SIEMENS

SIPROTEC 5
Security

V9.40 and higher

Manual

C53000-H5040-C081-A

NOTE

For your own safety, observe the warnings and safety instructions contained in this document, if available.

Disclaimer of Liability

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

Document version: C53000-H5040-C081-A.01

Edition: 12.2022

Version of the product described: V9.40 and higher

Copyright

Trademarks

Preface

Purpose of the Manual

This manual describes the security features of the SIPROTEC 5 devices and DIGSI 5, such as:

- Basic secure configuration
- Security-related device settings, parameters of the security functions and the default values
- Measures for system hardening
- Communication-interface matrix
- Instructions for security-conscious behavior, for example, backup and restore
- Explanation of security-specific log and audit messages, possible causes, and suitable countermeasures
  This information can be used as a basis for the secure design and secure operation of a complete system.

NOTE

The system characteristics that result from system-specific networking and the configuration of the products in a system are not described in this manual.

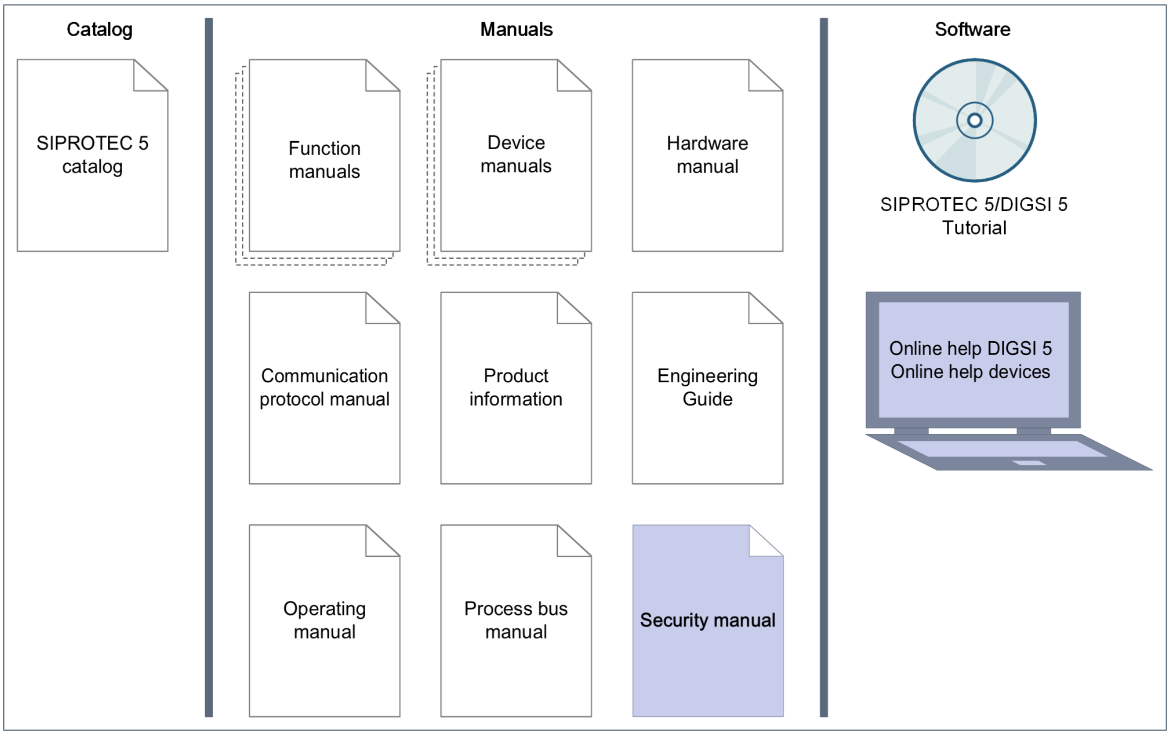
Target Audience

Protection system engineers, commissioning engineers, persons entrusted with the setting, testing and maintenance of automation, selective protection and control equipment, and operational crew in electrical installations and power plants.

Scope

This manual applies to SIPROTEC 5 and DIGSI 5 products with hardware and firmware versions V9.40 and higher.

Further Documentation



[dw_product-overview_SIP5_security-manual, 3, en_US]

- Device manuals
  Each Device manual describes the functions and applications of a specific SIPROTEC 5 device. The printed manual and the online help for the device have the same informational structure.
- Hardware manual
  The Hardware manual describes the hardware building blocks and device combinations of the SIPROTEC 5 device family.
- Operating manual
  The Operating manual describes the basic principles and procedures for operating and assembling the devices of the SIPROTEC 5 range.
- Communication protocol manual
  The Communication protocol manual contains a description of the protocols for communication within the SIPROTEC 5 device family and to higher-level network control centers.
- Security manual
  The Security manual describes the security features of the SIPROTEC 5 devices and DIGSI 5.
- Process bus manual
  The process bus manual describes the functions and applications specific for process bus in SIPROTEC 5.
- Product information
  The Product information includes general information about device installation, technical data, limiting values for input and output modules, and conditions when preparing for operation. This document is provided with each SIPROTEC 5 device.
- Engineering Guide
  The Engineering Guide describes the essential steps when engineering with DIGSI 5. In addition, the Engineering Guide shows you how to load a planned configuration to a SIPROTEC 5 device and update the functionality of the SIPROTEC 5 device.

- DIGSI 5 online help

  The DIGSI 5 online help contains a help package for DIGSI 5 and CFC.

  The help package for DIGSI 5 includes a description of the basic operation of software, the DIGSI principles and editors. The help package for CFC includes an introduction to CFC programming, basic examples of working with CFC, and a reference chapter with all the CFC blocks available for the SIPROTEC 5 range.
- SIPROTEC 5/DIGSI 5 Tutorial

  The tutorial on the DVD contains brief information about important product features, more detailed information about the individual technical areas, as well as operating sequences with tasks based on practical operation and a brief explanation.
- SIPROTEC 5 catalog

  The SIPROTEC 5 catalog describes the system features and the devices of SIPROTEC 5.

Indication of Conformity

This product complies with the directive of the Council of the European Communities on harmonization of the laws of the Member States concerning electromagnetic compatibility (EMC Directive 2014/30/EU) and electrical equipment for use within specified voltage limits (Low Voltage Directive 2014/35/EU).

This conformity has been proved by tests performed according to the Council Directive in accordance with the product standard EN 60255-26 (for EMC directive) and with the product standard EN 60255-27 (for Low Voltage Directive) by Siemens.

The device is designed and manufactured for application in an industrial environment.

The product conforms with the international standards of IEC 60255 and the German standard VDE 0435.

Standards

IEEE Std C 37.90

The technical data of the product is approved in accordance with UL.

For more information about the UL database, see *ul.com*

You can find the product with the **UL File Number E194016**.

IND. CONT. EQ.
69CA

Additional Support

For questions about the system, contact your Siemens sales partner.

Customer Support Center

Our Customer Support Center provides a 24-hour service.

Siemens AG	
Smart Infrastructure – Protection Automation	Tel.: +49 911 2155 4466
Customer Support Center	E-Mail: *energy.automation@siemens.com*

Training Courses

Inquiries regarding individual training courses should be addressed to our Training Center:

Siemens AG	
Siemens Power Academy TD	Phone: +49 911 9582 7100
Humboldtstraße 59	E-mail: *poweracademy@siemens.com*

90459 Nuremberg
Germany

Internet: *www.siemens.com/poweracademy*

Notes on Safety

This document is not a complete index of all safety measures required for operation of the equipment (module or device). However, it comprises important information that must be followed for personal safety, as well as to avoid material damage. Information is highlighted and illustrated as follows according to the degree of danger:

DANGER

DANGER means that death or severe injury **will** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid death or severe injuries.

WARNING

WARNING means that death or severe injury **may** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid death or severe injuries.

CAUTION

CAUTION means that medium-severe or slight injuries **can** occur if the specified measures are not taken.

✧ Comply with all instructions, in order to avoid moderate or minor injuries.

NOTICE

NOTICE means that property damage **can** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid property damage.

NOTE

Important information about the product, product handling or a certain section of the documentation which must be given attention.

OpenSSL

This product includes software developed by the OpenSSL Project for use in OpenSSL Toolkit (*http://www.openssl.org/*).
This product includes software written by Tim Hudson (*tjh@cryptsoft.com*).
This product includes cryptographic software written by Eric Young (*eay@cryptsoft.com*).

Table of Contents

1 Introduction

1.1 Objective

In the past, computers were islands of functionality with little interconnectivity, if any at all. Nowadays computer servers, Desktop PCs, and automation units are linked with each other.

On one hand, the current mode creates new business opportunities. On the other hand, these interconnected components, for example, applications that are not designed for use in heavily networked environments, can be attacked.

The most important aspect for this manual is to address the increasing use of the following technologies:

- Routable standard protocols, such as IP and TCP
- Connection of the traditionally isolated networks, such as remote stations
- Standard software components, such as the OEM (Original Equipment Manufacturer) operating systems like Windows

The manual serves as a recommendation for the secure commissioning and operations of the SIPROTEC 5 devices in networked environments.

1.2 Observance of Standards

Siemens offers products and technologies, which consider the leading cybersecurity standards. The major drivers for secure infrastructures are the standards and guidelines, such as IEC 62443, IEC 62351, BDEW White Paper, IEEE 1686, and NERC CIP (Critical Infrastructure Protection).

