Modicon MCSESM, MCSESP Series

Managed Switch Security

User Guide

Original instructions

EIO0000005492.00
03/2026

www.se.com

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

Safety Information

Important Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

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

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

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

Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

Before You Begin

Do not use this product on machinery lacking effective point-of-operation guarding. Lack of effective point-of-operation guarding on a machine can result in serious injury to the operator of that machine.

⚠ WARNING

UNGUARDED EQUIPMENT

- Do not use this software and related automation equipment on equipment which does not have point-of-operation protection.
- Do not reach into machinery during operation.

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

This automation equipment and related software is used to control a variety of industrial processes. The type or model of automation equipment suitable for each application will vary depending on factors such as the control function required, degree of protection required, production methods, unusual conditions, government regulations, etc. In some applications, more than one processor may be required, as when backup redundancy is needed.

Only you, the user, machine builder or system integrator can be aware of all the conditions and factors present during setup, operation, and maintenance of the machine and, therefore, can determine the automation equipment and the related safeties and interlocks which can be properly used. When selecting automation and control equipment and related software for a particular application, you should refer to the applicable local and national standards and regulations. The National Safety Council's Accident Prevention Manual (nationally recognized in the United States of America) also provides much useful information.

In some applications, such as packaging machinery, additional operator protection such as point-of-operation guarding must be provided. This is necessary if the operator's hands and other parts of the body are free to enter the pinch points or other hazardous areas and serious injury can occur. Software products alone cannot protect an operator from injury. For this reason the software cannot be substituted for or take the place of point-of-operation protection.

Ensure that appropriate safeties and mechanical/electrical interlocks related to point-of-operation protection have been installed and are operational before placing the equipment into service. All interlocks and safeties related to point-of-operation protection must be coordinated with the related automation equipment and software programming.

NOTE: Coordination of safeties and mechanical/electrical interlocks for point-of-operation protection is outside the scope of the Function Block Library, System User Guide, or other implementation referenced in this documentation.

Start-up and Test

Before using electrical control and automation equipment for regular operation after installation, the system should be given a start-up test by qualified personnel to verify correct operation of the equipment. It is important that arrangements for such a check are made and that enough time is allowed to perform complete and satisfactory testing.

⚠WARNING

EQUIPMENT OPERATION HAZARD

- Verify that all installation and set up procedures have been completed.
- Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices.
- Remove tools, meters, and debris from equipment.

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

Follow all start-up tests recommended in the equipment documentation. Store all equipment documentation for future references.

Software testing must be done in both simulated and real environments.

Verify that the completed system is free from all short circuits and temporary grounds that are not installed according to local regulations (according to the National Electrical Code in the U.S.A, for instance). If high-potential voltage testing is necessary, follow recommendations in equipment documentation to prevent accidental equipment damage.

Before energizing equipment:

- Remove tools, meters, and debris from equipment.
- Close the equipment enclosure door.
- Remove all temporary grounds from incoming power lines.
- Perform all start-up tests recommended by the manufacturer.

Operation and Adjustments

The following precautions are from the NEMA Standards Publication ICS 7.1-1995:

(In case of divergence or contradiction between any translation and the English original, the original text in the English language will prevail.)

- Regardless of the care exercised in the design and manufacture of equipment or in the selection and ratings of components, there are hazards that can be encountered if such equipment is improperly operated.
- It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer’s instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer’s instructions and the machinery used with the electrical equipment.
- Only those operational adjustments required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

About the Document

Document Scope

This document describes how to help improve the security of an industrial communication network by applying the IEC 62443 (Security of Industrial Automation and Control Systems) series of standards as a framework when working with MCSESM and MCSESP series managed switches.

This document is for SL-C2. SL-C1 is only mentioned on page 22 and then gives way to SL-C2.

This document is intended for Ethernet network planners, commissioners, administrators, operators, maintenance personnel, and decommissioning personnel. The contents may also be useful for solution providers, sales partners, and system integrators.

Validity Note

This document has been updated for the release of the firmware versions available at the publication date of this document.

Product Related Information

WARNING

LOSS OF CONTROL

- Perform a Failure Mode and Effects Analysis (FMEA), or equivalent risk analysis, of your application, and apply preventive and detective controls before implementation.
- Provide a fallback state for undesired control events or sequences.
- Provide separate or redundant control paths wherever required.
- Supply appropriate parameters, particularly for limits.
- Review the implications of transmission delays and take actions to mitigate them.
- Review the implications of communication link interruptions and take actions to mitigate them.
- Provide independent paths for control functions (for example, emergency stop, over-limit conditions, and error conditions) according to your risk assessment, and applicable codes and regulations.
- Apply local accident prevention and safety regulations and guidelines.[1]
- Test each implementation of a system for proper operation before placing it into service.

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

[1] For additional information, refer to NEMA ICS 1.1 (latest edition), "Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control" and to NEMA ICS 7.1 (latest edition), "Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems" or their equivalent governing your particular location.

WARNING

UNINTENDED EQUIPMENT OPERATION

- Only use software and hardware components approved by Schneider Electric for use with the system.
- Update your application program every time you change the physical hardware configuration.

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

General Cybersecurity Information

In recent years, the growing number of networked machines and production plants has seen a corresponding increase in the potential for cyber threats, such as unauthorized access, data breaches, and operational disruptions. You must, therefore, consider all possible cybersecurity measures to help protect assets and systems against such threats.

To help keep your Schneider Electric products secure and protected, it is in your best interest to implement the cybersecurity best practices as described in the Cybersecurity Best Practices document.

Schneider Electric provides additional information and assistance:

- Subscribe to the Schneider Electric security newsletter.
- Visit the Cybersecurity Support Portal web page to:
  - Find Security Notifications.
  - Report vulnerabilities and incidents.
- Visit the Schneider Electric Cybersecurity and Data Protection Posture web page to:
  - Access the cybersecurity posture.
  - Learn more about cybersecurity in the cybersecurity academy.
  - Explore the cybersecurity services from Schneider Electric.

Environmental Data

For product compliance and environmental information, refer to the Schneider Electric Environmental Data Program.

Related Documents

Title of documentation	Reference number
Modicon MCSESM, MCSESP Series Managed Switch Installation Guide	QGH59091 (EN) QGH59094 (FR) QGH59093 (DE) QGH59096 (IT) QGH59095 (ES) QGH59097 (CN)
Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide	QGH59084 (EN) QGH59087 (FR) QGH59086 (DE) QGH59089 (IT) QGH59088 (ES) QGH59090 (CN)
Modicon MCSESM, MCSESP Series Managed Switch Command Line Interface User Guide	QGH59098 (EN)
Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide	QGH59056 (EN) QGH59080 (FR) QGH59058 (DE) QGH59082 (IT) QGH59081 (ES) QGH59083 (CN)
Modicon Controller Platform Cybersecurity, User Guide	EIO0000001999 (ENG) EIO0000002004 (CHS) EIO0000002001 (FRE) EIO0000002000 (GER) EIO0000002002 (ITA) EIO0000002003 (SPA)

To find documents online, visit the Schneider Electric download center (www.se.com/ww/en/download/).

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

Terminology Derived from Standards

The technical terms, terminology, symbols and the corresponding descriptions in the information contained herein, or that appear in or on the products themselves, are generally derived from the terms or definitions of international standards.

In the area of functional safety systems, drives and general automation, this may include, but is not limited to, terms such as *safety*, *safety function*, *safe state*, *fault*, *fault reset*, *malfunction*, *failure*, *error*, *error message*, *dangerous*, etc.

Among others, these standards include:

Standard	Description
IEC 61131-2:2007	Programmable controllers, part 2: Equipment requirements and tests.
ISO 13849-1:2023	Safety of machinery: Safety related parts of control systems. General principles for design.
EN 61496-1:2020	Safety of machinery: Electro-sensitive protective equipment. Part 1: General requirements and tests.
ISO 12100:2010	Safety of machinery - General principles for design - Risk assessment and risk reduction
EN 60204-1:2006	Safety of machinery - Electrical equipment of machines - Part 1: General requirements
ISO 14119:2013	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection
ISO 13850:2015	Safety of machinery - Emergency stop - Principles for design
IEC 62061:2021	Safety of machinery - Functional safety of safety-related electrical, electronic, and electronic programmable control systems
IEC 61508-1:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: General requirements.
IEC 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Requirements for electrical/electronic/programmable electronic safety-related systems.
IEC 61508-3:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Software requirements.
IEC 61784-3:2021	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions.
2006/42/EC	Machinery Directive
2014/30/EU	Electromagnetic Compatibility Directive
2014/35/EU	Low Voltage Directive

In addition, terms used in the present document may tangentially be used as they are derived from other standards such as:

Standard	Description
IEC 60034 series	Rotating electrical machines
IEC 61800 series	Adjustable speed electrical power drive systems
IEC 61158 series	Digital data communications for measurement and control – Fieldbus for use in industrial control systems

Finally, the term *zone of operation* may be used in conjunction with the description of specific hazards, and is defined as it is for a *hazard zone* or *danger zone* in the *Machinery Directive* (*2006/42/EC*) and *ISO 12100:2010*.

NOTE: The aforementioned standards may or may not apply to the specific products cited in the present documentation. For more information concerning the individual standards applicable to the products described herein, see the characteristics tables for those product references.

Security Planning

Introduction

This chapter provides general information on security planning.

Security Terminology

The term *Security* can be subdivided into the following aspects:

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 previously listed aspects must be satisfied to consider a situation as helped to be secure.

Example for Confidentiality and Integrity

The device offers different user account roles with different degrees of access. This helps control confidentiality and integrity.

The following table presents examples of confidentiality and integrity controls, based on user account roles:

User account role	Description	Security impact
unauthorized	A user with this account role cannot log into the device.	Device management data remains confidential and retains its integrity.
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

User Interface Terminology

The following terms are found in the user interface and are explained throughout this document:

Aspect	Description
Vulnerability	A flaw or weakness of a system. Vulnerabilities can be unintentional (such as an unintended software problem), or they can be unavoidable (such as a system that offers a login). The union set of all vulnerabilities of a system is called an attack surface.
Threat	An action, event, or circumstance that results in an undesired 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 predicted. By defining these fundamental conditions, a threat model enables the 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 threat/ mitigation criticality, or other, appropriate criteria.
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.

Convenience and Security

Without 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 not secure 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 helps enforce the use of system-generated, long and truly random passwords for login:

- Such a system is considerably inconvenient for the database users.
- The confidentiality of personal data is maintained, because access controls limit exposure to authorized users only.

Neither of these extreme configurations is practical in most deployments.

Security planning therefore requires 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 helped to be reasonably secured because the confidentiality of the personal data is helped to be appropriately protected.

Allowlist Approach

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

An allowlist 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, that is, in a device in its default state. Therefore, plan a policy for the necessary functions.

Qualitative Security Philosophy

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

1. Elevated security consideration:
   - People with experience in security often 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, unmitigated vulnerabilities.
   - In a qualitative way, not using a structured approach at all can be seen as leading to higher security but can sometimes also lead to poorer convenience or usability.
2. Basic security consideration:
   - People mainly concerned with usability and convenience tend to focus on convenience while at the same time tend to overlook the security aspects of a system.
     Convenience considerations aim to minimize user, for example cognitive load. However, reducing this effort can unintentionally introduce new vulnerabilities or amplify existing ones within the system.
   - In a qualitative way, not using a structured approach at all can be seen as leading to good usability but can sometimes also lead to insufficient security.

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

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.

Threat Analysis

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

The threats are modeled and assessed in the following two steps:

1. 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.

2. 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.

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 unsuccessful 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.

Theoretical and Practical Degrees of Security

Consider the following limitations for barriers that provide a high degree of confidentiality:

- 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.

Strategies to Help Improve Security: Confidentiality Example

Regarding the previous example, there are two 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 threat risk/mitigation efficiency combinations need to be combined with other threat risk/mitigation combinations, for defense in depth. The resulting overview is also suitable for picking less critical threat risk/mitigation efficiency combinations as possible targets for hardening.

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 take into account elevated security considerations. 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 impactful).
- 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.

Overview

Introduction

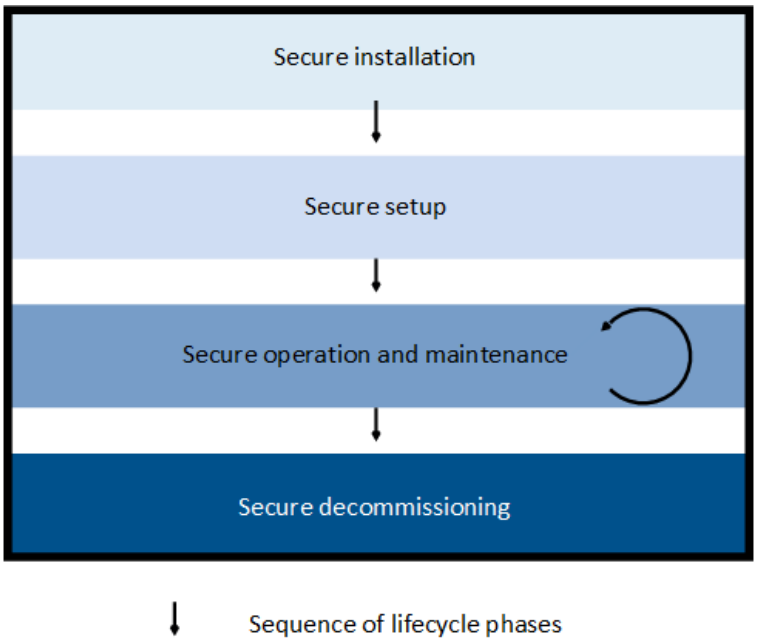
This document contains:

- Specific security considerations and actions to help secure your network device as described in Device Security in the Life Cycle Phases, page 54
- Specific security considerations and actions which enable a secured network device to help support and enhance the security and availability of your network as described in Network Security Support, page 89

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

- Secure installation, see Installation Step Sequence, page 56
- Secure setup, see Security Setup Overview, page 61
- Secure operation, see Operation, page 82
- Secure maintenance, see Maintenance, page 82
- Secure replacement, see Device Hardware Replacement, page 84
- Secure repair, see Device Hardware Repair, page 85
- Secure decommissioning, see Device Decommissioning, page 86

The following figure presents a device life cycle overview:



Device Security Measures

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.

