

Security properties:

- The device hardware except the connectors and LEDs is encapsulated with a hard casting compound.
- Trying to open the device will leave signs of mechanical processing.

Tampering evidence:

- The casting compound, the connectors, or the LEDs show signs of mechanical processing, like scratches, boreholes or partial application of new casting compound.

Check procedures:

- New device:
  - Check the condition of the casting compound, the connectors, and the LEDs.
    These components shall show no signs of mechanical processing.
- Device before sending it back to the manufacturer for repair or replacement:
  - Check and record the condition of the casting compound, the connectors, and the LEDs.
    These components shall show no signs of mechanical processing.
- Repaired device back from manufacturer:
  - If the device is the same:
    Check the condition of the casting compound, the connectors, and the LEDs against the recorded condition.
    The condition of these components shall only deviate minimally from the recorded condition and show no signs of mechanical processing.
  - If the device has been replaced (same device type):
    Check the condition of the casting compound, the connectors, and the LEDs.
    These components shall be new and show no signs of mechanical processing.
  - If the device has been replaced (other device type):
    Check according to the new device type’s security seal.

Decommissioning procedure:

- Deform the connectors and LEDs with a heavy tool, for example, with a hammer.

B Password strength and policy guide

Note:
This chapter is informational only.

A strong password is hard to break by both a brute-force attack and a dictionary attack. "Hard to break" means that the mean time an attack needs to succeed is higher than a specified time.

A strong password is at the same time reasonably convenient to memorize without the need to write it down or use a password management application.

To make a quantitative statement about which password policy satisfies your specific situation, the following values have to be at hand:

- The required mean attack resistance time
- The maximum accepted breach probability after the mean attack resistance time (if < 50%)
- The maximum assumed attack rate (mitigated or unmitigated)
- The desired password class (high- or low-complexity, see below)

When these values are given, you can look up a password policy that satisfies your requirements (see on page 142 “Password policy lookup tables (quantitative)”).

For a more in-depth approach, the following chapters provide a short introduction to the key concepts of password strength.

The following topics are covered in this chapter:

- A detailed discussion of password classes and password strength
- The suggestion to prefer low-complexity passwords over high-complexity passwords and the reasons for the suggestion
- A general discussion of password policies and the resulting password schemes
- A detailed discussion of password schemes and the resulting password strength
- A precise guide to a recommended password policy, based on quantitative considerations

The following topics are **outside** the scope of this document:

- The automated generation of strong passwords
- The secure administration and distribution of passwords
- A possible password change policy
- The handling of password breaches or leaks
- The human aspects for passwords, like social engineering

B.1 Password classes

Note:
The terms used in this chapter, like "password complexity", will be explained in the course of the sub-chapters.

Passwords can be grouped into 2 classes:

- **High-complexity passwords**:
  - High-complexity passwords have a minimum length.
  - They must consist of characters of the following character types: lowercase characters, upper case characters, digits and special characters.
  - Often, at least one character of each type is required.

  - The resulting password must not contain any word that can be found in a dictionary.
  - The minimum length required by the respective password policy is relatively low.
  - High-complexity passwords are relatively hard to memorize, especially if they are long.
  - Examples are "bZ1/Yc0$", "L{3}qz9M_k", or "*%Gr.43FD7xw".
- **Low-complexity passwords**:
  - Low-complexity passwords consist only of lowercase characters, for example, as a group of words.
  - Other character types are possible but not required.
  - The resulting password typically contains words that can be found in a dictionary.
  - The words in the password may be separated by a special character like "-".
  - The minimum length required by a specific password policy is higher than for high-complexity passwords of comparable strength.
  - Despite their greater length, low-complexity passwords are relatively easy to memorize.
  - Therefore, and counter-intuitively, low-complexity passwords may offer higher practical strength than high-complexity passwords.
  - Examples are "barrel-hamlet-famous", "imagine.lioness.knuckle.manager", or "natality painless yeomanry obligate quenched".

Note:
At the time of writing, high-complexity passwords are in more common use than low-complexity passwords. The reason is that users tend to create short passwords and common password policies favor high-complexity passwords.

B.2 Password policies

A password policy typically has the following properties:

- It stipulates quantitative requirements:
  - The minimum password length
  - The allowed character types from which the password characters shall be taken (typically, the types are: lowercase characters, uppercase characters, digits, and special characters)
  - The minimum number of characters of each type
- It stipulates qualitative requirements:
  - The password must not contain any words from a given dictionary
- It stipulates time requirements:
  - The chosen password must be changed after a specified max. time period.

In essence, a password policy indirectly stipulates:

- The minimum password strength
- The password class (high- or low-complexity)

Notes:

- A password policy is a template for developing password schemes that satisfy given minimum requirements.
- The maximum time after which a password shall be changed has no effect on the password strength.
  - A required interval for changing a given password is reasonable if you assume that your password will be or has already been breached during the interval and you have not noticed.
  - This requirement also takes care of the possibility that a password may have leaked to an attacker.
  - While requiring a maximum interval for changing a password is common for many office and Internet IT systems, embedded systems typically do not enforce a regular password change by themselves.
  - For a system not enforcing regular password change, you can still minimize the probability of an unnoticed, successful password attack by specifying the required attack resistance time much higher than the expected lifetime of the system. This can be accomplished by setting up a strong password policy.