1.3 Security Requirements

The most important security requirements are the following:

- Authentication and authorization of the users
- Assurance of the integrity of the transmitted data
- Protections against virus, trojans, and other malware
- Collection and saving of log files
- Operation of the system in a protected environment (physical security)
- Every user is given the only those rights that are necessary to fulfill the corresponding work.
- Assurance that in case of a system failure, a restoration is possible without or only with marginal data loss
- Only activate required services and ports
- Network load of critical systems is limited to the extent to make the systems continue to work under maximum load. For example, limit the number of broadcasts in the power-system components.

1.4 Security Services

In different CPUs (Port J) and communication modules, supported security services are different. The following table shows detailed information.

Table 1-1 Supported Services in CPUs (Port J) and Communication Modules

	CPU Types				Module Types				
Security Services	CP100	CP150	CP200	CP300	ETH-BA-2EL	ETH-BB-2FO	ETH-BD-2FO	ETH-YC-2FO	ETH-YA-2EL
DIGSI client authentication over TLS	■[1]	■	■	■	■	■	■	■	■
Web server over TLS	■	■	■	■	■	■	■	■	■
RBAC RADIUS client	■	■	–	■	■	■	■	■	■
RBAC LDAP client	–[2]	■	–	■	■	■	■	■	■
DDoS traffic limiter	■	■	–	■	■	■	■	–	–
Ethernet-based service restriction	■	■	–	■	■	■	■	■	■
Syslog over UDP	■	■	■	■	■	■	■	■	■
Syslog over TLS	–	■	–	■	■	■	■	■	■
EST client	–	■	–	■	■	■	■	■	■
IEEE 802.1X supplicant	■	–	–	–	■	■	■	–	–
Secure MMS over TLS	–	■	–	■	–	–	■	■	■
Security monitoring over SNMPv3	–	–	–	–	–	–	■	–	–
Asset monitoring over SNMPv3	–	–	–	–	–	–	■	–	–

NOTE

The CPU types CP100 and CP150 are for SIPROTEC 5 non-modular devices. The CPU types CP200 and CP300 are for SIPROTEC 5 modular devices.

The module types ETH-YA-2EL and ETH-YC-2FO are for SIPROTEC 5 Compact devices. The other module types are for SIPROTEC 5 devices.

[1] Symbol ■ indicates that the service is supported.

[2] Symbol – indicates that the service is not supported.

2 Measures for System Hardening

2.1 Overview

The Federal Office for Information Security (BSI) in Germany describes hardening in IT security as “[...] the removal of all software components and functions that are not absolutely necessary for the fulfillment of the intended task by a program.”

In practice, hardening measures fulfill the following objectives:

- Reducing the possibilities for exploiting vulnerabilities
- Minimizing the possible attack methods
- Restricting an attacker from available tools in case of a successful attack
- Minimizing available privileges of an attacker in case of a successful attack
- Increasing the probability of detecting a successful attack

A possible reduction of the complexity and the maintenance work of the system can also be regarded as a secondary objective of hardening, which can improve manageability and therefore minimize administration errors.

2.2 Intended Operational Environment

Siemens recommends applying the provided security updates by using the corresponding tooling and documented procedures that are available with the product. If supported by the product, an automatic means to apply the security updates across multiple product instances can be used.

Siemens recommends validating any security update before being applied, and supervision by trained staff of the update process in the target environment.

As a general security measure, Siemens recommends protecting the network access with appropriate mechanisms, for example, firewalls, segmentation, or VPN.

To run the devices in a protected IT environment, Siemens recommends configuring the environment according to the operational guidelines. You can find recommended security guidelines to Secure Substations at *https://www.siemens.com/gridsecurity*.

The following assumptions or constraints apply to the intended operational environment in which the SIPROTEC 5 devices are deployed as recommended in this manual:

- The control center does not communicate with the SIPROTEC 5 device directly.
- Remote Ethernet connections to substations are secured via virtual private Network (VPN) or transport layer security (TLS).
- The substation is physically protected (security perimeter).
- The role-based access control (RBAC) functionality is activated in the SIPROTEC 5 devices.
- The time server is configured and the device time is synchronized.
- The DIGSI 5 instances use client certificates issued by your certificate authority (CA) to establish the TLS connection to SIPROTEC 5 devices. For more information, refer to *6.5 DIGSI 5 Client Authentication*.
- The OPC UA PubSub protocol for IoT connectivity is activated on a communication module that does not support any other process-critical communication, for example, GOOSE/SV.

2.3 Supported LAN Services

2.3.1 List of Required Open Ports

Table 2-1 List of Required Open Ports

Service	Layer 4 Protocol	Layer 7 Protocol	Typical Client	Client Port	Typical Server	Server Port	Mainboard	Communication Module
DIGSI 5 protocol to Automation License Manager	TCP	DIGSI 5 protocol to Automation License Manager	DIGSI 5 PC	4410 (default value)	Automation License Manager on a separate server	4410 (default value)	–	–
DIGSI 5 protocol to SIPROTEC 5	TCP	HTTPS	DIGSI 5 PC	> 1024	SIPROTEC 5	443	■	■
Reporting/ IEC 61850/MMS	TCP	IEC 61850	IEC 61850 client (for example, SICAM PAS or SICAM A8000)	> 1024	SIPROTEC 5	102	■	■
Reporting/ IEC 61850/ Secure MMS	TCP	IEC 61850	IEC 61850 client (for example, SICAM PAS or SICAM A8000)	> 1024	SIPROTEC 5	3782	■	■
Time synchronization/SNTP	UDP[3]	SNTP	SIPROTEC 5	123	SNTP server	123	■	■
Monitoring via Simple Network Management Protocol (SNMPv3)	UDP	SNMPv3	PC with SNMP client (for example, SICAM PAS/1703/DIGSI 5 PC/remote DIGSI 5 PC)	> 1024	SIPROTEC 5	161	–	■
DNP3i	TCP	DNP3 TCP	SICAM PAS	20000 or next free port	SIPROTEC 5	20000	–	■
Synchrophasor	TCP UDP	–	Phasor data concentrator	> 1024	SIPROTEC 5	4712 4713	–	■
MODBUS TCP	TCP	MODBUS	Substation controller	> 1024	SIPROTEC 5	502	–	■
RTD unit	UDP	RTD	RTD unit	> 1024	SIPROTEC 5	Can be configured	■	■
Syslog client	UDP	–	SIPROTEC 5	–	Syslog server	514	■	■
Syslog TLS client	TCP	TLS	SIPROTEC 5	–	Syslog TLS server	6514	■	■
RADIUS[4] client	UDP	–	SIPROTEC 5	–	RADIUS server	1812	■	■
OPC UA	TCP	MQTT	SIPROTEC 5	–	Broker	8883	–	■
Web service	TCP	HTTPS	Web browser	–	SIPROTEC 5	4443	■	■

[3] UDP: User Datagram Protocol

[4] RADIUS: Remote Authentication Dial-In User Service

Service	Layer 4 Protocol	Layer 7 Protocol	Typical Client	Client Port	Typical Server	Server Port	Main-board	Commu-nication Module
LDAP[5] client	TCP	LDAP	SIPROTEC 5	–	LDAP server	389	■	■
Automatic certificate management with EST	TCP	EST	SIPROTEC 5	> 1024	EST server	8083	■	■

For more information about the supported communication protocols, refer to the *SIPROTEC 5 Communication Protocols Manual*.

2.3.2 Deactivation of Unnecessary System and Communication Services

After receiving the delivered devices, first of all, you must initialize the devices. Only after that, the devices are ready for operation.

By default, only the connection to DIGSI 5 is activated in the device. All other Ethernet services and ports are deactivated in the device by default and can be activated via DIGSI 5. Due to the secure default configurations, there is no open interface for potential attackers and only used services are activated in the network.

At any point, you can disable unnecessary services in the device via DIGSI 5.

2.3.3 Diagnostics Homepage

After commissioning, Siemens recommends disabling the Diagnostics Homepage services for operations on the mainboard and on the communication modules because the diagnostics services do not support HTTPS or access control. You can find more information on Homepage in the *DIGSI 5 online help*.

[5] LDAP: Lightweight Directory Access Protocol

2.4 Hardening Measures

The following hardening measures are applied:

- Hardening the Windows system
  The Windows system has to be hardened according to the manual *System Hardening for Substation Automation and Protection*. You can obtain this manual by visiting *https://www.siemens.com/gridsecurity* and accessing **Downloads Cyber Security** → **Manuals** → **Secure Substation - Manual**.
- Uninstalling or deactivating unnecessary software components, such as message simulation and data-flow test tools
- Deactivating unnecessary system and communication services, such as remote operation and remote maintenance
- Deactivating unnecessary user accounts
- Activating configuration options that improve security
- Limiting the rights of users and programs

NOTE

You can find a collection of Best-Practice hardening guides for various operating systems, server services, and standard applications, for example, at the Center for Internet Security via *http://www.cisecurity.org*.

3 Access Control

3.1 Access Control with Connection Password

3.1.1 Introduction

SIPROTEC 5 devices support user authentication and operations for protecting access to the security-relevant operations and functions. You can select between the centralized Role-Based Access Control (RBAC) option and the device-specific DIGSI 5 connection password option.

If you do not intend to use the RBAC feature, set up the devices to conduct a user authentication using the connection password.