Capability Security Levels

The document uses a markup convention to identify content that meets higher capability security levels. Material that satisfies SL C1 requirements is not labeled in this document. However, content that meets IEC 62443 Capability Security Level 2 or higher is labeled with the tag <SL-C2>.

Required Preparatory Work

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

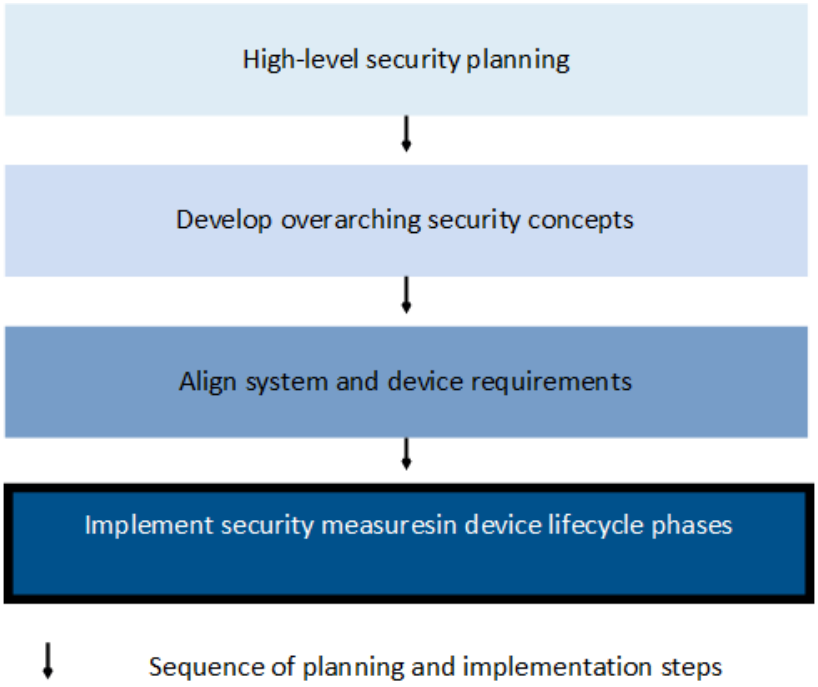
To be effective, these measures need a solid base. Before working through this document, first complete the required high-level security planning steps.

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.

The following figure presents a required preparatory work hierarchy before implementation:



The overarching system security concept may include:

- Hardware-related concepts:
  - Verification of the security seal of a device ([NDR3.13], IEC 62443-4-2 Network Device Requirement)
  - A suitable physical location for the device
  - Possible restrictions to the device's hardware interfaces
  - A decommissioning policy ([CR4.2], IEC 62443-4-2 Component Requirement)
- Setup- (Software-) related concepts ([CR7.6], IEC 62443-4-2 Component Requirement):
  - Concepts for helping secure the device itself:
    - A secure boot policy (<SL-C2>, IEC 62443 Security Capability Level 2)
    - A user account login policy
    - A user account password policy
    - A user account and access role policy
    - A secure management protocol policy ([CR7.7], IEC 62443-4-2 Component Requirement)
    - An SNMPv3 authentication and encryption types policy
    - An SNMPv3 trap password policy
    - A remote logging policy
    - A fallback policy for protocols that offer fallback
  - Concepts for helping secure the network through device functions:
    - 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], IEC 62443-3-3 System Requirement), ([SR7.3 RE1], Requirement Enhancement of IEC 62443-3-3 System Requirement), ([CR7.3], IEC 62443-4-2 Component Requirement)
  - A policy for device hardware replacement and repair ([CR7.4], IEC 62443-4-2 Component Requirement)

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

Software Setup Scenarios and Hardware Scenarios

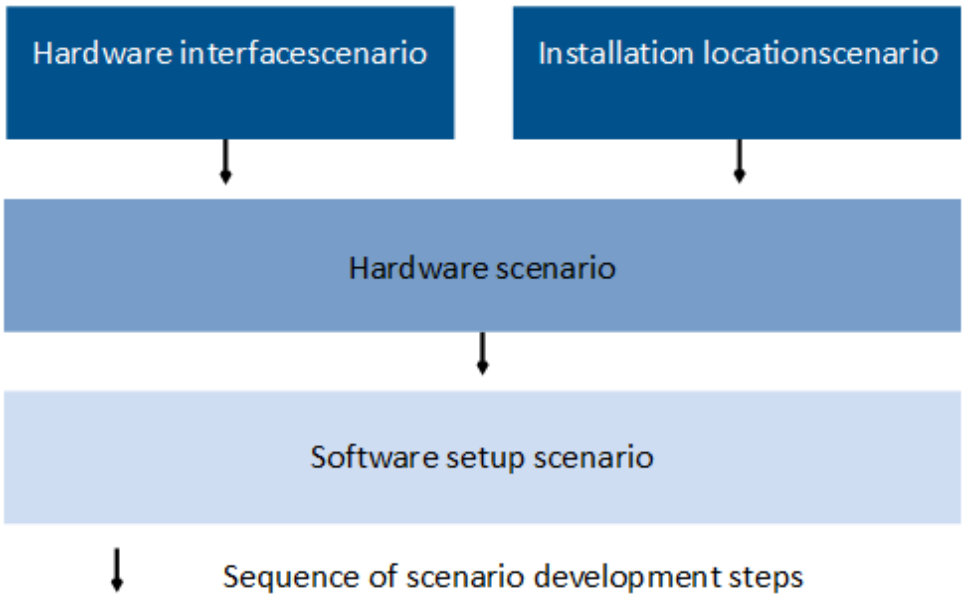
The software setup scenario consists of the required software setup steps. A particular software scenario typically has a specific hardware scenario as its base.

The hardware scenario consists of a secure installation location, and of possible device hardware interface access restrictions.

NOTE:

- A hardware scenario can by itself help mitigate a considerable part of the threats.
- 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.

The following figure presents basic scenario development steps:



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 this user guide:

- 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

It is a good practice to use software tools that support these steps.

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

You can assess the risk for an individual threat by combining exploitability and exploit severity.

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 consider a careful conversion of non-monetary risks (for example, personal injury) to monetary risks. This can be a demanding ethical assessment. There is no technical solution.

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 two-dimensional set of nine possible combinations into a one-dimensional index of five values.

The following table presents the threat risk matrix:

Exploit severity	**Exploitability**		
	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.

The following table presents 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.

The following table presents 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.

Defense in Depth

Introduction

This section introduces the concept of defense in depth that is necessary for planning the mitigation strategies and the complementary concept of hardening.

Purpose

Defense in depth is a 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 two 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.

Defense in Depth vs. Hardening

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

Hardening focuses on reducing the attack surface as broadly as possible by addressing general weaknesses across the system. 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 device functions – for the device security
- Least required device functions – for the network security support

Responsibilities

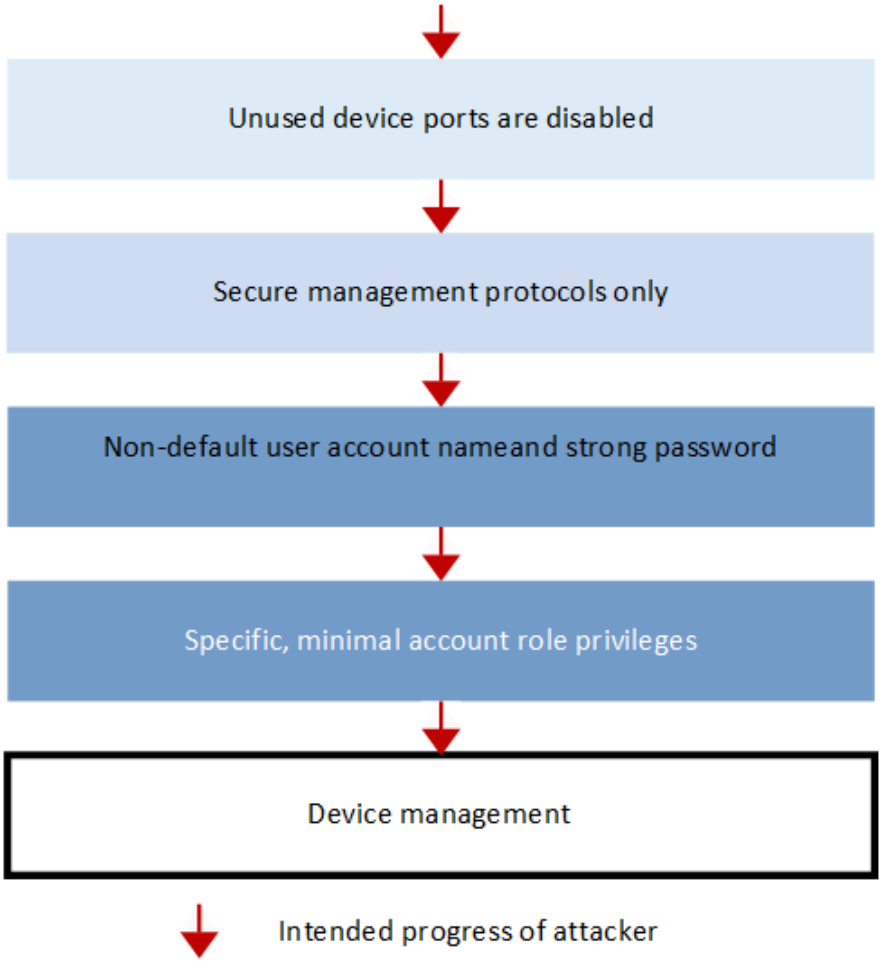
Defense in depth and hardening both require planning, implementation, and maintenance. The system operator is responsible for performing these steps.

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

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.

The following figure presents a 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).

The following table presents examples of the defense in depth barriers:

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.

ID	Barrier	Description
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.

Developing a Mitigation Strategy

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

You can determine the efficiency for an individual mitigation measure by combining effort and effectiveness.

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 two-dimensional set of nine possible combinations into a one-dimensional index of five values.

The following table presents a mitigation efficiency matrix:

Effectiveness	Effort		
	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.

The following table presents 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.

The following table presents examples for mitigation effectiveness:

Mitigation measure	Effectiveness	Remarks
Set the waiting period after a number of successive unsuccessful 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 undefined 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.

Mitigation Efficiency Value and Unit

The efficiency of a concrete, individual mitigation measure can take on a value in the range $0 \leq x \leq 1$. It has no unit, so it can be regarded as a factor.

A very high mitigation efficiency means a value close to 1, and a very low mitigation efficiency means a value close to 0. In theory, a mitigation efficiency of 1 means that the individual mitigation measure completely eliminates the associated risk, and 0 means that the individual mitigation measure has no effect at all.

If the risk reduction factor is defined as (1 - mitigation efficiency), the greater the mitigation effectiveness, the smaller the risk mitigation factor.

Alternatives to Mitigation

From a business-global view, there are alternatives to threat mitigation:

- **Risk acceptance:**
  - If the risk of a threat seems acceptable, a business may choose not to deploy any mitigation measures.
  - An example may be the leaking of unimportant data from a public system. The monetary risk of such a leak may be considered much lower than the monetary effort to help secure the public system. As a consequence, a business may choose to accept the risk.
  - In this document, the acceptance of a risk is implicitly dealt with when considering the residual risk. If the risk of an unmitigated threat is lower than the accepted risk, the threat may be considered as acceptable.
- **Risk avoidance:**
  - If a business process that has a risk associated can be avoided, the risk is also avoided. In terms of technical systems, this translates into not setting up certain network or device functions.
  - An example may be that an internal system with business-critical data is not connected to a public network but the subset of data intended to be publicly accessible is placed on another, dedicated system. The transfer of the publicly accessible data subset is then performed by a system that is only active while the transfer is performed. This avoids the permanent risk of leaking business-critical data from the internal system.
  - In this document, the avoidance of a risk is implicitly dealt with when excluding a device or network function from implementation because the risk cannot reasonably be mitigated.
- **Risk transference:**
  - In broad business terms, a certain business risk can be transferred to a third party.
  - An example can be buying insurance against the risk of fire in a data center. The risk of fire can never be completely ruled out, so it may be reasonably to purchase insurance.
  - Risk transference is outside the scope of this document.

  NOTE: This document focuses on technical mitigation measures, and does not detail the previously listed alternatives to mitigation.

Criticality Assessment and Mitigation Strategies

Mitigation Calculation

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

If two or more mitigation measures to address the same risk are independent of each other (that is, they do not influence each other), the combined risk reduction factor can be calculated by multiplying the individual risk reduction factors. This is the numeric background of the general guidance to combine mitigation measures if required or possible.

NOTE: When you combine two or more mitigation measures to address the same risk, the mitigations may influence each other. That is, the risk reduction factor may be higher or lower than the calculation of the combined mitigation efficiency (1 - mitigation efficiency$_1$) × (1 - mitigation efficiency$_2$) would give. Therefore, when you combine mitigation measures, verify if you have to consider the combined mitigation efficiencies individually.

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 two-dimensional set of 25 possible combinations into a one-dimensional index of 9 values.

The following table presents criticality matrix (threat risk and mitigation efficiency combined):

Mitigation efficiency	**Threat risk**				
	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

Mitigation Strategies

The following table presents criticality and mitigation strategies that are commonly applied. These are provided for illustration and do not represent recommendations.

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

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 Risk Value and Unit, page 24

Security Viewpoints: Binary or Continuous Values

The security of a system under consideration, with respect to a defined threat and defined circumstances (such as 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 such as *improving the security*, this can have two meanings:

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

A phrase such as *help improving the security* often means *lowering the residual risk*.

Cryptographic Key and Password Basics

The setup and operation of a network device typically involves the use of cryptographic keys and passwords.