In the following table, the minimum values stipulated by some example password policies are given, along with an exemplary description of the policy results.

Table 21: Password policy examples and qualitative password strength

Min, password length	Min no. of lowercase chars	Min no. of uppercase chars	Min no. of digits	Min no. of special chars	Password type and qualitative strength
6	1	1	1	1	High-complexity password, low strength ⚠
8	1	1	1	1	High-complexity password, medium strength
10	1	1	1	1	High-complexity password, higher strength
24	0	0	0	0	Low-complexity password, high strength

Note:
The qualitative password strength description in the above table assumes low security requirements. Your assessment may associate lower password strengths with the password policy examples given above. The password strength is considered in quantitative detail in the following chapters.

B.3 Password schemes

A password scheme results from a given password policy and has the following properties.

- A password scheme uses a specific password policy as a template.
- A specific scheme is one of several possible schemes that satisfy a specific policy.
- Different schemes can generate passwords of different strength.
- A minimum scheme barely satisfies the policy requirements, but no more.
  - Consequently, a password following a minimum scheme has a minimum strength.
- An extended scheme exceeds the policy’s minimum requirements.
  - A password following an extended scheme typically has larger strength than a password following a minimum scheme but in practice, extended schemes are rarely chosen by users.

Note:
In keeping with a conservative (skeptical) security approach, all password schemes discussed in this chapter are minimum schemes (see on page 128 “Conservative assumptions about users”). This helps ensure that the strength of an actual password meets or exceeds the required strength despite the minimum scheme it is based on.

B.4 Password attack strategies

For an attacker who aims to gain login access by breaking the account password, there are 2 basic attack strategies:

- **Dictionary attack**:
  - A dictionary attack is highly efficient if a password is in the dictionary (list) of passwords the attacker knows.
  - This applies in particular to frequently used passwords on lists that are available on the Internet.
  - For maximum efficiency, these lists are ordered with the most frequently used passwords first, for example "123456", "secret", "password1", or "Password.1".
  - If the real password is not in the attacker’s dictionary, the dictionary attack will fail.
- **Brute-force attack**:
  - A brute-force attack is necessary for highly random passwords that do not contain any word from a dictionary.
  - This attack basically tries all possible passwords for a given password scheme.
  - The number of possible passwords roughly grows exponentially with the password length.
  - A brute-force attack takes much longer than a dictionary attack but will eventually succeed, given enough time and a lack of mitigating factors.

Note:
An attacker can also try to steal a password or provoke a password leak, for example, by social engineering. Thus, for mitigation, passwords must be guarded well. These aspects are outside the scope of this document.

B.5 Basic security assumptions

In keeping with the conservative security approach, this main chapter makes qualitative assumptions about:

- Attackers
- Users
- The attack context

B.5.1 Aggressive assumptions about attackers

- An attacker looks for the most efficient way to gain access.
- To accomplish this, they will first look for the weakest aspects (most frequent existing vulnerabilities) of the target. This may make login attempts entirely redundant from the viewpoint of the attacker.
- If a login attack is necessary, they may use the following strategy:
  - They try to find an interface or a protocol that does not explicitly rate-limit attacks.
  - They try the most frequently used passwords first, so they will start with a dedicated dictionary attack. That is, they try a list of known frequent passwords.
  - If the dictionary attack does not succeed, they may either give up or switch to a brute-force attack.
  - They may either know the username of the account, or assume a low number of frequent usernames and perform a dictionary attack against the username. That is, they may use a list of frequent usernames. They may also try those usernames first that are typically associated with administrator privileges.
- If they do not succeed with the given target, interface, and protocol, they will switch to another target, interface, or protocol.

Conclusion: From a system view, closing or mitigating the weakest vulnerabilities first is necessary.

B.5.2 Conservative assumptions about users

- When users have the choice of either creating their own password or accept a password suggestion randomly generated by a system, users will tend to create their own password. The consequences may be:
  - Given a liberal high-complexity password policy, a user-chosen password will in practice almost always be weaker than a randomly suggested password (see details below).
  - When forced to follow a strict high-complexity password policy, users may experience problems in memorizing the password and thus may tend to either write it down or use an unapproved password management application.
- When choosing a password, users will create the easiest possible password, for example, using only lowercase characters.
- When a password policy enforces a minimum length, users will tend to use an as short as possible password of lowercase characters that just satisfies the minimum length.
- When a password policy also enforces a minimum number of other character types, users will create the easiest possible password that barely satisfies the password policy. That is, they tend to use a minimum scheme (see on page 126 “Password schemes”):
  - When at least one uppercase characters is required, users will tend to use only one uppercase character, and may put it at the start.
  - When at least one digit is required, users will tend to use only one digit. They may put it at the end or replace a single letter with a digit (for example "A" -> "4").