Furthermore, if RBAC is disabled, to prevent you from executing safety-critical actions on the device unintentionally, you can set up confirmation IDs. You can find more information about the confirmation ID in the *SIPROTEC 5, Operation* manual.

3.1.2 Connection-Password Configuration

The connection password follows the NERC-CIP-standard (North American Electric Reliability Critical Infrastructure Protection) and consists of the following parts:

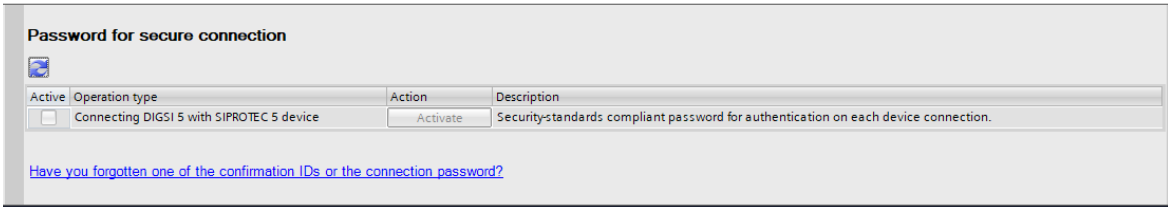
- Lower-case letters
- Upper-case letters
- Digits
- Special characters, for example, %, &, $

The length of the connection password ranges from 8 characters to 24 characters. DIGSI 5 verifies the length during entering.

The connection password is empty by default. When typing a new connection password, the input characters are concealed by asterisks. To confirm the connection password, enter it twice. This confirmation prevents erroneous entries.

NOTE

The deactivation of the connection password results in providing everyone unauthenticated and unrestricted access to the device through DIGSI 5 or through the browser-based user interface. If you wish to hinder this, set the connection password in the device.



Password for secure connection

Active	Operation type	Action	Description
□	Connecting DIGSI 5 with SIPROTEC 5 device	Activate	Security-standards compliant password for authentication on each device connection.

Have you forgotten one of the confirmation IDs or the connection password?

[sc_password_connection, 1, en_US]

Figure 3-1 Setting Window for the Connection Password

Once you enter a new connection password, DIGSI 5 transfers it to the device automatically.

Initialization of the connection password is possible only via the front USB interface or via an Ethernet interface of the device. In both cases, the entered connection password is securely transferred to the device via the TLS protocol. The connection password is not stored in the DIGSI 5 project or anywhere on the Windows PC. It is stored as a salted hash in the device.

If you have initialized the connection password, further access to the device (via DIGSI 5 or via the browser-based user interface) is possible only if you enter the correct connection password in the DIGSI 5 dialog while establishing a connection to the device. This procedure prevents unauthenticated access. Siemens recommends checking the connection password after initialization.

You can change the connection password online via an Ethernet connection. After entering the current connection password and entering and repeating the new connection password, the device accepts the change.

3.1.3 Authentication and Connection Password During Operation

The 1st sequence between DIGSI 5 and the device is an authentication procedure based on the TLS 1.2 protocol in which digital certificates are exchanged between DIGSI 5 and the device. This procedure ensures that only DIGSI 5 can have full engineering access to a SIPROTEC 5 device. If other applications try to gain access, they are blocked.

Following the TLS authentication, the SIPROTEC 5 device queries the connection password, if you have set one in the device.

To gain access to a device, the correct connection password is necessary. If you enter a wrong connection password, the device records this action in the security log. If you enter wrong connection password for 5 times, access to the device is blocked for 5 minutes. These operations are recorded in the security log of the device as well.

A session manager in DIGSI 5 monitors all passwords and entries relevant for identification for 30 minutes.

3.1.4 Resetting and Deactivating the Connection Password

If you forget the set connection-password, before deactivating it, you have to reset it.

Resetting the Connection Password for a Device with a Display

Proceed as follows:

✧ In the device, switch to the `Device functions` menu in the main menu.

✧ Select the `Security` > `Password recovery` menu item.

✧ Confirm the resetting of the password with the `Ok` softkey.

- or -

✧ Cancel the operation with `Esc`.

✧ Enter the confirmation ID **222222** and confirm it by pressing `Enter`.

✧ Enter the following keyboard shortcut as recovery code:
<1>, <2>, <3>, <4>, <5>, <6>, <FN>+<1>, <FN>+<2>, <FN>+<3>, <FN>+<4>, <FN>+<5>, and <FN>+<6>

NOTE

The time-out between key operations is 1 s.

Resetting the Connection Password for a Device without Display or a Device in Fallback Mode

Proceed as follows:

✧ Isolate the device from the power supply.

✧ Remove the battery from the device and wait for 2 minutes.

✧ Insert the battery into the device.

✧ Reconnect the device to the power supply.

The connection password is reset.

NOTE

If you forget the connection password, you must reset it before deactivating it.

Deactivating the Connection Password on a Device

Proceed as follows:

✧ Switch to the **`Device functions`** menu in the main menu of the device.

✧ Select the **`Security`** > **`Password switch`** menu item.

✧ Enter the confirmation ID **222222**.

✧ Deactivate the connection password.

NOTE

If the device battery no longer functions or has been taken out, the connection password is deactivated after restarting the device.

Deactivating the Connection Password in DIGSI 5

Proceed as follows:

✧ In DIGSI 5, enter the correct connection password.

DIGSI 5 is connected to the device.

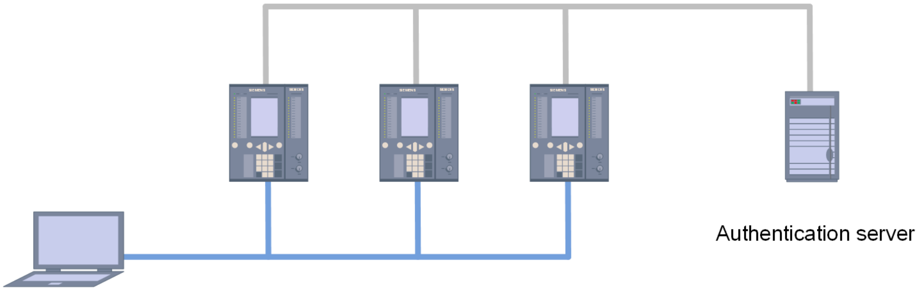
✧ Navigate to **Device** > **Safety and security** > **Operations safety and access control**.

✧ In the **Password for secure connection** section, uncheck the operation type **Connecting DIGSI 5 with SIPROTEC 5 device**.

3.2 Role-Based Access Control (RBAC) in SIPROTEC 5

3.2.1 Overview

To protect access to a SIPROTEC 5 device for performing security-relevant operations and functions, you can activate the RBAC feature. After activation, all users will be uniquely authenticated and authorized with their centrally managed user accounts as for each access attempt.



[dw_authentication_server, 2, en_US]

Figure 3-2 Authentication Server

SIPROTEC 5 devices support RBAC with predefined standards-based roles. User accounts are assigned roles; roles receive rights according to their functions.

The assignment between users and roles is defined in an authentication server. The assignment of rights to roles is predefined in the security configuration of the SIPROTEC 5 devices.

SIPROTEC 5 devices support the following requirements:

- Standard roles and roles-to-rights assignments from the IEC 62351-8 and IEEE 1686 standards
- Standard roles and rights recommended in the BDEW white paper
- Centralized management of user accounts, roles, and areas of responsibilities (AoR) in an authentication server
- Offline/emergency user account access when the authentication server is unreachable

You can enable or disable RBAC for a SIPROTEC 5 device via DIGSI 5. For more information, refer to *3.2.2.2 Activation of Authentication Servers*.

NOTE

If RBAC is deactivated, you can protect the device against unauthenticated access with the connection password and prevent unintended safety-critical actions with confirmation IDs. For more information, refer to *3.1.4 Resetting and Deactivating the Connection Password*.

3.2.2 Authentication Servers

3.2.2.1 General

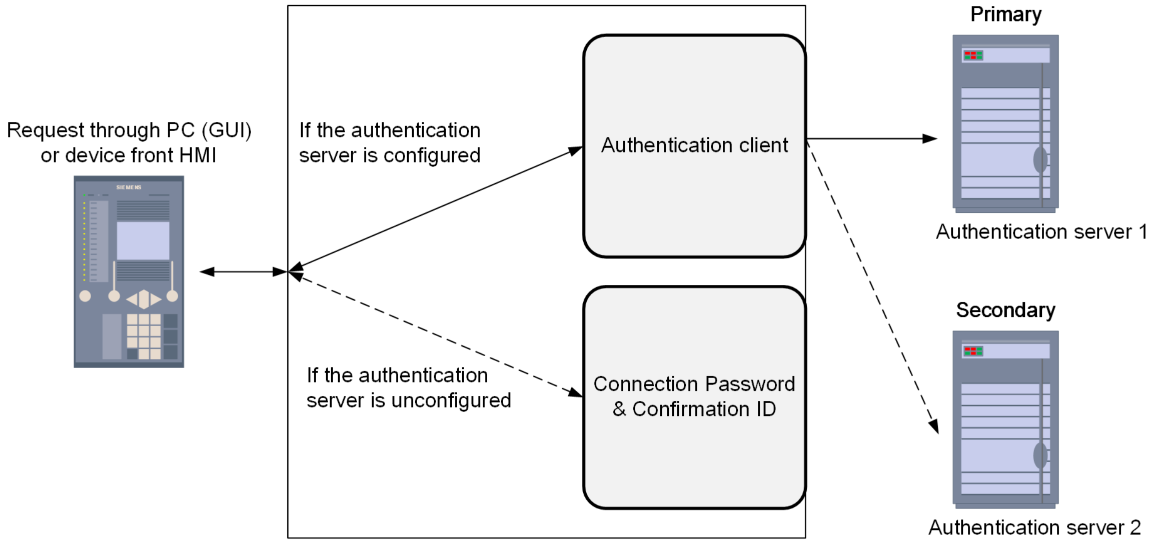
The main tasks of the authentication servers are user authentication and control of user access rights. The client implementation is integrated in the SIPROTEC 5 device firmware.