An example of an asymmetric cryptographic key is:

- SSH server keys

Examples of passwords are:

- User account passwords
- SNMPv3 passwords
- The configuration encryption password
- User passwords for the Integrated Authentication Server (IAS)
- SNMPv3 trap passwords
- Passwords for Email logging
- Passwords for a OPC UA connection

Cryptographic Key Policies

Cryptographic keys are used for two different types of cryptographic algorithms:

- Symmetric cryptographic algorithms
- Asymmetric cryptographic algorithms (also called public key algorithms)

The properties of symmetric and asymmetric algorithms are very different, and therefore, the properties of the respective keys are also different. This is why the policy guidelines for generating the keys apply to different aspects presented in the following table:

Aspect	Symmetric cryptographic keys	Asymmetric cryptographic keys
Key properties	1 key (used for encryption as well as decryption)	2 keys (key pair): • Private key: ◦ Must be kept secret ◦ For decryption or signing • Public key: ◦ Publicly available ◦ For encryption or signature verification
Key content	A large random number; it does not need to be prime.	• Private key: 2 separate large prime numbers • Public key: Product of the private key's prime numbers
Typical key generation	Manually or automated	Automated (compulsory)
Different key policy subjects	Key generation	Key signing
Common key policy subjects	Distribution, and rotation	Distribution, and rotation

For both cryptography types, this document provides general policy guidelines for key distribution and rotation.

For symmetric cryptography keys, this document also provides detailed policy guidelines for key generation (see Password and Cryptographic Key Comparison, page 33).

For asymmetric cryptography, the policy details for key generation and signing are outside the scope of this document.

Password and Cryptographic Key Comparison

From a cryptographic viewpoint, symmetric cryptography keys can be considered a subset (special case) of passwords.

NOTE: For asymmetric cryptography, the comparison between passwords and keys does not apply.

The following table presents comparison between passwords and symmetric cryptographic keys:

Property	Passwords	Symmetric cryptographic keys
Representation	ASCII string (in most cases)	• Hexadecimal • Base64-encoded • ASCII string
Length (representation)	Variable (allowed length range)	• Variable (allowed length range) • Fixed
Length (internal)	• Variable (when stored as value) • Fixed (when stored as hash)	Fixed
Creation	Manually by human users (in most cases)	• Automated, by dedicated software tools or systems • Manually by human users
Strength	Strength depends strongly on the enforced password policy. Without an enforced password policy, strength may be insufficient.	• Automated creation: High strength • Manual creation: Strength depends strongly on the enforced policy. Without a policy, strength may be insufficient.

For both passwords and symmetric cryptographic keys entered manually, their the strength depends strongly on the enforced policy. This is why a planning, setting up and enforcing a policy for manually generated passwords and keys is a good practice. A policy may include the requirement that passwords or keys be generated by a specialized application.

For details on the strength of manually generated passwords, see Password Strength and Policy Guide.

For symmetric cryptographic keys, an automated generation is a good practice. In cases where a key is entered manually, following a policy is also a good practice, see Considerations for Manually Entered Keys, page 109.

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

VLAN Plan

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR5.1]
- IEC 62443-3-3 System Requirement: [SR5.1]

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 undefined 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 to help secure a 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 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 VLAN Plan Considerations Depending on Redundancy Protocols, page 44.

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 document.

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 (MCSESP), and data link redundancy
  - Properties of the USB port
  - 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 such as 802.1X, the MAC authentication bypass, a dedicated authentication policy list, LDAP or RADIUS or TACACS+: These measures require planning for the client in the device and may also require planning for external servers:
  - 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.
  - Plan the TACACS+ server setup.

NOTE: For details on these topics, see Considering the Device Availability Requirements, page 58.

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.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide* for a suitable physical installation location:

- Chapter *Safety Information* for safety and regulatory topics
- Chapter *Technical Data* for the allowed device temperature ranges and climatic conditions
- Chapters *Installation Procedure > Installing the Device onto the DIN Rail > Grounding the Device* and *Installation Procedure > Connecting the Power Supply and the Signal Contact Lines* for the mechanical and electrical device installation.

Planning for Device Availability

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

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

Planning for Software Automatic Update from the External Memory

The device offers to automatically update the device software during system startup. The prerequisites are:

- The external memory function is enabled.
- On the external memory, there is a valid software image in the root directory

Disabling the Software automatic update from the External Memory can be an alternative to disabling the external memory function entirely.

For the setup of the Software automatic update from the External Memory, see Disable the Automatic Device Software Update from an External Memory (EAM), page 67.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings > External Memory* on how to enable/disable the software automatic update.

Planning for SSH Key Automatic Upload from the External Memory

The device offers to automatically upload an SSH key during system startup. The prerequisites are:

- The external memory function is enabled.
- On the external memory, there is a valid SSH key in the root directory

Disabling the SSH key automatic upload from the External Memory can be an alternative to disabling the external memory function entirely.

For the setup of the SSH key automatic upload from the External Memory, see Disable the SSH Key Automatic Upload from the External Memory, page 67.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings* > *External Memory* on how to enable/disable the SSH key automatic upload.

Planning the Configuration Load Priority for the External Memory

The device offers to assign a priority for the loading of a configuration profile from the External Memory.

Setting the Configuration load priority to **disable** for the External Memory can be an alternative to disabling the external memory function entirely.

For the setup of the Configuration load priority for the External Memory, see Disable the Configuration Load Priority for the External Memory, page 68.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings* > *External Memory* on how to set the Configuration load priority for the External Memory.

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.

For details, see Disable Logical Access to the Signal Contact, page 66.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide*:

- Chapter *Safety Information* for safety and regulatory topics
- Chapter *Technical Data* > *General Technical Data* for allowed signal contact operating conditions
- Chapter *Installation Procedure* > *Connecting the Power Supply and the Signal Contact Lines* > *Signal Contact (Optional)* for the electrical signal contact connection.

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.

For details, see Disable Logical Access to the Digital Input, page 66.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide*:

- Chapter *Safety Information* for safety and regulatory topics
- Chapter *Technical Data* > *General Technical Data* for allowed digital input operating conditions
- Chapter *Installation Procedure* > *Connecting the Power Supply and the Signal Contact Lines* for the electrical digital input connection

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.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide*, chapter *Ethernet Ports* > *Port LEDs* for the device and port LEDs.

Planning How to Verify the Security Seal

The actions described in this chapter conform to the following standards:

- IEC 62443 Security Capability Level 2: <SL-C2>
- IEC 62443-4-2 Network Device Requirement: [NDR2.13], [NDR3.11], [NDR3.13]

Plan on how the security seal on a new device shall be verified as described in Security Seal, page 106.

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, such as covering or obstructing a slot or a port, according to your requirements:

- Restrict physical access to the USB port.
- Restrict physical access to network ports or SFP 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 *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide*, chapters *General Presentation* > *Physical Description* and *Management Interfaces* for the hardware interfaces.

Planning a Secure Boot Policy

The actions described in this chapter conform to the following standards:

- IEC 62443 Security Capability Level 2: <SL-C2>

- IEC 62443-4-2 Network Device Requirement: [NDR3.12]
- Requirement Enhancement of IEC 62443-4-2 Network Device Requirement: [NDR3.10 RE1], [NDR3.14 RE1]

The device offers booting only from trustworthy, that is, cryptographically signed software images that have not been tampered with.

NOTE: The secure boot mode is required for a device setup compliant with SL-C2.

The default configuration sets the secure boot mode to disabled. When the secure boot mode is disabled, the Security Status function in the web-based interface notifies the user.

After the first successful boot from a proper, signed software image, you have the option to enable the secure boot mode. This initial boot process may have been taken place during manufacturing, or it may take place on the customer premises during a device software update.

Before you enable the secure boot mode:

- Verify if the device is trustworthy, that it has not been tampered with.

  For details on this verification, see Security Seal, page 106 and the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide*.
- Verify that you use only secure boot-enabled software images in the future. You do not need to downgrade to a non-secure boot-enabled software image.

  NOTE: Once you enable secure boot mode, you cannot disable it again. The device subsequently boots only from secure boot-enabled software images. Consequently the device refuses booting from any other software images, including images of older device software releases even if these are perfectly intact and trustworthy but do not support secure boot.

Upload of Unsigned Device Software

When the secure boot mode is off, the device offers the possibility to upload an unsigned software image into the device. The default setting Allow upload of unsigned device software is enabled.

NOTE: If you activate the secure boot mode, the device only accepts signed software images. The device no longer offers the possibility to upload an unsigned software image.

Planning a Dedicated User Account Login Policy

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR1.11], [CR2.5], [CR3.8]
- IEC 62443-3-3 System Requirement: [SR3.8]
- Requirement Enhancement of IEC 62443-3-3 System Requirement: [SR3.8 RE1], [SR3.8 RE2], [SR3.8 RE3]

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

The login policy consists of:

- Login attempts:

  The maximum number of unsuccessful user login attempts in a row until the device locks the respective user account
- Minimum password length:

  The minimum password length that the device helps enforce when changing a password or specifying a new password
- Login attempts period:

  The waiting time before the device automatically 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 Graphic User Interface (GUI) using HTTPS or HTTP

NOTE:

- For quantitative information on how to help ensure a secure login policy, see Attack Rate Mitigation.
- For quantitative information on how to provide for hard-to-break passwords, see 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. Choose a value that fits your requirements.
- Minimum password length:
  - For security reasons, plan a value as high as reasonable.
  - Consider the type of password 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.
  - Choose a minimum password length that fits your requirements.
  - For quantitative information on how to help ensure hard-to-break passwords, see 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. Choose a value that fits your requirements.

  NOTE: Access to the CLI using the serial port is exempt from the login policy. Users accessing the CLI through the serial port 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.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Device Security* > *User Management* for the device login functions.

Planning a Dedicated User Account Password Policy

The actions described in this chapter conform to the following standard: [CR1.7].

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

For detailed information on how to help ensure hard-to-break passwords, see Password Strength and Policy Guide.

Consider the type of password to use as described in Quantitative Password Strength:

- High-complexity passwords have the following properties (see High-Complexity Passwords):
  - No part of the password can be found in a dictionary
  - Contains ≥1 lowercase letters, ≥1 uppercase letters, ≥1 digits, and ≥1 special characters

- Low-complexity passwords have the following properties (see 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 letters, 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 letters
- The minimum number of lowercase letters
- The minimum number of digits
- The minimum number of special characters

NOTE: The minimum password length belongs to the user account login policy as described in Planning a Dedicated User Account Login Policy, page 39.

To help secure your system, develop an overarching user account password policy. When you do, consider the following aspects to deter attackers:

- It is a good practice to use account names that are non-standard, and are non-descriptive to unauthorized entities.
- It is a good practice to use different user account names on different devices.
- It is a good practice to use different passwords on different devices, including for user accounts with the same name.
- It is a good practice to use different SNMPv3 passwords on different devices.

For the user credentials in the delivery state, see Set Up a Dedicated User Account Login Policy, page 72.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Device Security* > *User Management* for the device password policy functions.

Planning a Dedicated User Account Name and Access Role Policy for Device Management

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR1.3] [CR1.4] [CR1.5]
- Requirement Enhancement of IEC 62443-4-2 Component Requirement: [CR1.1 RE1], [CR2.1 RE1], [CR2.1 RE2]
- IEC 62443-3-3 System Requirement: [SR2.1]
- Requirement Enhancement of IEC 62443-3-3 System Requirement: [SR2.1 RE1] [SR2.1 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.

The following table presents user account roles and privileges:

User account role	Privileges
unauthorized	None: The device refuses login.
guest	The device permits reading of device management data, except the audit trail. The device refuses any write access to data.
auditor	The device permits reading of device management data, including the audit trail. The device permits writing the audit trail to a log file, but refuses any other write access.
operator	The device permits reading and writing of device management data. The device refuses write access to security-relevant settings and the audit trail.
administrator	The device permits reading and writing of device management data, including security-relevant settings. This device also permits the reading of the audit trail.

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

User-name	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:

- Create user accounts with:
  - Dedicated names (<SL-C2>)
  - Chosen access roles that offer only the least required privileges
  - The password policy verification 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 (<SL-C2>).

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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Device Security > User Management* for the device user account name and access role functions.

Planning Configuration Encryption and the Associated Password

Plan a configuration encryption policy:

- Plan whether 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 verified against the user account password policy.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings* > *Load/Save* for the configuration encryption and the associated password.

Planning Session Timeouts (<SL-C2>)

Plan finite session timeouts for:

- The Graphic User Interface using HTTPS or HTTP
- The Command Line Interface through the serial port, SSH, or Telnet

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*:

- Chapter *Device Security* > *Management Access* > *Web* for the Graphic User Interface timeout function
- Chapter *Device Security* > *Management Access* > *CLI* for the SSH and serial port timeout function

Planning a Dedicated Logging Policy

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR2.8], [CR2.9], [CR2.10], [CR2.12], [CR3.9], [CR6.1], [CR6.2]
- IEC 62443-3-3 System Requirement: [SR2.8], [SR2.11], [SR2.12], [SR6.1]
- Requirement Enhancement of IEC 62443-3-3 System Requirement: [SR2.8 RE1], [SR2.11 RE1], [SR2.12 RE1]

Set up the device logging settings:

- Synchronize the device system clock to a trusted source (<SL-C2>, [CR2.11 RE1]).
- 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 as described in Logging Server Considerations (<SL-C2>), page 48.

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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Diagnostics* > *Syslog* for the device function.

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, such as 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. You may also elect to enable only the receive function. The delivery state for LLDP is globally disabled.

For details, see Set Up the LLDP Parameters (<SL-C2>), page 103.

VLAN Plan Considerations Depending on Redundancy Protocols

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR5.1]
- IEC 62443-3-3 System Requirement: [SR5.1]

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, page 34 that takes this particularity into account may require the use of VLAN IDs ≥2 for payload traffic and device management.