  - When at least one special character is required, users will choose from a limited pool of special characters, and will not exhaust the possible pool of special characters.
  - The properties of user-chosen passwords may make these passwords more vulnerable to a dictionary attack, and possibly even to a brute-force attack.
- When given the choice of either creating a short, complex password or a longer, less complex password, users will tend to choose a short, complex password that barely satisfies the required password policy, although a longer, even less-complex password may be stronger.
- When asked to create a long password, users will also create a password that barely satisfies the required password policy.

Conclusion: From a system view, a password policy needs to be strong enough so passwords created according to the resulting minimum scheme have sufficient strength.

B.5.3 Conservative assumptions about the attack context

- The username of an account under attack is assumed to be already known to the attacker. Username examples are "user", "admin", or "administrator".
  - This essentially eliminates the effort and time for guessing the username and is a typical skeptical security assumption.
- The attack rate may or may not be limited by system settings. In the worst case, it is unlimited.
  - In the absence of any network concept that detects anomalies or intrusions, this in essence means that the attacker is able to sustain a high attack rate for a long time.
- When performing a dictionary attack, the attacker has insider knowledge, that is, they already know the dictionary the password generation system uses to suggest long, low-complexity passwords.

Note:
We will shortly see that the seemingly paranoid assumption of an attacker knowing the complete password dictionary is not really a security problem. That is, a system-suggested, sufficiently long, low-complexity password can be both stronger **and** also easier to memorize than a typical high-complexity password of similar strength. This may seem counterintuitive but can be proven quantitatively, while assuming reasonable and even skeptical conditions.

B.6 Quantitative password strength

B.6.1 High-complexity passwords

The strength of a high-complexity password can be quantified as the number of possible passwords for a given scheme.

Note:
The preferred attack method to crack a high-complexity password is a brute-force attack. A good, high-complexity password will not give in to a dictionary attack.

For a high-complexity password of a given scheme, the number of possible passwords depends on the character type (more precisely: on the size of the pool from which the respective character is taken) and on how many characters of the given type appear.

The expected password strength depends on the assumptions how a password is created:

- **Optimistic password strength**:
  - Only truly random passwords have the highest possible expected information content.
  - Reasonable passwords of this type typically must be generated by an application.
  - **Caveat**: User-chosen high-complexity passwords typically have significantly less "randomness" (that is, entropy) and therefore tend to be weaker.
- **Skeptic password strength**:
  - When users are faced with a password policy, users will tend to make up a password scheme that barely satisfies the policy, that is, they will choose a minimum scheme.
  - User-chosen passwords therefore tend to have lower-than-possible strength.
  - The reason is that people tend to use certain characters more often than others.
  - For example, the character "e" appears in an general, English-language text with a probability of approx. 12.5% (1/8) and not with the probability of 3.8% (1/26).
  - To account for the unevenly distributed character frequencies to and pursue a skeptic approach, we can calculate with a smaller pool size than 26, for example, by assuming 8 (this approximates the frequency of the most frequent character, here, "e").
  - Similarly, to account for the unevenly distributed digit and special character frequencies, we can also calculate with a smaller pool size, for example, by also assuming 8.

The number of possible different high-complexity passwords of a given scheme is therefore:

$$N_{ph} = L^{l} \times U^{u} \times D^{d} \times S^{s}$$

Where:

- N_{ph}: Number of possible high-complexity passwords
- L: Pool size of lowercase characters (constant)
- l: Number of lowercase characters in the password (variable)
- U: Pool size of uppercase character (constant)
- u: Number of uppercase characters in the password (variable)
- D: Pool size of digits (constant)
- d: Number of digits in the password (variable)
- S: Pool size of special characters (constant)
- s: Number of special characters in the password (variable)

We see that the password strength grows with the length of the password. Unsurprisingly, we see that adding more characters, digits or special characters to an existing password makes the resulting password stronger.

Note:
A simple generator for high-complexity passwords, following a minimum password scheme, might in fact sometimes suggest passwords like "123456", "abcdef" or "secret". These passwords are weak because they most likely are in an attacker's dictionary. The skeptic probability for a randomly generated password to be like one of the given examples is $8^{-6} \approx 3.81 \times 10^{-6}$. Because there are many known weak passwords, the probability of a randomly generated password matching one of the known weak passwords is considerable – possibly too high to be accepted. Therefore, **checking a system-suggested or user-chosen high-complexity password against a list of known weak passwords can be regarded as mandatory.**

Example (optimistic strength)

An example password policy requires a length of 8 characters, with at least one lowercase character, one uppercase character, one digit, and one special character. Given the choice of making up their own password, the user chooses to use 5 lowercase characters, one uppercase character, one digit, and one special character.

In keeping with the conservative security approach given, the assumed password scheme chosen by the user is a minimum scheme that barely satisfies the password policy.

Table 22: High-complexity password components, optimistic strength

Character class ID	Class description	Pool characters	Assumed pool size
L	Lowercase characters	a-z	26
U	Uppercase characters	A-Z	26
D	Digits	0-9	10
S	Special characters	!"#$%&()*+'.-/:;	16[1]

[1] The special character pool size is given as 16 although the ASCII codes provides for 32 special characters. The reason for the smaller assumed pool size is that some characters may be impossible or hard to type on a given keyboard and may therefore not be chosen by a user.