A SIPROTEC 5 device sends the user name and password to an authentication server. With unique user names and passwords, the authentication server checks if the connecting users are correctly claimed. If the user is clearly identified, the authorization handles the assignment of the access rights. The user receives specific access rights to data or services of the SIPROTEC 5 device.

Furthermore, the following information of the access-attempt events is recorded for later analysis (audit trail):

- Connection attempts
- User name and role information
- Time of login

For more information on the recorded security events, refer to *9.4.3 Syslog Events SIPROTEC 5*.



[dw_connection_radius-server, 3, en_US]

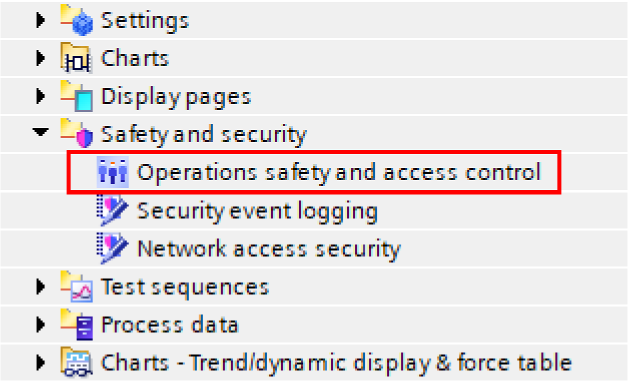
Figure 3-3 Connection between Device and Authentication Servers

3.2.2.2 Activation of Authentication Servers

✧ Open a project in DIGSI 5.

✧ Open the **Safety and security** menu item in the project tree.

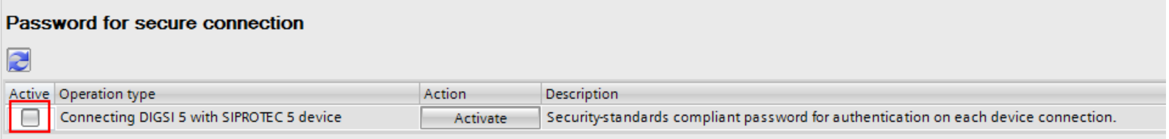
✧ Double-click the **Operations safety and access control** menu item.



[sc_project-tree_rbac, 2, en_US]

Figure 3-4 Project Tree

✧ If the connection password is activated in the **Confirmation IDs and connection password** section, deactivate it.



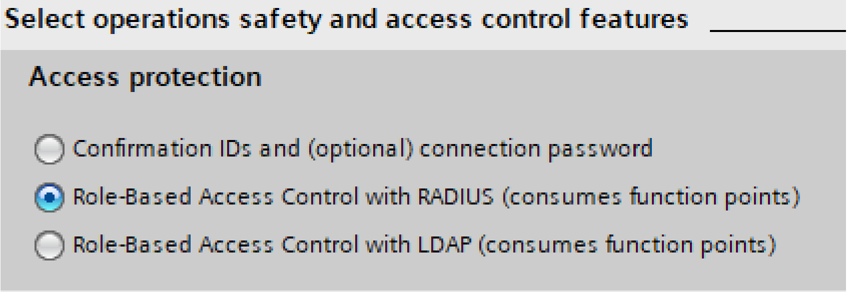
Password for secure connection

Active	Operation type	Action	Description
☐	Connecting DIGSI 5 with SIPROTEC 5 device	Activate	Security-standards compliant password for authentication on each device connection.

[sc_deactivate_connection_password, 1, en_US]

Figure 3-5 Deactivating the Connection Password

✧ Activate the RBAC with RADIUS feature or LDAP feature.



Select operations safety and access control features

Access protection

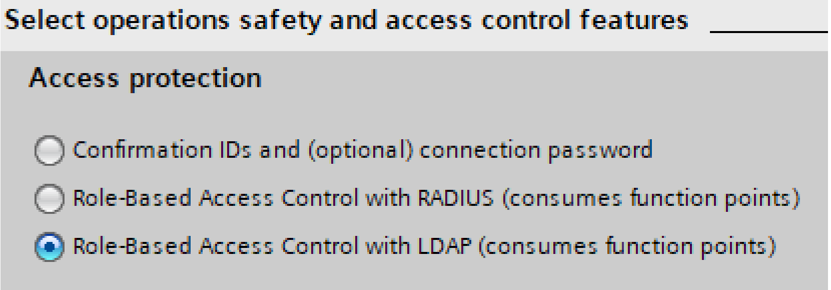
○ Confirmation IDs and (optional) connection password

● Role-Based Access Control with RADIUS (consumes function points)

○ Role-Based Access Control with LDAP (consumes function points)

[sc_rbac_select, 4, en_US]

Figure 3-6 Switching on the RADIUS



Select operations safety and access control features

Access protection

○ Confirmation IDs and (optional) connection password

○ Role-Based Access Control with RADIUS (consumes function points)

● Role-Based Access Control with LDAP (consumes function points)

[sc_LDAP_RADIUS_enabled, 1, en_US]

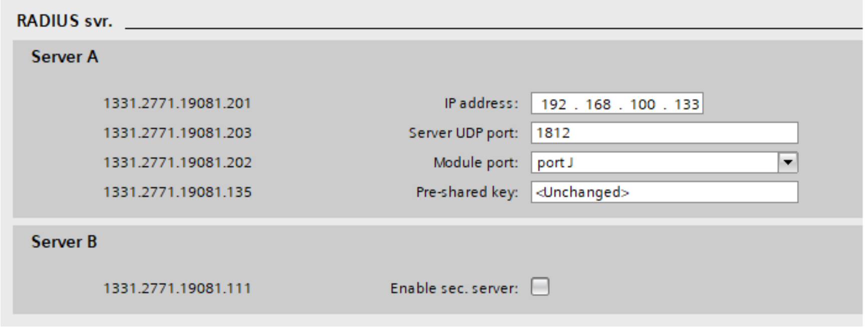
Figure 3-7 Switching on the LDAP

NOTE

When you activate the RBAC, the emergency access is not enabled by default. To use the emergency account, configure the emergency password first.

3.2.2.3 Configurations for the RADIUS-Server-Connection

To establish a connection between the SIPROTEC 5 device and a RADIUS server that is used as the authentication server, define the following parameters in DIGSI 5.



RADIUS svr.

Server A

1331.2771.19081.201	IP address:	192 . 168 . 100 . 133
1331.2771.19081.203	Server UDP port:	1812
1331.2771.19081.202	Module port:	port J
1331.2771.19081.135	Pre-shared key:	<Unchanged>

Server B

1331.2771.19081.111	Enable sec. server:	☐

[sc_radius-server, 2, en_US]

Figure 3-8 Example of a RADIUS-Server Configuration in DIGSI 5

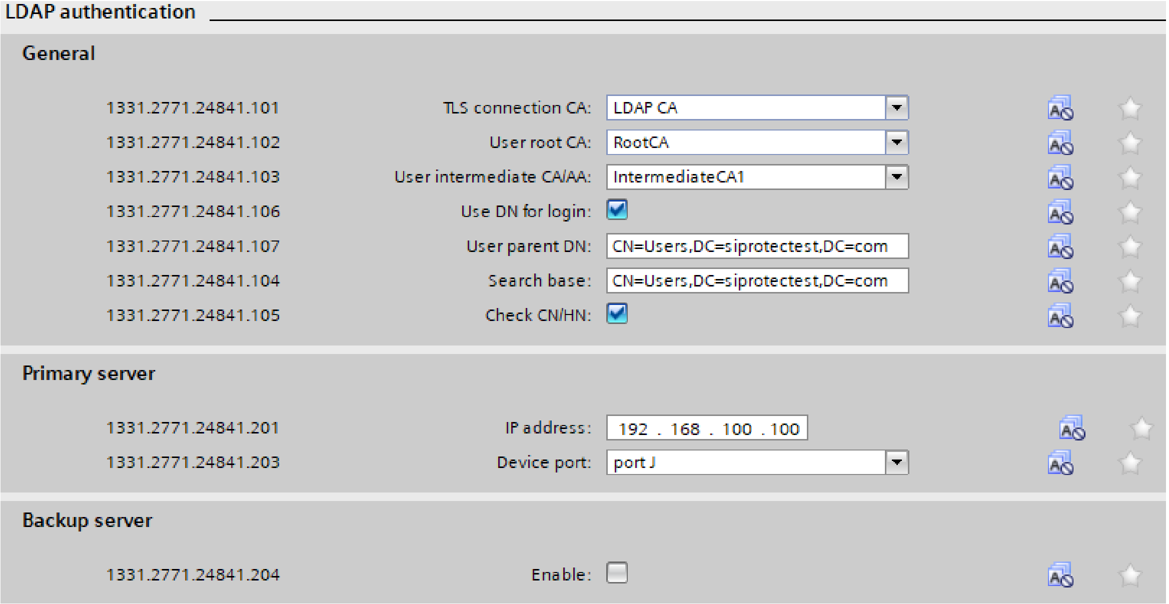
Parameter Name	Description
Server A	
IP address	IP address of the RADIUS server to be connected
Server UDP port	Port number of the RADIUS server to be connected
Module port	Device port, through which the SIPROTEC 5 device communicates with the RADIUS server
Pre-shared key	A key for the authentication and protection of the communication between the RADIUS server and the device When the configuration is loaded, the device verifies if the pre-shared key is the same as that mentioned in the RADIUS server.
Server B	
Enable sec. server	With this check box, you enable or disable server B.