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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*:

- Chapter *Switching* > *HIPER Ring* for the HIPER Ring function
- Chapter *Switching* > *Ring/Network Coupling* for the Ring/Network Coupling function

Advanced Authentication Measures (<SL-C2>)

If you intend to use advanced user authentication measures such as 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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*:

- Chapter *Network Security* > *802.1X* for the 802.1X function
- Chapter *Device Security* > *Authentication List* for the dedicated authentication policy list

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Controlling the Data Traffic* > *MAC Authentication Bypass* for the MAC authentication bypass function.

Impact of Network Aspects on System Planning

External Server Considerations

The actions described in this chapter conform to the following standards:

- IEC 62443 Security Capability Level 2: <SL-C2>
- IEC 62443-4-2 Component Requirement: [CR1.9]

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, such as assigning a VLAN ID to a user.
- Syslog servers offer log entry redundancy and virtually unlimited storage capacity.

For some protocols, such as system message logging (Syslog), you can use the remote server in the normal state of operation, and have a fallback 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 fallback operation for a certain protocol, verify if the protocol offers this possibility, and if it is appropriate for your situation. Then develop an overarching policy for the fallback.

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.

NOTE: These keys typically are asymmetric cryptography keys.
As such, these keys need a specific key policy.
This policy is different than the policy for keys for symmetric cryptography that is discussed in other locations of this document.

Asymmetric key 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 as described in Certificate and Revocation Management for Authentication, Logging and Email Servers (<SL-C2>), page 49.

Server Key Rotation

Server key rotation on a regular basis limits the amount of data encrypted or signed by a specific key. This key can be:

- For asymmetric cryptography (used for example by TLS): The private key of a specific key pair
- For symmetric cryptography (used for example by encrypted SNMPv3 traps): The key that both communications partners share

Given that the 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 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 can be used only for a limited period and is typically 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 two or more keys per server whose validity periods are adjacent or overlap.

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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*:

- 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

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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Advanced* > *DNS* > *DNS Client* for the device DNS client function.

Network Time Synchronization Considerations (<SL-C2>)

The actions described in this chapter conform to the following standard: [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.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*:

- Chapter *Time* > *SNTP* for the device SNTP client and server functions
- Chapter *Time* > *PTP* for the device PTP functions

Authentication Server Considerations (<SL-C2>)

This action conforms to the following standards:

- IEC 62443 Security Capability Level 2: <SL-C2>
- IEC 62443-4-2 Component Requirement: [CR1.9]

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.
- Plan the external TACACS+ 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 offers obfuscated 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 developing an overarching remote authentication policy and using only encrypted LDAP or obfuscated RADIUS.

NOTE: Encrypted LDAP can be considered preferable over obfuscated RADIUS or TACACS+ because encrypted LDAP employs newer and more sophisticated concepts for both establishing trust towards its authentication server and the encryption of the communication.
RADIUS and TACACS+ use obfuscated communication which offers weaker security than encrypted LDAP.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*:

- Chapter *Device Security* > *Authentication List* 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

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Access to the Device* > *TACACS+* for the device TACACS+ client function

Logging Server Considerations (<SL-C2>)

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR2.8], [CR2.9], [CR2.10], [CR2.12], [CR3.9], [CR6.1], [CR6.2]
- IEC 62443-3-3 System Requirement: [SR2.8], [SR2.11], [SR2.12], [SR6.1]
- Requirement Enhancement of IEC 62443-3-3 System Requirement: [SR2.8 RE1], [SR2.11 RE1], [SR2.12 RE1]

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.

This action conforms also to <SL-C2> and [CR1.9].

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 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.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*:

- Chapter *Diagnostics* > *Syslog* for the device Syslog function
- Chapter *Diagnostics* > *Audit Trail* for the device Audit trail

Email Logging Server Considerations

The actions described in this chapter conform to the following standards:

- IEC 62443 Security Capability Level 2: <SL-C2>
- IEC 62443-4-2 Component Requirement: [CR1.9]

If you intend to use Email servers 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. 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.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Diagnostics* > *Email Notification* for the device Email function.

Certificate and Revocation Management for Authentication, Logging and Email Servers (<SL-C2>)

The actions described in this chapter conform to the following standards:

- IEC 62443 Security Capability Level 2: <SL-C2>
- IEC 62443-4-2 Component Requirement: [CR1.9]

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:

- For authentication servers, as described in Authentication Server Considerations (<SL-C2>), page 47
- For logging servers, as described in Logging Server Considerations (<SL-C2>), page 48
- For Email logging servers, as described in Email Logging Server Considerations (<SL-C2>), page 49

NOTE: For software update and configuration servers, trust is managed by another concept, SSH Defined Host key fingerprints as described in Software Update and Configuration Server Considerations (<SL-C2>), page 45.

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 is typically replaced by another certificate shortly before the validity period of the present 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 as described in Server Key Rotation, page 46.

A certificate rotation scheme may include:

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

Device-Related Policies

Develop a Backup Policy for Device-Related Data

The actions described in this chapter conform to the following standards:

- IEC 62443-3-3 System Requirement: [SR7.3]
- Requirement Enhancement of IEC 62443-3-3 System Requirement: [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:

- Creating a backup copy of the device configuration profiles (<SL-C2>, [SR7.3] [SR7.3 RE1] [CR7.3] [CR7.3 RE1]).
- 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 a version control tool to track the device configuration history.

Develop a Policy for Replacing the Device Hardware

The actions described in this chapter conform to the following standards:

- IEC 62443 Security Capability Level 2: <SL-C2>
- IEC 62443-4-2 Component Requirement: [CR7.4], [CR1.9]
- IEC 62443-4-2 Network Device Requirement: [NDR2.13], [NDR3.11]

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
- How the security seal of the new device shall be verified ([NDR3.13]), see Security Seal, page 106
- 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 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

Develop a Policy for Device Hardware Repair

The actions described in this chapter conform to the following standards:

- IEC 62443 Security Capability Level 2: <SL-C2>
- IEC 62443-4-2 Component Requirement: [CR1.9]

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 present HTTPS certificate
- The present SSH host key or host key pair
- The present 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 (has a different base MAC address)
  - If you agree to receive a device of another, superior type or generation (has a different base MAC address and possibly also other properties)
- For the security seal on the device (Security Seal, page 106), specify:
  - How you verify the security seal's condition before sending the device to the manufacturer
  - How you verify the security seal's condition after receiving the device back from the manufacturer

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 indicated in the following list 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 present HTTPS certificate in the device and creates a new, self-signed HTTPS certificate
  - Deletes the present 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 as described in 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 as described in Security Seal, page 106.
- Physically destroy the device, including the flash memory chips. This destroys the data and secrets listed in the previous list item as described in Reset to the Delivery State.
- If required, physically destroy the external memory.

NOTE:

- The reset to the delivery state leaves the audit trail intact.
- The reset to the delivery state leaves the secure boot setting intact (<SL-C2>)
- 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

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.

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 as described in Planning a Dedicated User Account Name and Access Role Policy for Device Management, page 41.
- 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 verification 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 (<SL-C2>, [CR1.9])
- The extent of active measures that determine the device security status, such as:
  - Verifying the security status variable of the device
  - Verifying 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

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.

Device Security in the Life Cycle Phases

Develop the Device Configuration

Based on your documented overarching policies, plan (develop) the configuration for each considered device. If you follow an allowlist approach, include the necessary function policy from your allowlist 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 two ring ports and one 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 two 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 determined which device types you are using, 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.
  - Determine which concrete device type and variant 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.

Software vs. Hardware Measures (Logical vs. Physical)

This 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.

Security-Related vs. General Device Functions

The software setup measures 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 Security Setup Overview, page 61.

- Security-related device functions that help secure your system and improve its availability:

  The setup of these functions is described in Network Security Support, page 89.
- General device functions: The setup of the general device functions is outside the scope of this document. If you follow an allowlist approach, include the necessary function policy from your allowlist policy. The necessary function policy may stipulate which general device functions need to be disabled although they are not directly security-related.

  For details on general device functions, refer to:
  - *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*
  - *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*
  - *Modicon MCSESM, MCSESP Series Managed Switch Command Line Interface User Guide*
  - *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide* (for hardware-related setup steps)

Prerequisites for Installation and Setup

Before completing this section, first complete the system planning steps, including:

- Planning a suitable physical location for the device as described in Choosing a Secure Installation Location, page 57
- Planning restrictions to the device hardware interfaces as described in Planning Restrictions to the Device Hardware Interfaces, page 38
- If you follow an allowlist approach, develop a necessary function policy from your allowlist 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 as described in Planning a Dedicated User Account Login Policy, page 39
- Developing a dedicated user account **password** policy as described in Planning a Dedicated User Account Password Policy, page 40
- Developing a dedicated user account and access role policy for device management as described in Planning a Dedicated User Account Name and Access Role Policy for Device Management, page 41
  - Developing a dedicated policy for SNMPv3 authentication and encryption types, and for the related passwords
- Planning configuration encryption (<SL-C2>) as described in Planning Configuration Encryption and the Associated Password, page 43
- Planning session timeouts (<SL-C2>) as described in Planning Session Timeouts (<SL-C2>), page 43
- Developing a dedicated logging policy, possibly including remote logging as described in Planning a Dedicated Logging Policy, page 43
- Developing a policy for the servers that hold device software updates and configuration files (<SL-C2>) as described in Software Update and Configuration Server Considerations (<SL-C2>), page 45
- Planning a dedicated LLDP policy (<SL-C2>) as described in Planning a Dedicated LLDP Policy (<SL-C2>), page 44

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

- Network time synchronization considerations (<SL-C2>)

- Certificate and revocation management for authentication, logging and Email servers (<SL-C2>, [CR1.9])
- 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

Possible Further Prerequisites

Your network may require further system planning steps, including:

- Traffic segregation on Layer 2 by a VLAN plan
- Use of a network management system such as ConneXium Network Manager (optional)

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

Installation Step Sequence

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

- Choose a secure installation location as described in Choosing a Secure Installation Location, page 57
- Perform the initial software update as described in Software Update, page 59
- Perform the initial security setup as described in Security Setup Overview, page 61
- If required, modify the hardware interfaces for security as described in Possible Restrictions to the Device Hardware Interfaces, page 80
- Perform the initial device installation as described in Device Installation, page 80
- Operation measures as described in Operation, page 82
- Maintenance measures as described in Maintenance, page 82
- Decommissioning measures as described in Device Decommissioning, page 86

NOTE: Depending on your requirements, perform the steps in a different sequence.

Reasons for the 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 defined host fingerprints, prepared device configuration files and device labels, may be more conveniently available in an office location.
- Time-consuming steps such as 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 such as 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.

Preparation for Installation

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

- Verify the security seal of the device as described in Security Seal, page 106.
- Verify the available device software release on the Schneider Electric product pages on the Internet at .
- Determine which device software release to run on your devices.
- Download the respective software files.
- If you need 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, such as the server administrator.
- If desired, prepare the individual device configuration files based on the respective planned device configuration. If you need to enable the configuration encryption, see Options to Enable Configuration Encryption, page 65.
- Prepare the device labels.

  NOTE: To help keep your system secure, use the latest available release of the device software.

  If you need to load the device configuration or update the device software over a network, verify that you are using a secure transfer protocol, such as HTTPS, SFTP or SCP. Use FTP or TFTP only when the server and transfer network are verified as trusted through your network access controls, or when the files being transferred carry a valid cryptographic signature.

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

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*:

- Chapter *Updating the Switch Software* for details on how to:
  - Determine the running software release
  - Determine the stored software release
  - Load a previous software version, if required
  - Verify a newer available software release
  - Update the device software
- Chapter *Assistance in the Protection from Unauthorized Access > Making SSH Hosts Defined by the Device* for details on how to set up the defined hosts public key fingerprints.

Choosing a Secure Installation Location

Before completing this section, first plan a secure installation location as described in Planning a Secure Installation Location, page 36.

Select an installation location that provides suitable ambient conditions and restricts physical access to the device or its hardware interfaces.

Verify 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 as described in Restrict Physical (Visual) Access to the Device LEDs and Port LEDs.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide* for a suitable physical installation location:

- Chapter *Safety Information* for safety and regulatory topics
- Chapter *Technical Data* for the allowed device temperature ranges and climatic conditions
- Chapters *Installation Procedure > Installing the Device onto the DIN Rail > Grounding the Device* and *Installation Procedure > Connecting the Power Supply and the Signal Contact Lines* for the mechanical and electrical device installation.

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.

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

- Consider the power supply requirements as described in Considering the Power Supply Redundancy Requirements, page 58 ([SR7.5]).
- Consider the power budget requirements as described in Considering the Power Budget Requirements, page 58.
- Consider the data link redundancy requirements as described in Considering the Data Link Redundancy Requirements, page 59.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide*, chapters *Technical Data > General Technical Data* for the power requirements of the device.

Considering the Power Supply Redundancy Requirements

The actions described in this chapter conform to the following standard: [SR7.5].

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

- The device is powered by two 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 two separate mains cables.
- The mains cables to the redundant power supplies run along different paths as far as possible.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide*, chapters *Safety Information* and *General Presentation* for the power supply redundancy aspects of the device.

Considering the Power Budget Requirements

Verify that the power requirements are fulfilled as required:

- One single power supply can deliver power for every connected device.
  - Also consider the worst-case power requirements of the inserted SFPs.
- One single power supply can also deliver the worst-case set-up PoE or PoE+ power (MCSESP).

  NOTE: The condition **one single power supply** takes the possible inoperable state of one power supply in a dual power supply configuration into account.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide*, chapters *Technical Data* > *General Technical Data* for the power requirements of the device.

Considering the Data Link Redundancy Requirements

Verify 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.