The optimistic number of possible passwords of this scheme is therefore:

$$N_{pho} = 26^5 \times 26^1 \times 10^1 \times 16^1 = 49{,}426{,}524{,}160 \approx 4.94 \times 10^{10}$$

Where:

- N_{pho}: Number of possible high-complexity passwords, optimistic approach

Note:
Modifying an existing password by **replacing** lowercase characters by digits or special characters can actually make the password **weaker**. This seems to contradict the recommendation to include digits and special characters in a password. The explanation is that replacing lowercase characters by digits or special characters only helps against dictionary attacks, not against brute-force attacks. The recommendation to include digits and special characters is based on the assumption that the password prior to the modification is vulnerable to a dictionary attack. That again means that the original password wasn't a high-complexity password to begin with.

Example (skeptic strength)

Table 23: High-complexity password components, skeptic strength

Character class ID	Class description	Pool characters	Assumed, reduced pool size
L	Lowercase characters	a-z	8
U	Uppercase characters	A-Z	8
D	Digits	0-9	8
S	Special characters	!#$&+.-/ (example)	8

Assuming the same password scheme as above, but with a reduced pool size of 8 for each character type to account for frequent characters or digits like "e", "1", or ",", the skeptic number of possible passwords of this scheme is therefore:

$N_{phs} = 8^5 \times 8^1 \times 8^1 \times 8^1 = 8^8 = 2^{24} = 16{,}777{,}216 \approx 1.67 \times 10^7$

Where:
- N_{phs}: Number of possible high-complexity passwords, skeptic approach

We see that the skeptic password strength is much smaller than the optimistic strength.

B.6.2 Low-complexity passwords

The strength of a low-complexity password can also be quantified as the number of possible passwords for a given scheme.

Note:
The preferred attack method to crack a low-complexity password is a dictionary attack. A brute-force attack is possible but practically futile. Given the bigger length of a low-complexity password (for example, 24 lowercase characters), the skeptic number of possible passwords is on the order of 10^{21}. The optimistic number of possible passwords is even on the order of 10^{33}.

A low-complexity password contains words from a dictionary (word list). The strength of a low-complexity password depends on the following aspects:
- It strongly depends on the number of words in the password.
- It moderately depends on the size of the dictionary.
- It marginally depends on the detailed rules how passwords are chosen from the dictionary.
- It is virtually independent of the word length as long as a minimum length is maintained.

For the sake of security skepticism, let’s make 4 conservative assumptions:
- The dictionary from which the words are taken (for example, by a password-generating application) has only straightforward size (for example, only 2,048 entries).
- The entire dictionary is already known to the attacker. This is a very conservative assumption.
- Words from the dictionary shall be selected only once.
  - This excludes the equivalent of weak passwords like "111111" or "aaaaaa".
- Words selected from the dictionary shall not be adjacent to any of the words already selected.
  - This excludes the equivalent of weak of passwords like "123456", "654321, "abcdef" or "fedcba".

We will shortly see that a low-complexity password scheme following these assumptions still results in passwords of high skeptic strength. The optimistic strength for a low-complexity password does not need to be examined in detail because such a password would in essence describe a long, high-complexity password, against which a dictionary attack is practically futile.

There is one additional condition that needs to be satisfied:

- The minimum word length shall be high enough to contain much more possible words than there are words in the dictionary.
  - This ensures that the list entropy is not undermined by a low word entropy (we will discuss entropy shortly, (see on page 139 “Password entropy”)). This condition is easily satisfied by a password policy requiring a minimum number of characters.

Table 24: Low-complexity password properties

Parameter ID	Parameter	Description
S	Dictionary size	Number of words in the dictionary
w	Number of words	Number of such words in the password.

The approximate number of possible different low-complexity passwords of a given scheme is therefore:

$$N_{plo} \approx S^{w}$$

Where:

- N_{plo}: Number of possible low-complexity passwords, optimistic approach
- S: Dictionary size
- w: Number of words used in the password

Note:
For w ≥ 2, the above equation gives a slightly optimistic strength. Compared to the exact value, assuming a dictionary size of 2,048 and 6 words, it is off by +2.3%. For fewer words, the deviation is lower. For w = 1, the equation gives the correct strength.

The exact equation is:

$$N_{ple} = S \times (S - 3) \times (S - 6) \times \ldots \times (S - 3 \times (w-1))$$

Where:

- N_{ple}: Number of possible low-complexity passwords, exact approach

Note:
The multipliers S - 3, S - 6 etc. stem from the fact that the choice of the first word has S possibilities but the choice of the 2nd word has only (S - 3) possibilities. This is because the first word chosen, its immediate predecessor as well as its immediate successor shall not be chosen again, according to the last of the above given skeptic assumptions.