If a new RADIUS server is used, keep the account SECADM the same in the old and new RADIUS servers. For more information about the account SECADM, refer to *3.2.6 Basic Properties of the Assignment of Rights and Supported Roles*.

If the attribute **`ValidFrom`** is configured in the RADIUS server, according to the standard IEC 62351-8, the value of this attribute must follow the format ***`YYYYMMDDHHMMSSZ`*** (Year, Month, Day, Hour, Minutes, Seconds, Zulu time zone) and must be larger than ***`19700101000000Z`***. Otherwise, the user authentication fails.

3.2.2.4 Configurations for the LDAP-Server-Connection

To establish a connection between a SIPROTEC 5 device and an LDAP server via the protocol StartTLS over port 389, configure the following parameters in DIGSI 5.



LDAP authentication

General

1331.2771.24841.101 TLS connection CA: LDAP CA
1331.2771.24841.102 User root CA: RootCA
1331.2771.24841.103 User intermediate CA/AA: IntermediateCA1
1331.2771.24841.106 Use DN for login: ☑
1331.2771.24841.107 User parent DN: CN=Users,DC=siprotectest,DC=com
1331.2771.24841.104 Search base: CN=Users,DC=siprotectest,DC=com
1331.2771.24841.105 Check CN/HN: ☑

Primary server

1331.2771.24841.201 IP address: 192 . 168 . 100 . 100
1331.2771.24841.203 Device port: port J

Backup server

1331.2771.24841.204 Enable: □

[sc_LDAP, 2, en_US]

Figure 3-9 Example of a LDAP-Server Configuration in DIGSI 5

SIPROTEC 5 devices support 2 types of user certificates: end-entity certificates and attribute certificates. The imported user certificates can be in different types.

Table 3-1 Explanations of LDAP-Related Parameters in DIGSI 5

Parameter Names	Descriptions
General	
TLS connection CA	CA that issues the LDAP server certificate for the TLS connection between the SIPROTEC 5 device and the LDAP server
User root CA	The CA that issues the user intermediate CAs or the user certificates
User intermediate CA/AA	User intermediate certificate authority or attribute authority • If you keep the default value ***Not configured***, issuing and authentication of the user certificates are done by the set **User root CA**. • If you set the parameter **User intermediate CA/AA** to issue user certificates, authentication of the issued user certificates must be done by the intermediate CA/AA. For attribute certificates, the parameter is mandatory.
Use DN for login	With this checkbox, you can show or hide the parameter **User parent DN**. For LDAP binding strings, the differences are as follows: • Uncheck the parameter The LDAP binding strings are in the form of **<user name>**. • Check the parameter The LDAP binding strings are in the form of **<user name>,<user parent DN>**. For example, if you set the parameter **User parent DN** according to *Figure 3-9* and the user name is ***258***, then the LDAP binding string is **cn=258,CN=Users,DC=siprotectest,DC=com**. For LDAP servers that are based on the software OpenLDAP, check the parameter.
User parent DN	Parent distinguished name of an authenticated user If the operating system of the LDAP server is Linux, the parameter is mandatory.
Search base	The place that the search starts in the LDAP server
Check CN/HN	With this check box, you can enable or disable the check of CN (common name) in the end-entity certificates or HN (holder name) in the attribute certificates.
Primary server	
IP address	IP address of the LDAP server to be connected
Device port	Device port through which the SIPROTEC 5 device communicates with the LDAP server
Backup server	
Enable	Enable or disable the backup server with this check box

NOTE

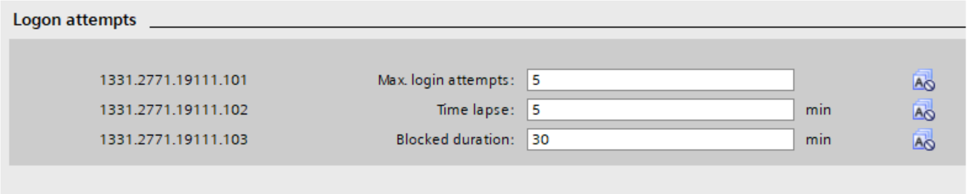
Siemens has only tested attribute certificates in the PULL mode of the Mircosoft product Active Directory.

If a new LDAP server is used, keep the account SECADM the same in the old and new LDAP servers. For more information about the account SECADM, refer to *3.2.6 Basic Properties of the Assignment of Rights and Supported Roles*.

3.2.3 Login Attempts

To secure logins with emergency accounts or with the cached user information, DIGSI 5 provides the following parameters. To handle incorrect remote-login attempts, you can configure related parameters in the authentication servers.

- **`Max. login attempts`**
  With this parameter, you set the maximum number of sequential login attempts for a user.
- **`Time lapse`**
  With this parameter, you set the time range after which the number of login attempts is set back to 0 after the last unsuccessful attempt.
- **`Blocked duration`**
  With this parameter, you set the time duration for which the device remains blocked after the maximum number of login attempts is reached.
  If you log on with wrong credentials, the login attempts are counted. Once the maximum number of login attempts has been reached, logging on is not possible for the set **`Blocked duration`**. If this **`Blocked duration`** has elapsed, login can be attempted again.



Logon attempts

1331.2771.19111.101	Max. login attempts:	5	
1331.2771.19111.102	Time lapse:	5	min
1331.2771.19111.103	Blocked duration:	30	min

[sc_logon_attempts, 2, en_US]

Figure 3-10 Login Attempts

NOTE

The login cannot be attempted if the following conditions are met:

- The login is blocked.
- The device time is not synchronized with a central time server and is earlier than the total of the login-blocked time and the **`Blocked duration`**.

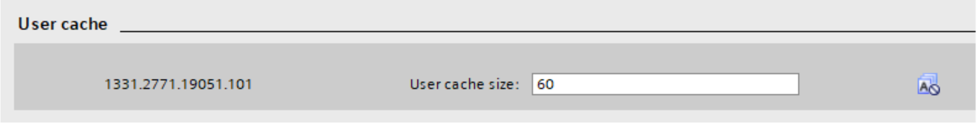
3.2.4 User Cache Size

With the RBAC user-cache feature enabled, the device caches user credentials that have been successfully authenticated by the authentication server. When the authentication server connectivity is interrupted, such users can log on to the device with their cached user credentials and operate the device with their cached roles. Each time a user logs on successfully, the device updates the corresponding user-cache entry with the latest credentials (the user name and the hashed password) and the role(s).

With the parameter **`User-cache size`**, you define the maximum number of cached user accounts. To disable the user-cache feature, set the size to ***0***.

NOTE

If the SIPROTEC 5 communication modules are used for the RBAC authentication, set the cache size to at least ***1***.



User cache

1331.2771.19051.101

User cache size: 60

[sc_rbac_user_cache, 2, en_US]

Figure 3-11 User-Cache Settings

3.2.5 Loading Security Settings

After a successful configuration of RBAC, load the security settings to the SIPROTEC 5 device.

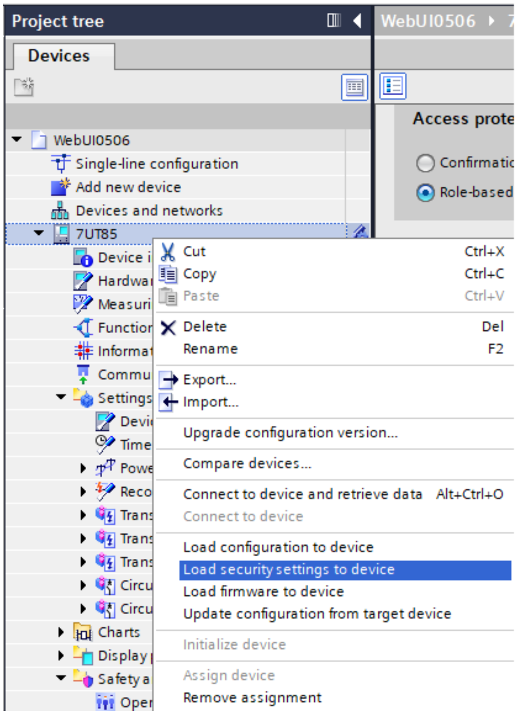
NOTE

Only the user accounts which are assigned with the role SECADM or the role Administrator have the authority to load security settings to a device.