Software Update

The actions described in this chapter conform to the following standards:

- IEC 62443 Security Capability Level 2: <SL-C2>
- IEC 62443-4-2 Component Requirement: [CR4.3]
- IEC 62443-4-2 Network Device Requirement: [NDR3.10], [NDR3.12], [NDR3.14]
- Requirement Enhancement of IEC 62443-4-2 Network Device Requirement: [NDR3.10 RE1], [NDR3.14 RE1]

The following description applies to:

- The initial software update for a device in its default state
- A software update as part of operation or maintenance

Verify if an updated release of the device software is available. You find information and software downloads on the Schneider Electric product pages on the Internet at . Then determine which software release to run on your device ([NDR3.10 RE1] <SL-C2>).

Initial Access to the Device Management

To update the software on the device, you need management access to the device.

A device in its default state must first be assigned an IP address. Schneider Electric Viewer can be used to assign this IP address to the device. After the IP address is assigned, Schneider Electric Viewer allows you to open the Graphic User Interface or the Command Line Interface of the device.

Initial Password Considerations

In the delivery state, the device has the following user account preconfigured (user credentials for the administrator account in the delivery state):

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

At the first login with the delivery state password, you are required to change the password ([CR1.10]). Use a dedicated password according to your password policy as described in Planning a Dedicated User Account Password Policy, page 40.

Software Update Server Considerations

If you need to update the device software over a network, verify that you are using a secure transfer protocol, such as HTTPS, SFTP or SCP. Use the unencrypted protocols FTP or TFTP only when the server and transfer network are verified as trusted through your network access controls, or when the files being transferred carry a valid cryptographic signature.

If you need to perform the initial software update for a device in its default state and you have the new software image on an SFTP or SCP server, first set up the SSH defined host fingerprints on the device as described in Set Up the SSH Defined Hosts Fingerprints on the Device, page 71. Use the fingerprint of the software update server. This enables the device to determine whether the software update server it contacts is trustworthy or not.

NOTE: Verify that the server fingerprints are from a trustworthy source, such as the server administrator.

Secure Boot Considerations

Before a possible device software update, determine if you need to apply your secure boot policy, if you have one:

- Verify if the present software and its settings belong to one of the following categories:
  - The image has not been cryptographically signed. Such a software image does not offer the secure boot setting.
  - The image has been cryptographically signed but the secure boot mode is disabled.
- Verify if the new software is cryptographically signed.

If **both** of the previous statements are true, apply your secure boot policy as described in Planning a Secure Boot Policy (<SL-C2>), page 38.

NOTE: If you do not have a secure boot policy, to help you determine whether to enable secure boot on that specific device or not, see Planning Configuration Encryption and the Associated Password, page 43
The secure boot mode is required for a device setup compliant with SL-C2.

If you determine 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 determine 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 as described in Develop a Backup Policy for Device-Related Data, page 50.

- Update the device software.
- Reboot the device for the new software to take effect.

Best Practices

To help keep your system secure, consider verifying 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 such as new functions, including new device functions that can assist in securing your network.

Detailed Documentation

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*:

- Chapter *Managing Configuration Profiles* for the device configuration profiles
- Chapter *Updating the Switch Software* for details on how to:
  - Determine the running software release
  - Determine the stored software release
  - Load a previous software version, if required
  - Verify a newer available software release
  - Update the device software
- Chapter *Assistance in the Protection from Unauthorized Access* > *Making SSH Hosts Defined by the Device* for details on how to set up the defined hosts public key fingerprints.

Security Setup Overview

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR7.1], [CR7.6]
- IEC 62443-4-2 Network Device Requirement: [NDR3.2], [NDR3.10], [NDR3.14]

The following descriptions apply to:

- The initial device security setup for a device in its default state
- Changes in the device security setup as part of operation or maintenance

To update the software on the device, you need management access to the device, which requires at least a preliminary IP address setup. Use Schneider Electric Viewer to assign an IP address to the device.

After the IP address is assigned, Schneider Electric Viewer offers you to open the device management ([CR7.1 RE1]). For the software update, see Software Update, page 59.

The Security Status function in the device GUI can help you gain a first overview of the device security status ([CR3.3]). The Security Status function monitors security configuration settings that are considered basic. Depending on your requirements, additional security setup steps may be required including the cases when the Security Status function reports **ok**.

Refer to:

- The *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Diagnostics* > *Status Configuration* > *Security Status* for the Security Status function

- The *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Assistance in the protection from unauthorized access* for a basic device security setup

You can find more details for the security setup further on in 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.
At the first login with the delivery state password, the device asks you to change the password ([CR1.10]). Use a dedicated password according to your password policy as described in Planning a Dedicated User Account Password Policy, page 40.

NOTE:

- If you need to perform the initial security setup for a device in its default state over a network, verify that you are using a secure transfer protocol, such as HTTPS, SFTP or SCP. Use the unencrypted protocols FTP or TFTP only when the server and transfer network are verified as trusted through your network access controls, or when the files being transferred carry a valid cryptographic signature.
- If you need to perform the initial security setup for a device in its default state and you have the configuration profile on an SFTP or SCP server, first set up the SSH defined host fingerprints on the device as described in Set up the SSH Defined Hosts Fingerprints on the Device, page 71. Use the fingerprint of the configuration profile server. This enables the device to determine whether the configuration profile server it contacts is trustworthy or not.
- Verify that the fingerprints are from a trustworthy source, such as 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) and *restrict physical access* means disabling a feature or an interface by a physical measure (a hardware modification). See Possible Restrictions to the Device Hardware Interfaces, page 80.

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 an allowlist 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 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 Ethernet Switch Configurator access.
- Enable the secure boot mode (<SL-C2>).
- 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 to the signal contact.
- Disable logical access to the digital input.
- Set up Power over Ethernet (MCSESP).

- Disable the automatic device software update from an external memory (EAM).
- Disable the SSH key automatic upload from the External Memory.
- Disable the Configuration load priority for the External Memory.
- Disable copying a software file into the device that lacks a valid cryptographic signature.
- Disable writing an unencrypted configuration profile to an external memory (EAM) (<SL-C2>).
- Disable loading an unencrypted configuration profile from an external memory (EAM) (<SL-C2>).
- Disable unencrypted 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.
- Set up the SSH Defined Hosts fingerprints on 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 port
- Disable access to the CLI service shell.

You can also choose to set up the following advanced user authentication measures as required, see Set Up Advanced User Authentication (<SL-C2>), page 78:

- Use 802.1X for user authentication.
- Use a dedicated authentication policy list.
- Use MAC authentication bypass for device authentication.
- Set up the following remote authentication protocol clients as needed, instead of or in addition to the local Integrated Authentication Server (IAS):
  - LDAP
  - RADIUS
  - TACACS+

When the device configuration is complete:

- Create a backup of the configuration according to your backup policy for device-related data.
- If required, include other device-related data such as 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 document 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 Defined Hosts entry on the clients.

Assign IP Address Parameters to the Device Management

At the first login with the delivery state password, you are required to change the password. Use a dedicated password according to your password policy as described in Planning a Dedicated User Account Password Policy, page 40.

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 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 when the server and transfer network are verified as trusted through your network access controls.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Specifying the IP Parameters* on how to specify an IP address for the device management.

Disable Ethernet Switch Configurator Access

The actions described in this chapter conform to the following standard: [CR4.3].

The delivery state of Ethernet Switch Configurator is enabled.

Set the Ethernet Switch Configurator protocol to **Off** after its initial use. This helps reduce the attack surface of the device.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Specifying the IP Parameters* > *Specifying the IP Parameters Using Ethernet Switch Configurator* on how to:

- Specify the IP address parameters for the device management
- Disable Ethernet Switch Configurator

Enable the Secure Boot Mode <SL-C2>

The actions described in this chapter conform to the following standards:

- IEC 62443 Security Capability Level 2: <SL-C2>
- IEC 62443-4-2 Network Device Requirement: [NDR3.12]
- Requirement Enhancement of IEC 62443-4-2 Network Device Requirement: [NDR3.10 RE1] [NDR3.14 RE1]

The setting Secure Boot enabled disables the booting from an unsigned software image. This helps secure the device against rogue device software without a valid cryptographic signature.

If you have a secure boot policy, apply your secure boot policy as described in Planning a Secure Boot Policy (<SL-C2>), page 38 for enabling the secure boot mode on that specific device.

If you do not have a secure boot policy, to help you determine, see Planning a Secure Boot Policy (<SL-C2>), page 38.

NOTE: The secure boot mode is required for a device setup compliant with SL-C2.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings* > *Software* > *Software Update* on how to enable the secure boot mode.

Enable Configuration Encryption (<SL-C2>)

Enable the configuration encryption and set the associated password according to your configuration encryption policy as described in Planning Configuration Encryption and the Associated Password, page 43.

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.
- The configuration encryption password is a symmetric cryptography key, so if you have already planned a policy for symmetric cryptography keys described in Cryptographic Key and Password Basics, page 32, apply it to this key.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, 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.

Set Up a VLAN Dedicated to Device Management Access

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR5.1]
- IEC 62443-3-3 System Requirement: [SR5.1]
- IEC 62443-4-2 Network Device Requirement: [NDR1.13]

Before completing this section, first plan the general and security-related device setup as described in VLAN Plan Considerations Depending on Redundancy Protocols, page 44.

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

Set up a VLAN dedicated exclusively to device management access. This helps reduce the attack surface of the device. It may also help improve the reachability of the device management when there is heavy general network traffic.

NOTE: If you use the HIPER Ring or Ring/Network Coupling redundancy protocol, assign a VLAN ID of 2 or higher for device management access. If you do not use either of these protocols, assign any available VLAN ID.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings* > *Global* > *Management Interface* on how to specify a VLAN for device management access.

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 Signal Contact Considerations, page 81.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Diagnostics* > *Status configuration* > *Signal Contact* for the signal contact.

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 Digital Input Considerations, page 81

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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings* > *Port* for disabling ports.

Set Up Power Over Ethernet (MCSESP)

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 does not help 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 the exact maximum power consumption of a PD is defined, you can additionally set the power limit for the given port to this defined 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 defined power consumption of the PD, this may help in powering more PDs simultaneously in certain cases.
- If the power consumption requirements of a PD are defined 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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings* > *Power over Ethernet (MCSESP)* for setting up Power over Ethernet.

Disable the Automatic Device Software Update from an External Memory (EAM)

The device offers to automatically update the device software during system startup. The prerequisites are:

- The external memory function is enabled.
- On the external memory is a valid software image that is referred to in the file startup.txt.

Disable the automatic device software update from an external memory. This helps secure the device against a rogue device software image on an external memory being 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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings* > *External Memory* on how to disable the automatic software update from the external memory.

Disable the SSH Key Automatic Upload from the External Memory

The device offers to automatically upload an SSH key during system startup. The prerequisites are:

- The external memory function is enabled.
- On the external memory is a valid SSH key that is referred to in the file startup.txt.

Disabling the SSH key automatic upload from the external memory can be an alternative to disabling the external memory function entirely.

Disable the SSH key auto upload from an external memory. This helps secure the device against a rogue SSH key on an external memory being copied to the device and take effect after a reboot.

In the delivery state setting, the SSH key auto upload from an external memory is enabled.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings* > *External Memory* on how to enable/disable the SSH key auto upload.

Disable the Configuration Load Priority for the External Memory

The device offers to assign a priority for the loading of a configuration profile from the external memory:

- **disable**

  The device loads the configuration profile only from the internal non-volatile memory (**NVM**).

- **first**

  The device loads the configuration profile from the external memory first.

  When the device does not find a configuration profile in the external memory, it loads the configuration profile from the internal non-volatile memory (**NVM**).

In the delivery state setting, the Configuration load priority for the external memory is **first**.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings* > *External Memory* on how to set the Configuration load priority for the external memory.

Disable Copying a Software File Into the Device That Lacks a Valid Cryptographic Signature

The actions described in this chapter conform to the following standards:

- IEC 62443 Security Capability Level 2: <SL-C2>
- IEC 62443-4-2 Network Device Requirement: [NDR3.2], [NDR3.12]
- Requirement Enhancement of IEC 62443-4-2 Network Device Requirement: [NDR3.10 RE1], [NDR3.14 RE1]

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 device 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 allows the upload of a software file into the device that lacks a valid cryptographic signature.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings* > *Software* > *Software Update* > *Allow upload of unsigned device software* on how to allow the upload of unsigned device software.

Disable Writing an Unencrypted Configuration Profile to an External Memory (EAM) (<SL-C2>)

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 as described in Enable Configuration Encryption (<SL-C2>), page 65.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings* > *Load/Save* > *Configuration Encryption* on how to disable writing an unencrypted configuration profile to an external memory.

Disable Loading an Unencrypted Configuration Profile from an External Memory (EAM) <SL-C2>

The actions described in this chapter conform to the following standard: [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 as described in Enable Configuration Encryption (<SL-C2>), page 65.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings* > *Load/Save* > *Configuration Encryption* on how to disable loading an unencrypted configuration profile from an external memory.

Disable Unencrypted Management Protocols

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR4.3]
- IEC 62443-4-2 Network Device Requirement: [NDR1.13]

Disable unencrypted management protocols:

- Disable SNMPv1/v2 (delivery state: disabled).
- Disable Telnet (delivery state: disabled).
- Disable HTTP (delivery state: enabled – redirects to HTTPS).

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Assistance in the Protection from Unauthorized Access* for disabling unencrypted management protocols.

Set Up Management IP Access Restrictions

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR3.1,] [CR7.7], [CR4.3]
- IEC 62443-4-2 Network Device Requirement: [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:

Protocol	Minimum required 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

NOTE: HTTP (delivery state enabled) may be useful for the initial setup of the device. However, it is not secure 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.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Assistance in the Protection from Unauthorized Access > Restricting Access to Device Management* for setting up IP access restrictions.

Set Up a Dedicated HTTPS Certificate for the Device

The actions described in this chapter conform to the following standards:

- IEC 62443 Security Capability Level 2: <SL-C2>
- IEC 62443-4-2 Component Requirement: [CR1.8], [CR1.9], [CR4.1], [CR4.3]
- IEC 62443-3-3 System Requirement: [SR3.1], [SR4.1]
- Requirement Enhancement of IEC 62443-3-3 System Requirement: [SR4.1 RE1]

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 resolve the *Trust On First Use* issue 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 *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Setting Up the Configuration Environment > HTTPS Certificate* for an example of setting up your own HTTPS certificate.