This unwieldy formula can safely be approximated by a skeptic approximation, that is, by dividing the result of the approximate, optimistic equation by 2:

$$N_{pls} = S^{w} / 2 \text{ (for } w \geq 2\text{)}$$

Where:

- N_{pls}: Number of possible low-complexity passwords, skeptic approach

Example

Note:
In keeping with the conservative security approach, the assumed password scheme chosen by the user is a minimum scheme that barely satisfies the password policy. The word list is assumed to contain only 2,048 words. The minimum word length is 6.

An example password policy requires a length of 24 characters (therefore 4 words with 6 characters minimum length each), with at least 1 lowercase character. Uppercase characters, digits, and special characters are possible but not required. Given the choice of making up their own password, a user chooses the password "barrel-hamlet-famous-staple", possibly with the help of an application.

The number of possible passwords of this scheme is therefore:

$$N_{pl} = 2{,}048^4 / 2 = 2^{43} = 8{,}796{,}093{,}022{,}208 \approx 8.79 \times 10^{12}$$

Note:
Despite the above, conservative assumptions, the low-complexity password strength in this example is much higher than for the aforementioned high-complexity password examples. This holds even if we compare the conservative strength of the low-complexity password to the optimistic strength of the high-complexity password.

B.7 Attack resistance time (quantitative)

The theoretical (but impractical) resistance to an attack can be calculated as the maximum time the password withstands an attack until it is broken with 100% probability.

This time can be calculated as the number of necessary attacks, divided by the attack rate:

$T_{sb} = N_a / r_a$

Where:

- T_{tb}: Theoretical max. time to 100% probable password breach, in seconds
- N_a: Number of necessary attacks
- r_a: Attack rate (in attacks per second)

Of course, accepting a 100% probability for a password breach is a weak concept. In practice, a 50% probability is often assumed instead because the assumption of 50% makes the equations a bit easier.

The practical resistance to an attack is typically calculated as the mean time the password withstands the attack until it is broken with 50% probability. This is half the time for a 100% probability breach:

$T_{sp} = N_a / r_a / 2$

Where:

- T_{pb}: Mean time to practical (50% probable) password breach

The (unsurprising) result is that the attack resistance time increases with a higher number of possible different passwords and decreases with higher attack rate.

The (unsurprising) conclusion is: To make a login password as strong as possible, you have 2 possibilities, and you can combine these:

- Specify a strong password policy by setting up an appropriate password policy, either for high-complexity or for low-complexity passwords, thus enabling strong-enough resulting minimum schemes.
- Wherever possible, set up a login policy to lower the effective attack rate for a given interface and protocol.

B.7.1 Examples, unmitigated attack rate

In keeping with the conservative security approach, the assumed attack rate is high and unmitigated, so we assume 1,000 attacks per second. An example for such a possible high rate is an attack using SNMPv3 get requests. SNMP has no obvious means of attack rate mitigation. We accept a 50% probability of a breach.

For the password example strengths in the previous chapters, the mean attack resistance time is:

Table 25: Attack resistance time for different password scheme examples, for an unmitigated attack rate

Password class	Approach	Password strength	Unmitigated attack rate per second	Attack resistance time	
				in seconds	in usual units
High complexity	Optimistic	4.94×10^{10}	1,000	2.47×10^{7}	9.53 months
	Skeptic	1.67×10^{7}	1,000	8.38×10^{3}	2.33 hours
Low complexity	Skeptic	8.79×10^{12}	1,000	4.39×10^{9}	139 years

We see that despite the very conservative assumptions for the low-complexity password, the low-complexity password results in a much attack higher attack resistance time than a high-complexity passwords. This holds even if we compare to the optimistic case of the high-complexity password.

B.7.2 Attack rate mitigation

The rate (strength) of a dictionary or brute-force attack can be given as the number of login attempts per second.

The lower the attack rate, the longer it takes to reach the mean number of attempts until the password is accepted.

Let’s assume that an attacker is capable of delivering many attacks per second to a certain interface and protocol (an attack rate ≥ 1 / sec = 3,600 / hour). How this affects the system under attack depends on if the system has mitigating parameters set up. Examples for protocols offering such mitigation parameters are HTTPS and SSH.

There are 2 settings that provide mitigation:
- The maximum number of successive failed login attempts until the system enforces a waiting time
- The enforced waiting time the system has set up.

The assumed high attack rate is thus effectively reduced to:

$r_{am} = n_{sf} / t_w$

Where:
- r_{am}: Mitigated attack rate
- n_{sf}: Number of successive failed login attempts
- t_w: The enforced waiting time

We see that the mitigated attack rate only depends of the mitigating parameters’ values, not on the high attack rate originally assumed. This makes these mitigations parameters particularly effective.

Note:
This approximate equation is slightly skeptic. The real mitigated attack rate is slightly lower.

Mitigation examples

Skeptic example: An example system is set up to ignore logins after 10 successive failed login attempts. This is a fairly high value, assuming users tend to value convenience. After the condition triggers, the target system enforces a one-minute wait time (a fairly low value, also convenient) and ignores any login attempts during that time. What is convenient for the users, is regarded skeptically from a security perspective.

r_{am} = 10 / 1 min = 10 / min = 600 / hour.