How to Load the Security Settings

Proceed as follows:

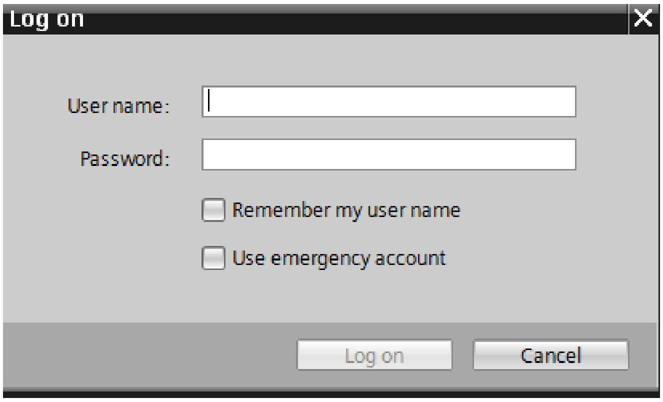
- ✧ Select the device in the project tree.
- ✧ Right-click the device.
- ✧ In the opened context menu, select **Load security settings to device**.



[sc_secutrans, 1, en_US]

Figure 3-12 Menu Selection Load Security Settings to Device

If you have activated RBAC, the following login dialog appears:



[sc_logondev, 2, en_US]

Figure 3-13 Log in to the Device

✧ Enter the **User name**.

✧ Enter the **Password**.

✧ Click **Log on**.

The transmission of the security settings to the device starts. Once the device receives the security settings, it verifies the provided authentication-server-settings by trying to authenticate the provided user name and password combination. The device accepts the security settings only if the authentication succeeds. The transmission result is finally displayed.

✧ Confirm the result with **OK**.

The security settings are now activated in the device.

NOTE

Loading security settings works only if at least one of the configured authentication servers is accessible.

If no authentication server is reachable, the device rejects the security settings. The cached credentials of security administrators or administrators are inapplicable for this action.

3.2.6 Basic Properties of the Assignment of Rights and Supported Roles

A role is a combination of rights defined for the SIPROTEC 5 device. You can assign a role to users in various contexts. The roles a user has in specific contexts determines what the user is or is not allowed to do in the SIPROTEC 5 device.

The following tables show the overview of the basics of rights and supported roles according to:

- IEEE 1686
- BDEW white paper
- IEC 62351-8 standard
- SIPROTEC 5 operational requirement

NOTE

You cannot change the security settings via the device operation panel regardless of your access rights.

Roles in DIGSI 5

Table 3-2 Overall Assignment of Rights and Supported Roles in DIGSI 5

Rights	Functionality of Rights	Assignment of Supported Roles						
		VIEWER	OPERATOR[6] + ENGINEER	ENGINEER	INSTALLER	SECADM	SECAUD[7] + ENGINEER	Administrator
None	Viewing general information on the IED	■	■	■	■	■	■	■
View data	Viewing operational data on the IED	–	■	■	■	–	■	■
Force values	• Changing values • Overwriting actual data • Triggering a process	–	■	–	–	–	–	■
Change CFG	Changing/downloading/uploading the configuration	–	■	■	■	–	■	■
Change FW	Changing the firmware	–	–	–	■	–	–	■
Audit trail	Audit trail	–	–	–	–	–	■	■
Security management	Managing and performing the security functions	–	–	–	–	■	–	■

Roles on the Browser-Based User Interface

Table 3-3 Overall Assignment of Rights and Supported Roles for the Browser-Based User Interface

Rights	Functionality of Rights	Assignment of Supported Roles						
		VIEWER	OPERATOR[8] + ENGINEER	ENGINEER	INSTALLER	SECADM	SECAUD[9] + ENGINEER	Administrator
None	Viewing general information on the IED	■	■	■	■	■	■	■
View data	Viewing operational data on the IED	–	■	■	■	–	■	■
Force values	• Changing values • Overwriting actual data • Triggering a process	–	■	–	–	–	–	■
Change CFG	Changing/downloading/uploading the configuration	–	■	■	■	–	■	■

[6] In DIGSI 5, the role OPERATOR cannot work independently.

[7] In DIGSI 5, the role SECAUD cannot work independently.

[8] For the browser-based user interface, the role OPERATOR cannot work independently.

[9] For the browser-based user interface, the role SECAUD cannot work independently.

Roles on the On-Site Device

Table 3-4 Overall Assignment of Rights and Supported Roles on the On-Site Devices

Rights	Functionality of Rights	Assignment of Supported Roles						
		VIEWER	OPERATOR	ENGINEER	INSTALLER	SECADM	SECAUD	ADMIN
None	Viewing general information on the IED	■	■	■	■	■	■	■
View data	Viewing operational data on the IED	■	■	■	■	■[10]	■[10]	■
View CFG settings	Viewing configuration settings on the IED	■	■	■	■	■	–	■
Force values	• Changing values • Overwriting actual data • Triggering a process	–	■	–	–	–	–	■
Change CFG	Changing the configuration	–	–	■	■	–	–	■
Change FW	Changing the firmware	–	–	–	–	–	–	–
Audit trail	Audit trail	–	–	–	–	–	■	■
Security management	Managing and performing the security functions	–	–	–	–	–	–	–

NOTE

The ID of the role Administrator is FFFF8460 (hexadecimal) or -31648 (decimal).

Extra Supported Roles

Besides the standards-based supported roles, the following extra supported roles are available. These roles address familiar operations that are supported by the device with the RBAC disabled, for example, protection against unintended operations with confirmation IDs.

Roles	Hexadecimal IDs	Decimal IDs
OPERATOR_SWITCHING	FFFFFF9A	-102
SWITCHING_AUTHORITY	FFFFFF99	-103
INTERLOCKING_MODE	FFFFFF98	-104

User names that are assigned with the extra supported roles can only work on the on-site devices. To use such user names, you must configure them on the authentication server first. You can find more information on configuration of the authentication server in the download area under *http://www.siemens.com/gridsecurity* > **Cyber Security Products and Solutions** > **Cyber Security General Downloads** > **Application Notes**.

[10] Logs are excluded.

Table 3-5 Overall Assignment of Rights and Extra Supported Roles on the On-Site Devices

Rights	Functionality of Rights	Assignment of Extra Supported Roles		
		OPERATOR_SWITCHING	SWITCHING_AUTHORITY	INTERLOCKING_MODE
None	Viewing general information on the IED	■	■	■
View data	Viewing operational data on the IED	■	■	■
View CFG settings	Viewing configuration settings on the IED	■	■	■
Force values	• Changing values • Overwriting actual data • Triggering a process	■	■	■
Change authority	Switching the authority	–	■	–
Change interlock mode	Changing the interlock mode	–	–	■

3.2.7 User Names on the On-Site Devices

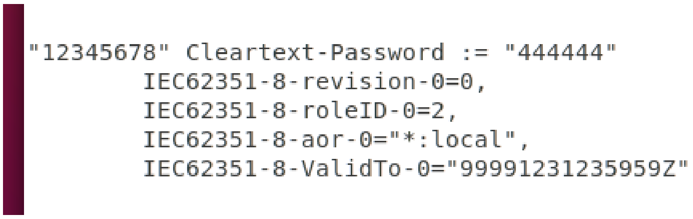
On the on-site devices, there are 2 kinds of user names:

- Default user names
  SIPROTEC 5 devices are delivered with the following predefined user names for exclusive login via the device operation panel. These user names are mapped to the roles that the SIPROTEC 5 devices support:
  - VIEWER
  - OPERATOR
  - ENGINEER
  - INSTALLER
  - SECADM
  - SECAUD
  - OPERATOR_SWITCHING
  - SWITCHING_AUTHORITY
  - INTERLOCKING_MODE
  - ADMIN
- User-defined user names
  The on-site device allows you to log on with individual numerical user names and numerical passwords that are centrally managed in the authentication server like other user accounts. Such user names are entered by selecting the **USER_ID** option on the login page of the on-site devices.
  When configuring such user names in the authentication server, consider the following conditions:
  - The user names and passwords are numerical only.
  - The length of the user names is between 1 digit and 8 digits.
  - The length of the passwords is between 1 digit and 16 digits.

NOTE

You can only use the user-defined user names on the device operation panel and cannot use them in DIGSI 5 or the browser-based user interface. For this restriction, set the **Area of Responsibility** (AoR) field as follows:

- For the default user names, you can set the AoR field to any value. The maximum length of the AoR field is 49 characters.
- For the user-defined user names, set the AoR field to ***:local** on the authentication server.



```
"12345678" Cleartext-Password := "444444"
        IEC62351-8-revision-0=0,
        IEC62351-8-roleID-0=2,
        IEC62351-8-aor-0="*:local",
        IEC62351-8-ValidTo-0="99991231235959Z"
```

[sc_user_cfg_RADIUS, 1, --_--]

Figure 3-14 User Configuration on the Authentication Server

3.2.8 Logging on to the Device via the Device Operation Panel

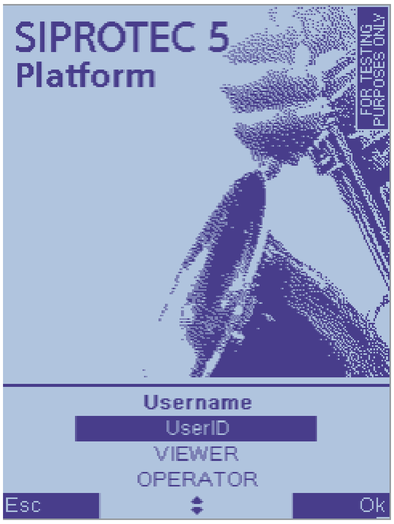
User authentication and authorization start with the SIPROTEC 5 device. In this case, the device is the authentication client and sends an access request to the authentication server.
This request contains the user credentials.

How to Log on to the Device

Proceed as follows:

✧ Press the softkey **Login** on the device.