Set Up a Dedicated SSH HostKey for the Device

The actions described in this chapter conform to the following standards:

- IEC 62443 Security Capability Level 2: <SL-C2>
- IEC 62443-4-2 Component Requirement: [CR4.1], [CR4.3]
- IEC 62443-3-3 System Requirement: [SR3.1], [SR4.1]
- Requirement Enhancement of IEC 62443-3-3 System Requirement: [SR4.1 RE1]

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 resolve the *Trust On First Use* issue 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 key generation and signing tools on the Internet, for example, by searching for the keywords *SSH key generation tool*.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *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.

Set Up the SSH Defined Hosts Fingerprints on the Device

If you need to load the device configuration or update the device software from an SFTP or SCP server, set up the SSH defined 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 determine whether the SFTP or SCP server it contacts is trustworthy or not.

NOTE: Verify that the fingerprints are from a trustworthy source, such as the server administrator.
If you need to load the device configuration or update the device software over a network, verify that you are using a secure transfer protocol, such as HTTPS, SFTP or SCP. Use FTP or TFTP only when the server and transfer network are verified as trusted through your network access controls, or when the configuration files are encrypted.

NOTE: For authentication, logging, and Email logging servers, trust is managed by another concept, TLS certificates and revocations lists as described in Certificate and Revocation Management for Authentication, Logging and Email Servers <SL-C2>, page 49.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Assistance in the Protection from Unauthorized Access > Making SSH Hosts Defined by the Device* for details on how to set up the defined hosts' public key fingerprints.

Set Up a Dedicated User Account Login Policy

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR1.11], [CR2.5], [CR3.8]
- IEC 62443-3-3 System Requirement: [SR3.8]
- Requirement Enhancement of IEC 62443-3-3 System Requirement: [SR3.8 RE1], [SR3.8 RE2], [SR3.8 RE3]

Before completing this section, first plan a dedicated user account login policy as described in Planning a Dedicated User Account Login Policy, page 39.
For quantitative information on how to help ensure a secure login policy, see Attack Rate Mitigation. For quantitative information on how to help ensure hard-to-break passwords, see 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 Graphic User Interface (GUI) using HTTPS or HTTP

Apply your planned user account login policy. This helps ensure that the device locks out a user after the specified maximum number of unsuccessful login attempts in a row, requires a password with minimum length, and helps enforce the specified waiting period after an unsuccessful login attempt.

Set up a dedicated user account login policy as required:

- Login attempts:
  - Specify the maximum number of unsuccessful login attempts 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 automatically unlocks a locked user account (delivery state: 0 – no waiting time).

NOTE: Access to the CLI using the serial port is exempt from the login policy. Users accessing the CLI through the serial port 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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Device Security > User Management* for the device login functions.

Set Up a Dedicated User Account Password Policy

The actions described in this chapter conform to the following standard: [CR1.7].

Before completing this section, first plan a dedicated user account password policy as described in Planning a Dedicated User Account Password Policy, page 40.
For quantitative information on how to help ensure hard-to-break passwords, see Password Strength and Policy Guide.

Set up a dedicated user account password policy as required:

- Minimum required number of uppercase letters (delivery state: **1**)
- Minimum required number of lowercase letters (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 as described in Set Up a Dedicated User Account Login Policy, page 72.
  The enforcement of the password policy belongs to the account names and access roles for device management as described in Set Up Dedicated User Account Names and Access Roles for Device Management (<SL-C2>), page 73.

In the delivery state, the device has the following user account preconfigured (user credentials for the administrator account in the delivery state):

User-name	Password	User account role	Privileges
admin	**private** (May have been changed at first login.)	**administrator**	The device permits the reading and writing of device management data, including security-relevant settings. The device 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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Device Security > User Management* for the device password policy functions.

Set Up Dedicated User Account Names and Access Roles for Device Management <SL-C2>

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR1.3], [CR1.4], [CR1.5]
- Requirement Enhancement of IEC 62443-4-2 Component Requirement: [CR1.1 RE1], [CR2.1 RE1], [CR2.1 RE2]
- IEC 62443-3-3 System Requirement: [SR2.1]
- Requirement Enhancement of IEC 62443-3-3 System Requirement: [SR2.1 RE1] [SR2.1 RE2]

Before completing this section, first plan a dedicated user account name and access role policy as described in Planning a Dedicated User Account Name and Access Role Policy for Device Management, page 41, and plan a dedicated policy for SNMPv3 authentication and encryption types, and for the related SNMPv3 passwords.

The SNMPv3 passwords are symmetric cryptography keys, so if you have already planned a policy for symmetric cryptography keys described in Cryptographic Key and Password Basics, page 32, apply it to these keys.

In the delivery state, the device has the following user account preconfigured (user credentials for the administrator account in the delivery state):

User-name	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: SNMPv3 passwords are symmetric cryptography keys, so if you have already planned a policy for symmetric cryptography keys described in Cryptographic Key and Password Basics, page 32, apply it to these keys.

Set up dedicated user accounts as required:

- Create user accounts. For each new user account, perform the following steps (<SL-C2>):
  - Create a user account with a dedicated name.

    Note that user account names are case-sensitive.
  - Assign the new user account a strong password.

    Avoid standard passwords such as *private* or *public*, including for accounts with non-descriptive names.
  - Assign the new user account an access role that offers only the least required privileges.
  - Enforce the password policy verification for the new user account (in the delivery state, the password policy verification is not enforced).
  - Save the settings temporarily to allow the device to verify the password of the new account against the enforced password policy.
- 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.
- Help secure existing user accounts:
  - To help enforce the password policy, verify the existing user accounts (in the delivery state, the password policy verification is not enforced).
  - Set up the SNMPv3 settings as previously described for a new user account.
  - If you enforce the password policy subsequently for an existing user account, re-enter the password and save the changed settings temporarily to allow the device to verify the password against the policy.
  - If you change user account data for the presently logged-in user, the device notifies you that you will be logged out.

    To avoid this, consider changing user account data only for user accounts other than the presently logged-in one.

    This may need an additional user account with administrator privileges.

- Remove user accounts that have standard names (<SL-C2>):
  - 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.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Device Security* > *User Management* for the device user account name and access role functions.

Specify Finite Session Timeouts (<SL-C2>)

The actions described in this chapter conform to the following standard: [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:

- Graphic User Interface using HTTPS or HTTP (delivery state: 160 minimum)
- For the Command Line Interface through the serial port, SSH, or Telnet (delivery state: 160 minimum)

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*:

- Chapter *Device Security* > *Management Access* > *Web* for the Graphic User Interface timeout function
- Chapter *Device Security* > *Management Access* > *Command Line Interface* for the SSH and serial port timeout function

Set Up Time Synchronization for the Device Clock (<SL-C2>)

The actions described in this chapter conform to the following standard: [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 as described in Network Time Synchronization Considerations (<SL-C2>), page 47.

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.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*:

- Chapter *Time* > *SNTP* for the device SNTP client and server functions
- Chapter *Time* > *PTP* for the device PTP functions

Set Up Certificates and Possible Revocation Lists for Authentication, Logging and Email Servers

The actions described in this chapter conform to the following standards:

- IEC 62443 Security Capability Level 2: <SL-C2>
- IEC 62443-4-2 Component Requirement: [CR1.9]

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

- Authentication servers
- Logging servers
- Email logging servers

This enables the device to determine 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 Defined Host key fingerprints as described in Software Update and Configuration Server Considerations (<SL-C2>), page 45.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*:

- Chapter *Device Security* > *LDAP* > *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.

Set Up Logging

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR1.2], [CR1.8], [CR2.8], [CR2.9], [CR2.10], [CR2.11], [CR2.12], [CR3.1], [CR3.9], [CR6.1], [CR6.2]
- IEC 62443-3-3 System Requirement: [SR2.8], [SR2.11], [SR2.12], [SR6.1]
- Requirement Enhancement of IEC 62443-3-3 System Requirement: [SR2.8 RE1], [SR2.11 RE1], [SR2.12 RE1]

Set up logging:

- Consider setting up the device to synchronize its system clock to a trusted source (<SL-C2>, [CR2.11 RE1]).
- Set up the minimum severity level to be logged.

  The setting depends on your functional and security requirements.
- Set up logging destinations:
  - The required settings depend on your 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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*:

- 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

Disable SNMPv1/v2 Write Access

The actions described in this chapter conform to the following standard: [CR6.2].

NOTE: If you cannot or do not need 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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Device Security* > *Server* > *SNMP* > *Configuration*.

Disable SNMPv1 Traps

The actions described in this chapter conform to the following standard: [CR6.2].

The device can send SNMPv1 traps. SNMPv1 traps are unencrypted. From a security perspective, this may be considered not secure.

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

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Diagnostics* > *Status Configuration* > *Alarms (Traps)* for the device SNMPv1 trap send function.

Enable SNMPv3 Traps

The actions described in this chapter conform to the following standard: [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).

NOTE: The SNMPv3 trap passwords are symmetric cryptography keys, so if you have already planned a policy for symmetric cryptography keys as described in Cryptographic Key and Password Basics, page 32, apply it to these keys.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Diagnostics* > *Status Configuration* > *Alarms (Traps)* for the device SNMPv3 trap send function.

Set Up Dedicated Login Banners

The actions described in this chapter conform to the following standard: [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.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*:

- 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

Set Up the DNS Client Functions

Set up the device DNS client using one of the following options:

- 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, you can disable it to help reduce the attack surface. Using only the local, static, hostname table for the DNS client can be considered more secure than using an external DNS server.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Advanced* > *DNS* for the device DNS functions.

Advanced: Disable Access to the CLI Service Shell

You can disable access to the CLI service shell (delivery state: enabled). However, disabling the CLI service shell is permanent. To re-enable the CLI service shell, you have to send the device to the manufacturer.

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

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, 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.

Set Up Advanced User Authentication (<SL-C2>)

The actions described in this chapter conform to the following standard: [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 the following remote authentication protocol clients as needed, instead of or in addition to the local Integrated Authentication Server (IAS):
  - LDAP, preferably using encrypted communication
  - RADIUS (offers obfuscated communication)
  - TACACS+ (offers obfuscated communication)

  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.
  - The RADIUS client in the device exclusively offers obfuscated communication which is considered weaker than encrypted LDAP.
  - The TACACS+ client in the device exclusively offers obfuscated communication which is considered weaker than encrypted LDAP.

  NOTE: If you use authentication servers, this requires setup and maintenance of these external servers. The system operator is responsible to plan and implement these steps.

Refer to:

- *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*:
  - 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
  - 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
- *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*:
  - Chapter *Controlling the Data Traffic* > *MAC Authentication Bypass* on how to set up the MAC authentication bypass
  - Chapter *Access to the Switch* > *TACACS+* on how to set up the TACACS+ client in the device

Create a Backup of the Device-Related Data

The actions described in this chapter conform to the following standards:

- IEC 62443-3-3 System Requirement: [SR7.3]
- Requirement Enhancement of IEC 62443-3-3 System Requirement: [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.

- Consider creating a backup copy of the device configuration profile (<SL-C2>, [SR7.3], [SR7.3 RE1], [CR7.3], [CR7.3 RE1]).
- 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 Defined Hosts entry on the clients.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings* > *Load/Save* on how to save the device configuration.

Possible Restrictions to the Device Hardware Interfaces

Before completing this section, first plan possible restrictions to the device's hardware interfaces as described in Planning Restrictions to the Device Hardware Interfaces, page 38.

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.

⚠⚠DANGER

ELECTRIC SHOCK

Do not open or attempt to service the device.

Failure to follow these instructions will 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) and *disable logical access* means disabling a feature by a logical measure (a software setup). Refer to Security Setup Overview, page 61.

The following descriptions apply to possible hardware modifications in the following cases:

- For a device in its default state before installation
- After initial installation
- As part of operation or maintenance

Perform the following modification steps to restrict access to the device hardware interfaces, such as covering or obstructing a slot or a port, as required. Restrict physical access:

- To the USB port
- To network ports or SFP slots
- To the signal contact
- To the digital input
- Restrict physical (visual) access to the device LEDs and port LEDs.

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

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide* for a suitable physical installation location:

- Chapter *Safety Information* for safety and regulatory topics
- Chapter *Technical Data* for the allowed device temperature ranges and climatic conditions
- Chapters *Installation Procedure* > *Installing the Device onto the DIN Rail* and *Installation Procedure* > *Connecting the Power Supply and the Signal Contact Lines* for the mechanical and electrical device installation

Verifying the Security Seal

The actions described in this chapter conform to the following standard: [NDR3.13].

On the new device, verify the security seal as described in Security Seal, page 106.

Data Connections

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

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide*:

- Chapter *Installation Procedure* > *Installing an SFP Transceiver (Optional)* for the SFP slots
- Chapter *Ethernet Ports* for the network ports
- Chapter *Installation Procedure* > *Preparing the Device for Operation* > *Connecting Data Cables* for details on how to make data connections.

Signal Contact Considerations

If you use the signal contact, consider the following aspects:

- **To help protect the device**, connect the signal contact only to a circuit that meets the electrical and safety 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.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide* for the signal contact:

- Chapter *Technical Data* > *General Technical Data* for the allowed signal contact operating conditions
- Chapter *Installation Procedure* > *Connecting the Power Supply and the Signal Contact Lines* for the electrical signal contact connection

Digital Input Considerations

If you use the digital input, consider the following aspects:

- **To help protect the device**, connect the digital input only to a circuit that meets the electrical, and safety requirements of the device.

- **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.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide* for the digital input:

- Chapter *Technical Data* > *General Technical Data* for the allowed digital input operating conditions
- Chapter *Installation Procedure* > *Connecting the Power Supply and the Signal Contact Lines* for the electrical digital input connection

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 helps reduce the required security steps during the operation phase to the considerations already described in this document, the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide*, *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, and *Modicon MCSESM, MCSESP Series Managed Switch Command Line Interface User Guide*.