Optimistic example: A system ignore logins after already 5 successive failed login attempts (a smaller value) and then enforces a 2-minute wait time (a larger value). These values may be more inconvenient for the users, but are regarded as more desirable from a security perspective.

r_{am} = 5 / 2 min = 2.5 / min = 150 / hour.

We see that setting up reasonable attack mitigation parameters can significantly lower the effective attack rate, often by an order of magnitude or more.

B.7.3 Examples, mitigated attack rate

The login with the protocols HTTPS and SSH provides mitigating parameters. In keeping with the conservative security approach, the assumed mitigated attack rate is relatively high because the mitigation parameters were chosen to be convenient for the users. So we assume 600 attacks per hour (that is, 10 per minute or 1/6 per second).

For the password example strengths in the previous chapters, the mean attack resistance time is:

Table 26: Attack resistance time for different password scheme examples, for a mitigated attack rate

Password class	Approach	Password strength	Mitigated attack rate per second	Attack resistance time	
				in seconds	in usual units
High complexity	Optimistic	4.94×10^{10}	1/6	1.48×10^{11}	4,698 years
	Skeptic	1.67×10^{7}	1/6	5.03×10^{7}	1.59 years
Low complexity	Skeptic	8.79×10^{12}	1/6	2.63×10^{13}	836,194 years

Note:
We see that attack rate mitigation can be very effective in raising the provided attack resistance time. However, this only applies to protocols that offer the said mitigation parameters. In the worst case (that is, with a skeptic approach), we still have to assume the unmitigated attack rate, as may be the case for the SNMPv3 protocol.

B.8 Required attack resistance time (quantitative)

For a required mean attack resistance time, an assumed attack rate, and a specific, accepted breach probability, we can calculate the required password strength:

$N_{pr} = T_{ar} \times r_a \times (1 / P_b)$

Where:

- N_{pr}: Required password strength
- T_{ar}: Required attack resistance time
- r_a: Assumed tack rate (in attacks per second), either mitigated or unmitigated
- P_b: Accepted breach probability when the required mean attack resistance time has elapsed

The (unsurprising) result is that the required password strength increases with a higher required attack resistance time, with a higher assumed attack rate and with a lower accepted breach probability.

The commonly accepted breach probability is 50%. This gives the simplified equation:

$N_{pr} = T_{ar} \times r_a \times 2$

Note:
Your situation may require a lower breach probability than 50%. In this case, use the former equation.

B.9 Password entropy

The strength of a given password scheme can be expressed as:
- Possibilities (symbol N): The number of possible different passwords
- Entropy (symbol H): The expected information content for a random number in the range 1…N.

Entropy in the context of information theory has the following properties:
- It has the unit "shannon" (short: "Sh"). It can be non-integer.
- Its value can be interpreted as the minimum number of bits required to hold a number in the range 1…N. If the entropy value is non-integer, it has to be rounded up to the nearest integer to give the minimum number of bits.

The password entropy is a more convenient way of representing the password strength than the number of possible passwords. Whereas the typical number of possible passwords for a given scheme is > 10^6, the entropy of a reasonable strong password typically is in the range 20…45. The reason is that there is a logarithm involved.

The entropy can be calculated from the password strength:

$$H_p = \log_2 (N_p)$$

Where:
- H_p: The password entropy (min. number of bits required to represent N_p)
- $\log_2$: The Logarithm function to the base of 2
- N_p: The password strength (as the number of possibilities)

The calculated entropy of a given password strength can be non-integer number. In keeping with security skepticism, the number of bits associated with the entropy is rounded to the nearest integer in the following way:
- For the entropy **required** for a certain password scheme, the number of bits is rounded **up**.
- For the entropy **provided** by a certain password scheme, the number of bits is rounded **down**.

Generally, there are 3 basic types of entropy in relation to password strength:
- The **Shannon entropy** H_1 represents the **detailed** approach.
- The **max. entropy** H_{max} represents the **optimistic** approach.
- The **min. entropy** H_{min} represents the **skeptic** approach.

As we follow the skeptic approach, we only deal with the **min. entropy** H_{min}.

In this main chapter, using only the min. entropy is incorporated by the following approach:
- **For high-complexity passwords**, the applied skeptic pool size for any character type is chosen to be only 8, instead of 26, 10, or 16 (or even 32). This results in 3 sh per character.
- **For low-complexity passwords**:
  - Only the size of a known dictionary (for example, 2,048) is taken into account. This results in a dictionary entropy of 11 sh.
  - The length of individual words is ignored, only a minimum length is required (for example, 6).
  - The strength of a given password scheme is calculated conservatively, by dividing the approximate formula’s value by 2, if the number of words in the password is ≥ 2.

B.10 Calculating the required password entropy

For a required mean attack resistance time, a specified attack rate, and a specified, accepted breach probability, we can calculate the required password strength as the required password entropy.