A user-name selection appears in the lower area of the device display.



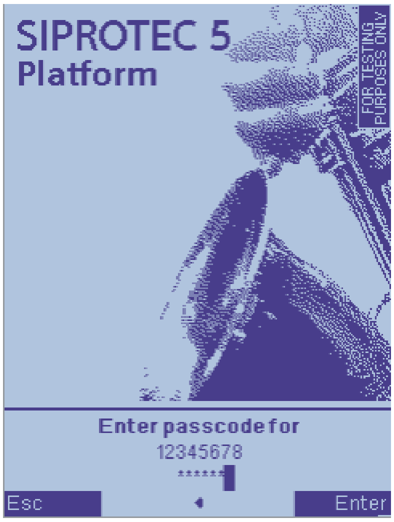
[sc_login, 2, en_US]

Figure 3-15 User-Name List

✧ Use the up and down navigation keys to select your intended user name or enter a user ID.

✧ Confirm the selection by pressing the softkey **OK**.

The prompt for entering the passcode appears.



Enter passcode for
12345678
******

[sc_enter_passcode, 2, en_US]

Figure 3-16 Passcode Entering Page

✧ Enter the numerical passcode.

✧ Complete the input with the softkey **Enter**.

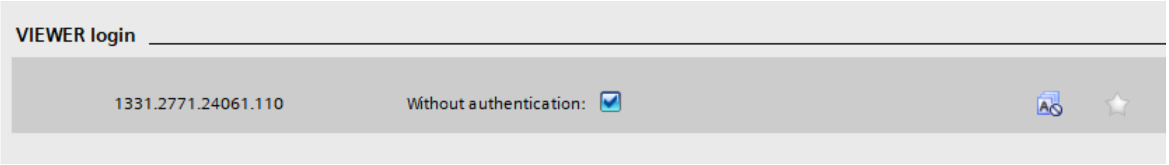
NOTE

If the message *Blocked by another client* is displayed, wait for 1 minute and log on again.

For more information on logging-on to the device via DIGSI 5, see also *DIGSI Online help*.

3.2.9 Login without Authentication

If you want to access a device with the user name VIEWER and without any credentials, select the parameter **Without authentication** in DIGSI 5.


VIEWER login

1331.2771.24061.110 Without authentication: ☑

[sc_no_authentication, 1, en_US]

Figure 3-17 Authentication Configuration for the User Name Viewer

The parameter is unchecked by default.

3.3 Role-Based Views in DIGSI 5

With this feature in DIGSI 5, the UI display adapts to the respective roles with which the user has logged in to the Windows session. When you launch DIGSI 5, your user name as per the Windows login session and your supported role(s) are displayed on the top right side of the DIGSI 5 UI. This feature is best suited for the user accounts that are centrally managed in a Microsoft Active Directory domain controller. A centrally managed user account can be added to one or more centrally defined user groups that translate to the roles that DIGSI 5 recognizes.

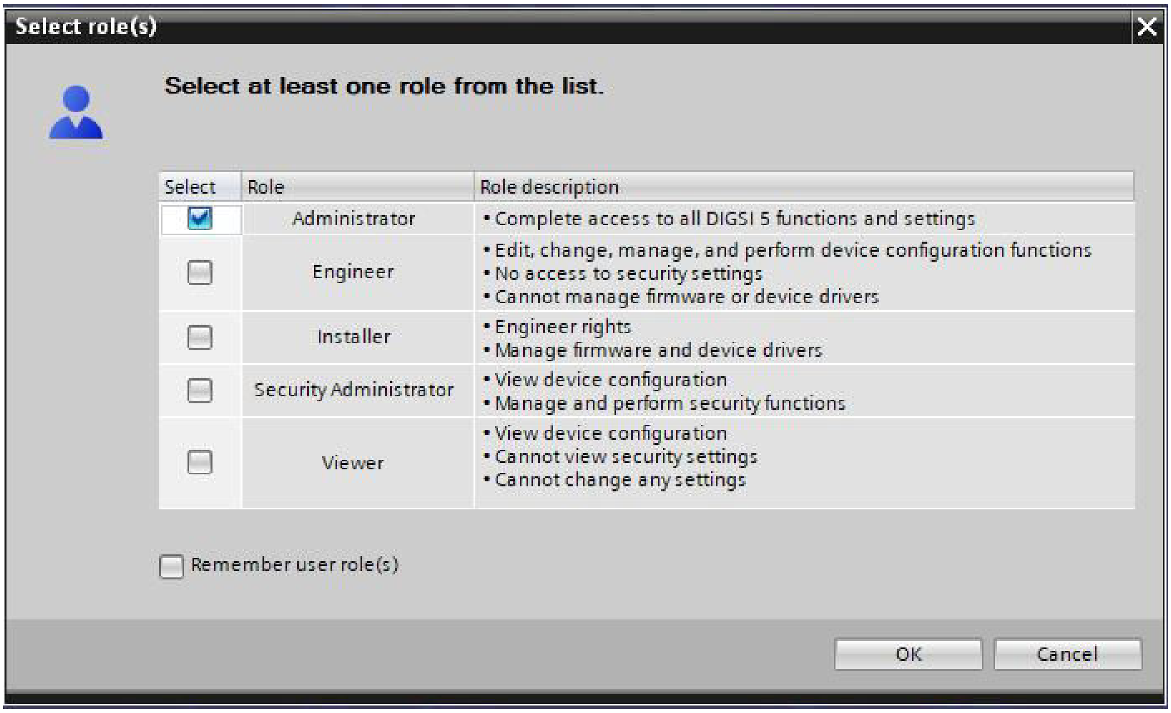
The roles are generally configured by the Security Administrator in the Active Directory (AD). The following group names must be used while configuring different roles in the Active Directory:

DIGSI	Active Directory (AD)
Administrator	SIEMENS ADMIN
Engineer	IEC ENGINEER
Security Administrator	IEC SECADM
Installer	IEC INSTALLER
Viewer	IEC VIEWER

If the Windows supported role (user groups in Active Directory) on your PC matches with the following list of roles predefined in DIGSI 5, then the respective role name is displayed along with the user name:

- Administrator:
  In this role, the user is able to view the DIGSI 5 UI in its entirety (which is the only UI option available in versions of DIGSI 5 prior to V7.90).
- Engineer:
  In this role, the user has access to all functions except for managing security, firmware and device drivers.
- Installer:
  In this role, the user has access to all functions except for managing security options.
- Security Administrator:
  In this role, the user can manage the security options but can only view the rest of the device settings.
- Viewer:
  In this role, the user can only view the device configuration but cannot edit them or access the security settings.

If the Windows supported role does not match any of the predefined roles supported by DIGSI 5, then the role name **Administrator** is displayed by default. If you still want to restrict your access to DIGSI 5 functionalities to prevent unintended changes to the project, you may do so by manually selecting a specific role for your current DIGSI 5 session. You can click the user name or the supported role to open the **Select role(s)** dialog and select the required role. The permissions associated with each role are mentioned in the **Select role(s)** dialog.



Select role(s)

Select at least one role from the list.

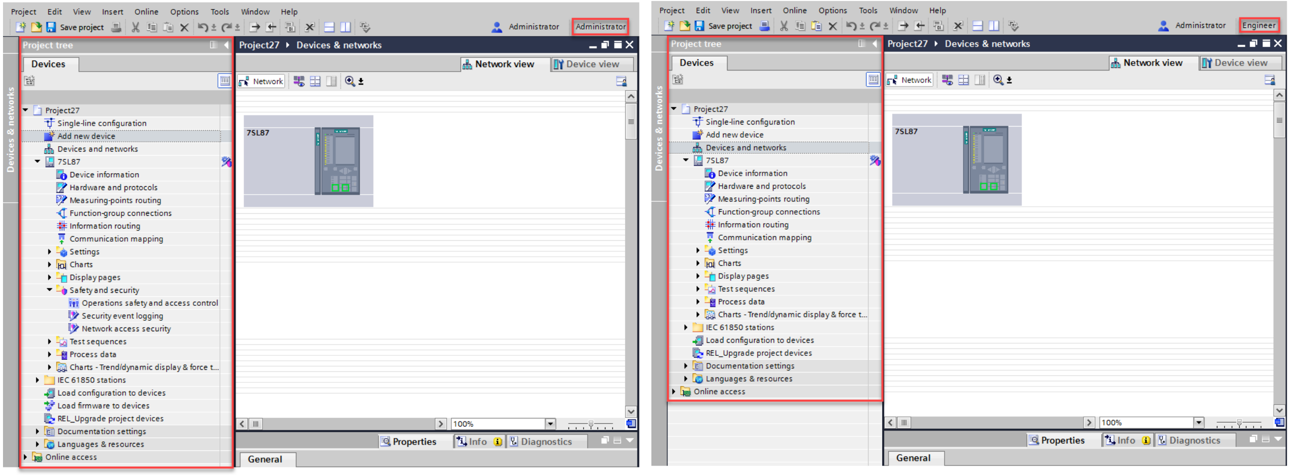
Select	Role	Role description
☑	Administrator	• Complete access to all DIGSI 5 functions and settings
□	Engineer	• Edit, change, manage, and perform device configuration functions • No access to security settings • Cannot manage firmware or device drivers
□	Installer	• Engineer rights • Manage firmware and device drivers
□	Security Administrator	• View device configuration • Manage and perform security functions
□	Viewer	• View device configuration • Cannot view security settings • Cannot change any settings

□ Remember user role(s)

[sc_digsi_user_roles, 2, en_US]

The selected roles are then enforced on the DIGSI 5 UI in the same way that the device enforces them on the HMI (read-only, read and write, hide).