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

- Environmental conditions as described in Device Installation, page 80
- Device availability requirements as described in Considering the Device Availability Requirements, page 58
- Data connections as described in Data Connections, page 81

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 as described in Operation and Maintenance Policy, page 53.

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 as described in Operation and Maintenance Policy, page 53.

Verify the Security Seal (Regularly or Triggered by an Event)

The actions described in this chapter conform to the following standard: [NDR3.11].

On the device, verify the security seal as described in Security Seal, page 106.

Software Update

The actions described in this chapter conform to the following standard: [NDR3.10].

If required, perform a device software update.

For the security aspects of the software update, see Software Update, page 59.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Updating the Switch Software* for details on how to:

- Determine the running software release
- Determine the stored software release
- Load a previous software version, if required
- Verify a newer available software release
- Update the device software

Hardware Changes

⚠⚠DANGER

ELECTRIC SHOCK

Do not open or attempt to service the device.

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

Typical application cases include:

- Connecting or removing an external device on an Ethernet port
- Inserting or removing an SFP
- Connecting or removing a power supply
- Connecting or removing a PoE-/PoE+-powered device (PD) on a port (MCSESP)

  NOTE:

  - Depending on your system availability requirements, provide a redundant data upstream connection.
  - Consider the worst-case power requirements of the inserted SFPs.
  - Connecting an additional power supply to a device with an existing power supply forms a redundant power supply that helps the device availability ([SR7.5]). Consider the worst-case device power budget for every power supply, in case one of the redundant power supplies becomes inoperable ([SR7.5]).
  - 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:

- *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide*:
  - Chapter *Ethernet Ports* for the network ports and SFP slots
  - Chapter *Installation Procedure* > *Preparing the Device for Operation* > *Connecting Data Cables* on details how to make data connections
  - Chapter *Installation Procedure* > *Installing an SFP Transceiver* for installing an SFP
  - Chapter *Disassembly* > *Removing an SFP Transceiver* for removing an SFP

- *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Configuring the Ports* > *Enabling/Disabling the Port* for enabling or disabling a port
- *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings* > *Power over Ethernet (MCSESP)* for setting up PoE/PoE+

Device Hardware Replacement

⚠⚠DANGER

ELECTRIC SHOCK

Do not open or attempt to service the device.

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

The actions described in this chapter conform to the following standard: [CR7.4].

Perform the following steps:

- According to your backup policy as described in Develop a Backup Policy for Device-Related Data, page 50
- According to your hardware replacement policy as described in Develop a Policy for Replacing the Device Hardware, page 50

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.
- On the new device, verify the security seal as described in Security Seal, page 106 ([NDR3.11]).
- On the new device, perform an initial software update as described in Software Update, page 59.
- 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 as described in Security Setup Overview, page 61.
  - If you have enabled configuration encryption as described in Options to Enable Configuration Encryption, page 65.
- On the new device, restrict the hardware interfaces if required as described in Possible Restrictions to the Device Hardware Interfaces, page 80.
- Install and connect the new device in its environment.
- For the former device:
  - If you need the device repaired, follow your hardware repair policy described in Device Hardware Repair, page 85.
  - If you need to decommission the device, follow your hardware decommissioning policy described in Device Decommissioning, page 86.

Refer to:

- *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings* > *Load/Save* on:
  - How to save the former device's configuration
  - How to load the configuration into the new device

- *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Loading Software Updates* for the new device on how to:
  - Determine the running software release
  - Determine the stored software release
  - Load a previous software version, if required
  - Verify a newer available software release
  - Update the device software
- *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide*:
  - Chapter *Disassembly > Removing the Device* for mechanically removing the former device from its environment
  - Chapters *Installation Procedure > Installing the Device onto the DIN Rail* and *Installation Procedure > Connecting the Power Supply and the Signal Contact Lines* for the mechanical and electrical installation of the new device.

Device Hardware Repair

⚠⚠DANGER

ELECTRIC SHOCK

Do not open or attempt to service the device.

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

Should your device need repair, follow your device hardware repair policy as described in Develop a Policy for Device Hardware Repair, page 51.

Consider the following steps:

- Keep a backup copy of the device configuration as described in Create a Backup of the Device-Related Data, page 79.
  - 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 as described in Deletion of Confidential Data and Secrets, page 86.
- Record the condition of the security seal on the device as described in Security Seal, page 106.
- Send the device to the manufacturer for repair.

- When the device is back from repair:
  - Verify 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).
  - Verify the security seal of the repaired device as described in Security Seal, page 106. 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 as described in Options to Enable Configuration Encryption, page 65.
  - 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 *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide*:

- Chapter *Disassembly* > *Removing the Device* for mechanically removing the device from its environment
- Chapters *Installation Procedure* > *Installing the Device onto the DIN Rail* and *Installation Procedure* > *Connecting the Power Supply and the Signal Contact Lines* for the mechanical and electrical installation of the repaired device.

Device Decommissioning

When decommissioning a device, follow your device hardware decommissioning policy described in Develop a Policy for Device Hardware Decommissioning, page 51.

⚠⚠DANGER

ELECTRIC SHOCK

Do not open or attempt to service the device.

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

NOTE: If you have high security requirements, consider physical destruction of the device and the external memory (EAM) as described in Secure Physical Destruction of the Device and its Accessories, page 87. Secure physical destruction addresses the possible reading-out of memory blocks from the flash memory and makes deletion and wiping unnecessary as described in Deletion of Confidential Data and Secrets, page 86.
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.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide*, chapter *Disassembly* > *Removing the Device* for mechanically removing the device from its environment.

Deletion of Confidential Data and Secrets

Resetting the device to the delivery state performs normal file deletion operations on the device, and on the external memory (EAM), 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.

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.
  - If an external memory is connected, then the device also deletes the configuration profiles saved in the external memory.
  - Resets the boot parameters.
  - Deletes the present HTTPS certificate in the device and creates a new, self-signed HTTPS certificate.
  - Deletes the present SSH host key pair in the device and creates a new, self-signed SSH host key pair.
  - If the external memory (EAM) 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 *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Managing Configuration Profiles > Resetting the Device to the Default Setting* on how to reset the device to the delivery state.

Helping Secure Physical Destruction of the Device and its Accessories

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

- Destroy the security seal on the device as described in Security Seal, page 106.
- 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 (EAM). This addresses:
  - The configuration profiles on the external memory
  - The software files on the external memory
  - Any other files on the external memory

Helping Secure Removal of Device-Related Data from the Administration Environment

The actions described in this chapter conform to the following standards:

- IEC 62443 Security Capability Level 2: <SL-C2>
- IEC 62443-4-2 Component Requirement: [CR1.9]

To help secure the 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

Helping Secure Disposal of the Device Hardware

To help secure the disposal of the device hardware, follow your disposal policy.

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

Network Security Support

This 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.

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

Prerequisites for Setting Up Network Security

Only secured device can help improve the security and availability of your network. Before completing this section, first complete the required steps to secure the device itself as described in Device Security in the Life Cycle Phases, page 54.

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 as described in Compiling a Threat Profile, page 24:
  - Develop a network threat model.
  - Collect the perceivable threats to the network.
  - Assess the network threat risks.
- Develop a general network defense strategy as described in Defense in Depth vs. Hardening, page 26.
- Develop a general network mitigation strategy as described in Developing a Mitigation Strategy, page 28:
  - Collect the perceivable network mitigations.
  - Assess the network mitigation efficiency.
- Develop an individual mitigation strategy as described in Criticality Assessment and Mitigation Strategies, page 30:
  - Assess the criticality of the individual network threat/mitigation combinations.
  - Develop a mitigation strategy based on the individual criticality values.

Deploying Defense in Depth for Your Network

Defense in depth creates several barriers that a potential attacker must overcome sequentially. Before completing this section, first set up a dedicated plan for defending your network in depth Defense in Depth, page 26.

From a system view, there are two 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 Security Setup Overview, page 61.

- The network-related way:

  The network-related way deploys specific device functions as measures to help secure the network. These measures are described in chapters that follows.

Network-related mitigation measures are described in Measures to Help Secure the Network, page 90.

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

Harden Your Network

Network-related mitigation measures are described in Measures to Help Secure the Network, page 90.

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

Measures to Help Secure the Network

The following 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 such as HiVRRP, VRRP, OSPF or RIP are outside the scope of this document.

Restrict Logical Access to Your Network

Set Up VLANs for Traffic Segregation

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR5.1]
- IEC 62443-3-3 System Requirement: [SR5.1]

The essential prerequisite for setting up VLANs on the device is that you have created a VLAN plan for your network as described in VLAN Plan, page 34.

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, use only VLAN IDs ≥2 for payload traffic and device management as described in VLAN Plan Considerations Depending on Redundancy Protocols, page 44.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Switching* > *VLAN* on how to set up VLANs for traffic segregation.

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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*:

- 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.

Set Up the Port Security

The actions described in this chapter conform to the following standard: [NDR1.13].

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 allowlist, the device can take a configurable action, such as sending an SNMP trap to the network management station or disabling the port.

Port Security can also operate on IPv4 source addresses. In this mode, the network device translates the allowed IPv4 source addresses into the associated MAC source addresses during the setup of Port Security.

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 undefined network nodes. However, if the Port security function is configured to automatically disable a given port when the function detects undesired frames, this can lead to a Denial of Service (DoS) situation. An attacker may send deliberately crafted frames to cause a DoS.
Configure the Port Security function according to your specific needs.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Network Security* > *Port Security* on how to set up Port Security.

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 serves as 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 automatically disable a given port when the function detects a rogue node, this can lead to a Denial of Service (DoS) situation. An attacker may send deliberately crafted frames to cause a DoS.
- Configure the DHCP Snooping function according to your specific needs.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Network Security* > *DHCP Snooping* on how to set up DHCP Snooping.

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 described in Set Up DHCP Snooping, page 92 for determining trusted source IDs, VLANs, and ports for defined 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 described in Set Up the Port Security, page 92 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 automatically disable a given port when the respective function is triggered, this can lead to a Denial of Service (DoS) situation. An attacker may send deliberately crafted frames to cause a DoS.
Configure the IP Source Guard function according to your specific needs.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Network Security* > *IP Source Guard* on how to set up IP Source Guard.

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 divert, snoop or manipulate legitimate traffic. However, if the Dynamic ARP Inspection function is configured to automatically disable a given port when the function is triggered, this can lead to a Denial of Service (DoS) situation. An attacker may send deliberately crafted frames to cause a DoS.
- Configure the Dynamic ARP Inspection function according to your specific needs.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Network Security* > *Dynamic ARP Inspection* on how to set up Dynamic ARP Inspection.

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.

- 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:

- *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Controlling the Data Traffic* > *MAC Authentication Bypass* on how to set up the MAC authentication bypass
- The *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Network Security* > *802.1X* > *802.1X Global* > *MAC Authentication Bypass Format Options* on the MAC authentication bypass format.

Help Secure the Network Protocols Used

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 set up 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.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*:

- 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.

Helping Secure the Redundancy Protocols Used

Helping secure the redundancy protocols used can also help enhance and maintain the availability of your network.

Set Up RSTP Guards and Helper Protocols

The actions described in this chapter conform to the following standard: [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 divert, snoop or manipulate legitimate traffic. However, if a function is configured to automatically disable a given port when the respective function is triggered, this can lead to a Denial of Service (DoS) situation. An attacker may send deliberately crafted frames to cause a DoS.

Configure the RSTP guards and helper protocols according to your specific needs.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*:

- 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.

Set Up the Media Redundancy Protocol (MRP) Parameters.

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR3.1], [CR5.1]
- IEC 62443-3-3 System Requirement: [SR5.1]

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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Switching* > *L2 Redundancy* > *MRP* for instructions on how to set up MRP.

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 *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Redundancy* > *Media Redundancy Protocol (MRP)* > *MRP over LAG* on how to set up MRP over LAG.

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 *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Redundancy* > *Sub Ring with LAG* on how to set up Sub Ring with LAG.

Set Up the HIPER Ring Parameters

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR3.1], [CR5.1]
- IEC 62443-3-3 System Requirement: [SR5.1]

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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Switching* > *L2 Redundancy* > *HIPER Ring* on the device HIPER Ring function.

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 *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Redundancy* > *HIPER Ring Client* > *HIPER Ring over LAG* on how to set up HIPER Ring over LAG.

Set Up the Redundant Coupling Protocol Parameters

The actions described in this chapter conform to the following standard: [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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Switching* > *L2 Redundancy* > *Redundant Coupling Protocol* on the device Redundant Coupling Protocol.

Set Up Ring/Network Coupling Parameters

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR3.1], [CR5.1]
- IEC 62443-3-3 System Requirement: [SR5.1]

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 *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Switching* > *L2 Redundancy* > *Ring/Network Coupling* on the device Ring/Network Coupling function.

Set Up the Attack Protection Support Functions

Set Up the Denial of Service (DoS) Parameters

The actions described in this chapter conform to the following standard: [CR7.2].

Consider setting up DoS filters.

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

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Network Security* > *DoS* > *DoS Global* on the device DoS filter functions.

Set Up the Rate Limiter

The actions described in this chapter conform to the following standard: [CR7.2].

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

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

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Switching* > *Rate Limiter* on the device Rate Limiter functions.

Set Up the Management MAC Address Conflict Detection

The actions described in this chapter conform to the following standard: [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 sends a trap.

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

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Basic Settings* > *Network* > *Global* > *Management Interface* on the device's Management MAC address conflict detection function.

Set Up Access Control Lists (ACLs)

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR7.2]
- IEC 62443-4-2 Network Device Requirement: [NDR1.13], [NDR5.2], [NDR5.3]
- Requirement Enhancement of IEC 62443-4-2 Network Device Requirement: [NDR5.2 RE1]

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

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Network Security* > *ACL* for the device ACL function.

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 (such as 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 **deny** rule as the final 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 1,000.