Given the above equation $N_{pr} = T_{ar} \times r_a \times (1 / P_b)$ (see on page 138 “Required attack resistance time (quantitative)”), the entropy is:

$$H_{prb} = \log_2 (N_{pr}) = \log_2 (T_{ar} \times r_a \times (1 / P_b))$$

$$H_{prb} = \log_2 (T_{ar} \times r_a) - \log_2 (P_b)$$

Where:

- H_{prb}: Required password entropy for the required breach probability P_b
- N_{pr}: The required password strength (as the number of possibilities)
- T_{ar}: Required attack resistance time
- r_a: Assumed attack rate (in attacks per second), either mitigated or unmitigated
- P_b: Accepted mean breach probability when the required mean attack resistance time has elapsed

In theory, a breach probability of 100% is possible (although mostly not accepted). This leads to:

$$H_{pr100} = \log_2 (T_{ar} \times r_a / 1) = \log_2 (T_{ar} \times r_a)$$

Where:

- H_{pr100}: The theoretically required password entropy for a breach probability of 100%

In literature, a breach probability of 50% is often accepted. This leads to:

$$H_{pr50} = \log_2 (T_{ar} \times r_a / 0.5) = \log_2 (T_{ar} \times r_a) + \log_2 (2) = \log_2 (T_{ar} \times r_a) + 1$$

$$H_{pr50} = H_{p100} + 1$$

Where:

- H_{pr50}: The required password entropy for a breach probability of 50%

We see that an accepted breach probability of 50% raises the required password entropy by 1 sh, in comparison to the theoretical (and practically unacceptable) breach probability of 100%.

The generalized formula for a required password entropy, assuming a specified breach probability is:

$$H_{prb} = H_{p100} - \log_2 (P_{br}) = H_{p100} + | \log_2 (P_{br}) |$$

Where:

- H_{prb}: The required password entropy for an arbitrary breach probability
- P_{br}: The required breach probability (< 1) within the attack time.

We see that an arbitrarily required breach probability < 100% simply adds more required entropy to the theoretical (and undesirably low) password entropy H_{pr100}.

Note:
Because $P_{br} < 1$, $\log_2 (P_{br}) < 0$ and therefore $-\log_2 (P_{br}) > 0$.

B.11 Password policy lookup tables (quantitative)

To find a password policy that quantitatively meets the specified requirements, we need the following values at hand:

- The required mean attack resistance time
- The maximum accepted breach probability after the mean attack resistance time (if < 50%)
- The maximum assumed attack rate (mitigated or unmitigated)
- The desired password class (high- or low-complexity)

We can then look up the required password policy, using a series of tables:

B.11.1 Password entropy lookup tables

Table input:

- T_{ar}: Required attack resistance time
- r_a: Assumed attack rate

Table output:

- H_{pr50}: Required password entropy for an accepted breach probability of 50%

Table 27: Lookup table for required password entropy (in Sh, rounded up)

Required attack resistance time T_{ar}	**Assumed attack rate r_a**					
	1 / min.	**10 / min.**	**1 / sec.**	**10 / sec.**	**100 / sec.**	**1,000 / sec.**
1 day	12	15	18	21	25	28
1 week	15	18	21	24	27	31
1 month	17	20	23	26	29	33
1 year	21	24	26	30	33	36
10 years	24	27	30	33	36	40
100 years	27	30	33	36	40	43
1,000 years	30	34	36	40	43	46

Password entropy lookup table for < 50% breach probability

Table input:

- P_{br}: Required max. breach probability after the acceptable mean attack time has elapsed

Table output:

- H_{ab}: Required additional password entropy for breach probability P_{br}

Table 28: Lookup table for additional required password entropy (in Sh, rounded up)

Accepted max. breach probability P_{br}	Required additional password entropy H_{ab}
50%	0
10%	3
1%	6
1‰ (10^{-3})	9
100 ppm (10^{-4})	13
10 ppm (10^{-5})	16
1 ppm (10^{-6})	19
100 ppb (10^{-7})	23
10 ppb (10^{-8})	26
1 ppb (10^{-9})	29

For < 50% breach probability, add the required password entropies from the 2 tables:

$$H_{prb} = H_{pr50} + H_{ab}$$

Where:

- H_{prb}: Required password entropy for a breach probability P_{br} < 50%
- H_{pr50}: Required password entropy for standard breach probability of 50%
- H_{ab}: Additional required entropy for an accepted breach probability < 50%

B.11.2 Password policy lookup table, low-complexity passwords

Table input:

- H_{prb}: Required password entropy for the required breach probability

Constants:

- S: Dictionary size, assumed to be 2,048
- L_w: Minimum length of any word in dictionary: assumed to be 6

Table output:

- n_w: Minimum number of words required by the password policy
- n_c: Minimum overall number of characters required by the password policy

Table 29: Lookup table for password policy (for low-complexity passwords)

Required password entropy (H_{prb})	Required no. of words n_w	Required no. of characters n_c	Required no. of any character type	Provided entropy (skeptical)
12…21	2	**12**	0	21
22…32	3	**18**	0	32
33…43	4	**24**	0	43
44…54	5	**30**	0	54
55…65	6	**36**	0	65
66…75	7	**42**	0	76

Notes on low-complexity passwords (see on page 132 “Low-complexity passwords”):

- **If only lowercase characters are used, this permitted.** This is a conservative approach. Other character types are possible but will not increase the provided password entropy.
  - Reason: The entropy of a low-complexity password is already calculated in a very conservative way by the dictionary entropy.
- **The password policy need not require a minimum number of other character types.**
  - This is why 0 is given as the requirement in the table above.
- The number of words in the password is a required minimum.
  - A higher word count will **significantly** increase the password entropy.
- The dictionary size is assumed to be 2,048 (11 sh of entropy). This is a conservative approach.
  - Higher dictionary sizes will result in **moderately** higher password entropy. For example, a dictionary size of 4,096 represents 12 sh of entropy.
- The detailed rules how passwords are chosen from the dictionary, have a **marginal** effect on the entropy: The stricter the rules, the lower the skeptic entropy.
- The minimum word length is assumed to be 6. This is a conservative approach. Higher minimum word lengths will **not** increase the password entropy.
  - Reason: An individual word’s entropy must be much higher than the dictionary entropy, the key parameter for a low-complexity password. Only then, the dictionary entropy is unimpaired by the word entropy.
  - Calculation: For 11 sh of dictionary entropy and 3 sh skeptic entropy for a lowercase character, we need words with at least 4 characters. To make a conservative approximation, we chose a word length of 6 which represents 18 sh of skeptic entropy.

B.11.3 Password policy lookup table, high-complexity passwords

Table input:

- H_{prb}: Required password entropy for the accepted breach probability

Constants:

- L: Pool size of lowercase characters (assumed to be 8)
- U: Pool size of uppercase character (assumed to be 8)
- D: Pool size of digits (assumed to be 8)
- S: Pool size of special characters (assumed to be 8)

Table output:

- n_c: Required total number of characters in the password

Table 30: Lookup table for password policy (for low-complexity passwords)

Required password entropy (H_{prb})	Req. total chars (n_c)	Req. lowercase chars (l)	Req. uppercase chars (u)	Required digits (d)	Req. special chars (s)
12…24	**8**	**1**	**1**	**1**	**1**
25…27	**9**	**1**	**1**	**1**	**1**
28…30	**10**	**1**	**1**	**1**	**1**
31…33	**11**	**1**	**1**	**1**	**1**
34…36	**12**	**1**	**1**	**1**	**1**
37…39	**13**	**1**	**1**	**1**	**1**
40…42	**14**	**1**	**1**	**1**	**1**
43…45	**15**	**1**	**1**	**1**	**1**
46…48	**16**	**1**	**1**	**1**	**1**
49…51	**17**	**1**	**1**	**1**	**1**
52…54	**18**	**1**	**1**	**1**	**1**
55…57	**19**	**1**	**1**	**1**	**1**
58…60	**20**	**1**	**1**	**1**	**1**
61…63	**21**	**1**	**1**	**1**	**1**
64…66	**22**	**1**	**1**	**1**	**1**
67…69	**23**	**1**	**1**	**1**	**1**
70…72	**24**	**1**	**1**	**1**	**1**
73…75	**25**	**1**	**1**	**1**	**1**

Note:
The suggested password length starts with 8. The required password entropies in the range 12…21 sh could theoretically be satisfied with a shorter password length 4…7. These short password policies are not suggested because, from a skeptic security perspective, the resulting passwords are highly susceptible to dictionary attacks as well as brute-force attacks.

Note on the required numbers of lowercase characters (l), uppercase characters (u), digits (d), and special characters (s):

- All characters types are required to appear a minimum number of times in the password policy, for example, 1 per type.
- Requiring a higher minimum number for the digits or special characters will **not** yield higher password entropy because the skeptic assumptions about the pool sizes for the character types are the same.
- A password policy should therefore allow for the other characters but only require a minimum number of 1.
- Theoretically, a minimum number of 0 would also suffice if the password were strictly random, for example, created by an application.
- In practice, with user-chosen passwords, this is not viable: Users may understand such a policy as an invitation to create weak passwords, for example, consisting only of lowercase characters or digits, like "abcdefgh" or "12345678".

C Index

D Further support

Technical questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You find the addresses of our partners on the Internet at www.hirschmann.com.

A list of local telephone numbers and email addresses for technical support directly from Hirschmann is available at hirschmann-support.belden.com. This site also includes a free of charge knowledge base and a software download section.

Technical Documents

The current manuals and operating instructions for Hirschmann products are available at doc.hirschmann.com.

Customer Innovation Center

The Customer Innovation Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
  You find the training courses on technology and products currently available at www.belden.com/solutions/customer-innovation-center.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Customer Innovation Center, you decide against any compromise in any case. Our client-customized package leaves you free to choose the service components you want to use.

E Readers' Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

	Very Good	Good	Satisfactory	Mediocre	Poor
Precise description	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Comprehensive	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

Did you discover any errors in this manual?
If so, on what page?

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

E-mail:

Date / Signature:

Dear User,

Please fill out and return this page
- as a fax to the number +49 (0)7127/14-1600 or
- per mail to
  Hirschmann Automation and Control GmbH
  Department 01RD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen
  Germany

HIRSCHMANN

A BELDEN BRAND