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, two or more ACLs can be active simultaneously.
- Each assignment has a priority.
- If there are two 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 directly affect data packet forwarding, plan them carefully, and tested thoroughly, before deployment. 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.

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 unneeded 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 also restrictive, you can modify the ACLs (for example, add new **permit** rules) or their assignments appropriately.

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

Plan your ACLs by considering the following:

- 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 two 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 each ACL to reflect its purpose, 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.

    This rule is general and has no exceptions. If exceptions are required, deal with them in the next planning step, Refine the ACL by planning exceptions.
  - 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 a **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 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

Set up your ACLs by considering the following:

- 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

Test your ACLs by considering the following:

- 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: Unexpected, undesired packets may include packets targeted at the device-under-test 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 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

Administer your ACLs by considering the following:

- 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

Set Up the Network Time Synchronization Parameters (<SL-C2>)

The actions described in this chapter conform to the following standard: [CR2.11 RE1].

Before completing this section, first complete the required steps to help secure the device itself as described in Set Up Time Synchronization for the Device Clock (<SL-C2>), page 75.

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.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*:

- Chapter *Time* > *SNTP* for the device SNTP client and server functions
- Chapter *Time* > *PTP* for the device PTP functions

Set Up the Logging Parameters

The actions described in this chapter conform to the following standards:

- IEC 62443-4-2 Component Requirement: [CR1.2], [CR1.8], [CR2.11], [CR3.1]

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

- Your device logging policy
- 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>).
- Secure logging also relies on the synchronization of the device system clock to a trustworthy source as described in Set Up Time Synchronization for the Device Clock (<SL-C2>), page 75 ([CR2.11 RE1]).
- 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.

Refer to the *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Diagnostics* > *Syslog* for the device Syslog function.

Audit Trail (Created by Persistent Logging)

The actions described in this chapter conform to the following standard: [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.

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 previous 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. You can enable only the receive function.

Setting up LLDP on the device may require that other network devices have their own LLDP function appropriately enabled.

Refer to:

- *Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide*, chapter *Diagnostics > LLDP > LLDP Configuration* for the device LLDP function
- *Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide*, chapter *Operation Diagnosis > Topology Discovery* for an explanation of LLDP use cases

Security Seal

Overview

This chapter describes 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.

The actions described in this chapter conform to the following standards:

- IEC 62443 Security Capability Level 2: <SL-C2>
- IEC 62443-4-2 Network Device Requirement: [NDR3.11]

The devices are equipped with mechanical components that have the function of a security seal. The type and location of the security seal depends on the device hardware family.

The purpose of the security seal is:

- To either thwart attempts to manipulate the internal hardware of the device
- Or to uncover manipulations through visible traces

A security seal can be of the following type:

- Glued front label as described in Glued Front Label, page 106
- Potted device as described in Potted Device, page 107

Glued Front Label

Security properties:

- The front label is glued to the front panel and 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 label has cutaways, cuts, scratches, wrinkles or folds, especially in the corners where the screws are located.

Verification procedures:

- New device:
  - Verify that the front label is new and has no exposed screws, cutaways, cuts, scratches, wrinkles, or folds, especially in the corners where the screws are located.
- Device before sending it to the manufacturer for repair or replacement:
  - Verify and record the condition of the front label.

    The front label shall have no exposed screws, and no cutaways, cuts, scratches, wrinkles, or folds, especially in the corners where the screws are located.

- Repaired device back from manufacturer:
  - If the device and the front label are both the same:

    Verify the condition of the front panel against the recorded condition. The front label shall be approximately in the same condition as before.

    The front label shall have no exposed screws, and no cutaways, cuts, scratches, wrinkles, or folds, especially in the corners where the screws are located.
  - If the device is the same but the front label is new:

    The front label is new and shall have no exposed screws, and no cutaways, cuts, scratches, wrinkles, or folds, especially in the corners where the screws are located.
  - If the device has been replaced (same device type):

    Verify that the front label is new and has no exposed screws, and no cutaways, cuts, scratches, wrinkles, or folds, especially in the corners where the screws are located.
  - If the device has been replaced (other device type):

    Verify according to the new device type's security seal.

Mechanical decommissioning procedure:

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

Potted Device

Security properties:

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

Tampering evidence:

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

Verify procedures:

- New device:
  - Verify the condition of the casting compound, the connectors, and the LEDs.

    These components shall show no signs of mechanical processing.
- Device before sending it to the manufacturer for repair or replacement:
  - Verify 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:

    Verify 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):

    Verify 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):

    Verify according to the new device type’s security seal.

Mechanical decommissioning procedure:

- Deform the connectors and LEDs with a heavy tool, for example, with a hammer.

Considerations for Manually Entered Keys

Symmetric cryptography keys can be considered as special cases of high-complexity passwords. Therefore, several principles that apply to passwords also apply to symmetric cryptographic keys.

NOTE: This chapter addresses only keys for symmetric cryptography. A key is typically considered a symmetric key if the same value is used for both encryption and decryption.

For asymmetric cryptography, the comparison of keys to passwords does not apply. A key usually is for asymmetric cryptography when the key is part of a key pair (public and private key).

If you need to enter keys for symmetric cryptography manually, consider the following:

- Include as much entropy (randomness) in the key string as possible. A key with a higher entropy is stronger because it is harder to guess through a brute-force attack.
- If possible, use a software tool to generate a random key value of the required length and in the required format (for example, hexadecimal- or Base64-encoded).
- If you have to enter a key value manually, avoid including character sequences that repeat, increase or decrease. This reduces the key strength.

  If possible, set up and follow (help enforce) a policy for manually generated keys.

For key-strength guidance, see Residual Weaknesses of User-Generated Keys, page 112.

Quantitative Key Strength

The strength of a key can be quantified as the number of possible keys for a given key entry scheme. The key entry scheme depends on the key entry policy.

Depending on the actual policy:

- The scheme can be derived from the policy with basic security or elevated security considerations as described in Key Entry as ASCII String, page 109.
- The policy strictly specifies a scheme as described in Key Entry as Hexadecimal String, page 111.

Key Entry as ASCII String

An example key policy for the entry of a 128-bit key requires an ASCII string of variable length with at least 12 characters, including at least 2 uppercase letters, 2 digits, and 2 special characters.

This is a considerably stronger policy than the password policy in the chapter about high-complexity passwords as described in Example: Password Strength with Basic Security Considerations. The reason is that when a manually entered key serves as a primary key, its minimum strength should be higher than that of a password.

NOTE: To account for the fixed key length, the key value is derived from the variable length ASCII string by a cryptographic hash function, for example, SHA-1. The resulting key has a different value and representation. It may look more random than the original ASCII string, but the derived key has the same strength as the ASCII string.

Example: Key Strength with Basic Security Considerations

In keeping with the elevated security approach given, the password scheme chosen by the user is a minimum scheme that barely satisfies the key entry policy: The user chooses to use six lowercase letters, two uppercase letters, two digits, and two special characters.

The following table presents a key with the length of 12 ASCII characters, elevated security strength:

Character class IDskeptic	Class description	Pool characters	Pool size
L	Lowercase letters	a-z	26
U	Uppercase letters	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 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 number of possible keys of this scheme with basic security considerations is as follows:

$N_{pkao} = 26^6 \times 26^2 \times 10^2 \times 16^2 \approx 5.34 \times 10^{15}$

Where:
N_{pkao}: **N**umber of possible **k**eys, **A**SCII entry, **b**asic **s**ecurity approach

The number of possible keys with basic security considerations together with the key policy is much lower than the theoretically possible different keys ($2^{128} \approx 3.40 \times 10^{38}$). That is, the example policy helps enforce only a tiny fraction of about 10^{-23} of the possible keys even with the basic security considerations.

Example: Key Strength with Elevated Security Considerations

The reduced pool size is 8 for each character type to account for frequent characters or digits such as *e*, *1*, or *,*.

The following table presents a key with length of 12 ASCII characters, elevated security strength:

Character class ID	Class description	Pool characters	Reduced pool size
L	Lowercase letters	a-z	8
U	Uppercase letters	A-Z	8
D	Digits	0-9	8
S	Special characters	!#$&+.-/ (example)	8(1)
(1) The special character pool size is given as 8 although the ASCII codes provides for 32 special characters. The reason for the smaller 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 conservative number of possible keys with elevated security considerations is as follows:

$N_{pkas} = 8^6 \times 8^2 \times 8^2 \times 8^2 = 8^{12} = 2^{36} \approx 6.87 \times 10^{10}$

Where:
N_{pkas}: **N**umber of possible **k**eys, **A**SCII entry, **e**levated **s**ecurity approach

The number of possible keys with elevated security considerations together with the previous key policy is much lower than the theoretically possible different keys ($2^{128} \approx 3.40 \times 10^{38}$). That is, the example policy helps enforce only a minute fraction of about 10^{-28} of the possible keys.

Key Entry as Hexadecimal String

Example: General Security Policy

An example key policy for the entry of a 128-bit key requires a hexadecimal string with a length between 16 and 32 characters.

In keeping with the elevated security approach, the password scheme chosen by the user is a minimum scheme that barely satisfies the key entry policy: The user chooses to use just 16 hexadecimal characters.

The following table presents a key with the length of 16 hex characters, basic security policy:

Character class ID	Class description	Pool characters	Pool size
H	Hexadecimal characters	0-9, a-f	16

The number of possible keys of this scheme is therefore:

$N_{pkho} = 16^{16} = 2^{64} \approx 1.84 \times 10^{19}$

Where:
N_{pkho}: **N**umber of possible **k**eys, hexadecimal characters, basic security policy

The number of possible keys together with the basic security key policy is much lower than the theoretically possible different keys ($2^{128} \approx 3.40 \times 10^{38}$). That is, the example policy helps enforce only a small fraction of about 10^{-11} of the possible keys with the basic security approach.

Example: Elevated Security Policy

The key policy for the entry of a 128-bit key requires a hexadecimal string of fixed length with 32 characters. This is a common situation.

The following table presents a key with the length of 16 hex characters, elevated security policy:

Character class ID	Class description	Pool characters	Pool size
H	Hexadecimal characters	0-9, a-f	16

The number of possible keys of this scheme is as follows:
$N_{pkhs} = 16^{32} = 2^{128} \approx 3.40 \times 10^{38}$

Where:
N_{pkhs}: **N**umber of possible **k**eys, hexadecimal characters, elevated security policy

The number of possible keys together with the elevated security key policy matches the number of theoretically possible different keys. That is, the example key entry policy theoretically helps enforce a strong key.

> **NOTE:** For the entry of a 256-bit key, the policy should require 64 hexadecimal characters. This helps ensure that the number of possible keys for a 256-bit key matches the number of theoretically possible different keys ($2^{256} \approx 1.16 \times 10^{77}$).

Conclusion

As the previous examples show, a policy for manual key entry that helps enforce strong key values shall require a fixed number of hexadecimal characters. The result is a key with a high theoretical strength.

However, the real key strength resulting from a strong policy can still be lower:

- Only truly random key values have the highest possible expected information content.
- Therefore, reasonably strong keys typically shall be generated by an application.
- User-chosen keys typically have significantly less randomness (that is, entropy) than application-generated keys and therefore tend to be considerably weaker than application-generated keys, despite matching a strong scheme.

There are two aspects that can impair a key's strength including the cases when the key is generated according to a strong scheme:

- Residual weaknesses of user-generated keys
- Residual weaknesses of application-generated keys

Residual Weaknesses of User-Generated Keys

Users, even if following a strong key scheme, might choose hexadecimal keys that include sequences such as *1111*or *1234*. Even if such a sequence makes up only a part of the key, it impairs the key strength. Reason: Such sequences have a high probability of occurring, which means that their entropy (randomness) is low. Therefore, such keys are considered weak because these sequences most likely are in an attacker's dictionary. This makes such keys more vulnerable to a dictionary attack, which requires less effort than a brute-force attack.

Even with basic security implementations, the probability for a user-generated password to contain a previously given example sequence is $16^{-4} \approx 1.52 \times 10^{-5}$ per sequence. In reality, the probability is much higher (rough guess: 10^{-3}) because users tend to follow patterns instead of choosing real random sequences. Furthermore, a user-generated key may contain multiple weak sequences which weakens the key further.

User-generated keys frequently contain known weak sequences. Verify any user-generated key against a list of known weak sequences before accepting it.

Residual Weaknesses of Application-Generated Keys

An application-generated key typically is stronger than a user-generated key. Nevertheless, a simple generator for hexadecimal keys might in fact also sometimes suggest keys that include sequences such as *1111* or *1234*. Such keys may be considered weak because the sequences may be in an attacker's dictionary.

The probability for an application-generated password to contain a previously given example sequence is $16^{-4} \approx 1.52 \times 10^{-5}$ per sequence. Compared to user-generated keys, this is the elevated security probability. It is also less likely than for user-generated keys that an application-generated key contains multiple weak sequences.

Because there are many known weak key sequences, the probability of an application-generated key containing one of the known weak sequences may be unacceptable. In this case, **consider verifying a system-generated key value against a list of known weak sequences.**

Example of Random Key Value Generation (Tool Use)

If you have access to a Linux command shell (for example, bash) and have the hexadecimal dump utility **xxd** installed, you can generate high-entropy key as a hexadecimal string with the following command line:

- For a 256-bit key value (32 bytes):

  $ **xxd -l 32 -c 32 -p /dev/random**

  Example output:

  26744caec971fc17300df577c8f7e7fda1297aa51881af5be7e58d0de3-f55a68

- For a 128-bit key value (16 bytes):

  $ **xxd -l 16 -c 16 -p /dev/random**

  Example output:

  d773b4352a6de7c043477b4b55d106ff

  NOTE: The random number device **/dev/random** delivers a virtually unlimited sequence of random bytes, with reasonable entropy, in binary format (the byte values are **0x00** .. **0xff**).
  You can use other tools than **xxd** to read the desired number of bytes from the random number device and to convert the bytes to the required format.

Index

E

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

www.se.com

EIO0000005492.00