The following figure shows the difference in UI display when a user logs in with different supported roles (**Administrator** and **Engineer**). The user logged in as **Engineer** does not have access to security settings and also cannot manage firmware or device drivers.



[sc_digsi_admin_engineer_view, 1, en_US]

Supported Roles and Rights

Action	ADMIN	ENGINEER	INSTALLER	VIEWER	SECADM
Import device driver	Y	N	Y	N	N
Uninstall device drivers	Y	N	Y	N	N
Print and print preview	Y	Y	Y	Y	N
Check consistency	Y	Y	Y	Y	N
Export	Y	Y	N	Y	Y

Action	ADMIN	ENGINEER	INSTALLER	VIEWER	SECADM
Import	Y	Y	N	N	N
Edit – Rename, cut, paste, delete	Y	Y	N	N	Y
Edit – copy	Y	Y	Y	Y	Y
Create/Delete project	Y	Y	N	N	Y
Archive project	Y	Y	Y	Y	Y
Save project	Y	Y	N	N	Y
Save project as	Y	Y	Y	Y	Y
Single-line Editor	W	W	R	R	N
Add new device	Y	Y	N	N	N
Device and networks Editor	W	W	R	R	N
Load configuration to devices	Y	Y	N	N	N
Load firmware to devices	Y	N	Y	N	N
IEC Station	Y	Y	N	N	N
Hardware and protocols Editor	W	W	R	R	R
Add new display page	Y	Y	N	N	N
Add new test sequence	Y	Y	N	N	N
Device information Editor	W	W	R	R	R
Measuring-points routing Editor	W	W	R	R	N
Function-group connections Editor	W	W	R	R	N
Information routing Editor	W	W	R	R	N
Communication mapping Editor	W	W	R	R	N
Settings Editor	W	W	R	R	N
Recorder interaction Editor	W	W	R	R	N
Fault-display configuration Editor	W	W	R	R	N
Circuit-breaker interaction Editor	W	W	R	R	N
Display pages Editor	W	W	R	R	N
Time settings Editor	W	W	R	R	R
Recorder signal ordering	W	W	R	R	N
Device settings Editor	W	W	R	R	R
Network access security	W	N	N	N	W
Security event logging Editor	W	N	N	N	W
Operations safety and access control	W	N	N	N	W
Assignment and removing assignment of device	Y	Y	N	N	N
Online Load firmware and load configuration	Y	Y	N	N	N
Factory reset, Secure credential reset and load SCF to device	W	N	N	N	Y
Download SCRF, SFRF and remove saved credentials	Y	Y	N	N	Y
Get process data	Y	Y	N	N	N
Protection functions	Y	N	N	N	N
Process data access	W	R	R	R	N
Online – SLE	W	W	R	R	N
Online – Device information Editor					
Online – Device information Editor: Device information	W	W	R	R	R

Action	ADMIN	ENGINEER	INSTALLER	VIEWER	SECADM
Online – Device information Editor: Resource consumption	R	R	R	R	R
Logs Tab					
Online – Device information Editor: Device-diagnosis log	W	W	R	R	R
Online – Device information Editor: Security log	R	N	N	N	R
Online – Device information Editor: Diagnostic information	R	R	R	R	R

Legend	
Y	Yes
N	No
W	Write access
R	Read-only

Switching the Supported Roles between the Offline and Online Configuration

- Regardless of what roles are applied for/by the user while working with DIGSI 5 offline, once the user successfully logs on to an RBAC-enabled device, DIGSI 5 reconfigures its UI if necessary to match the role(s) as determined by the device for the logged-on user. After a connection is established with any RBAC-enabled device, the project tree and menus/toolbar buttons state is updated based on the online supported role(s) and all the opened Editors are closed. Further, the online supported role is displayed on the top right side of the DIGSI UI.
- When the user deletes the saved online credentials in DIGSI 5 or when the online session times out, the online roles of the user are retained.

3.4 Emergency Access

Usernames for Emergency Access

Emergency access is provided if access to the device is needed but the connection to the RBAC server is lost. You can log on with the following usernames for this purpose:

Username	Role[11]	Connection Mode	Restriction
EMERGENCYUSER_DIGSI	ADMIN	Remote	These usernames are specific for emergency access. Do not use them in the authentication servers.
EMERGENCYUSER	ADMIN	Local	
REMOTEEMERGENCY-VIEWER	VIEWER	Remote	
EMERGENCYVIEWER	VIEWER	Local	

Emergency access is not enabled by default. Configurations of the emergency access require the security-administrator role. Siemens recommends configuring the emergency access via DIGSI 5 during the device commissioning or during the configuration of the cybersecurity parameters.

NOTE

For devices in version 8.83 and higher, it is necessary to take the latest DIGSI 5 for the configuration of emergency access.

Activation of the Emergency Account

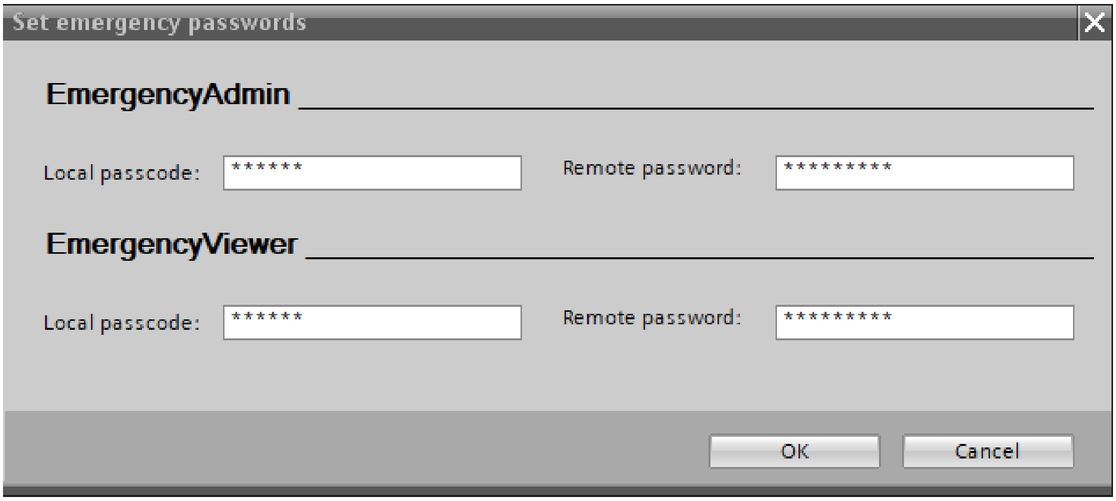
- Start DIGSI 5.
- Open the project in DIGSI 5.
- Switch to the **Safety and security** menu item in the project tree.
- Double-click the **Operations safety and access control** menu item.
- Under **Emergency Account Settings**, click **Configure**.

With the refresh button 🔄, you can check the status of the emergency account in the device:

Status	Description
Yes	The emergency account is configured.
No	The emergency account is not configured.
Unknown	The emergency account is not configured or DIGSI 5 fails to read the latest status of the emergency account from the device.

[11] For more information about the roles, refer to *3.2.6 Basic Properties of the Assignment of Rights and Supported Roles*.

- Enter the HMI passcodes and the remote passwords.



Set emergency passwords

EmergencyAdmin

Local passcode: ******

Remote password: *********

EmergencyViewer

Local passcode: ******

Remote password: *********

[sc_set_emergency_password, 4, en_US]

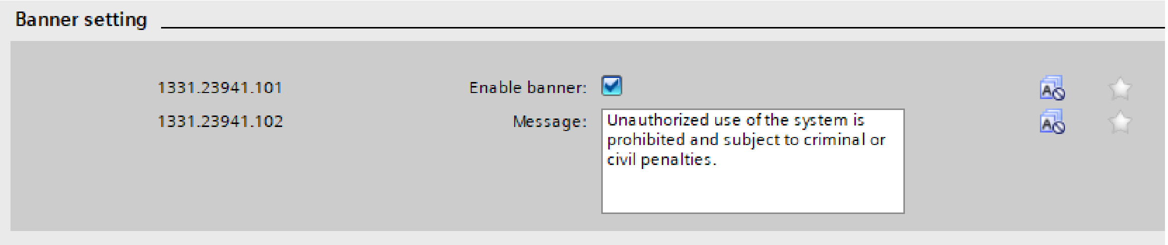
Figure 3-18 Dialog for Entering the Emergency Passwords

Type	Length	Restriction
HMI passcode	6 to 16 numbers	Can only be entered via the device operation panel
Remote password	8 to 16 characters	Can be entered via DIGSI 5 and the browser-based user interface The passwords must consist of upper-case letters, lower-case letters, numbers, and special characters.

- Confirm the input with **OK**.

3.5 Banner Setting

For security reasons, you can enable the **Banner setting** feature and enter a message via **Project** > **Target device** > **Safety and security** > **Operations safety and access control** in DIGSI 5 in the role of a SECADM or ADMIN. Then, when you are trying to log on to the device via DIGSI 5 or via the device operation panel, you can see that a banner message pops up.



Banner setting

1331.23941.101 Enable banner: ☑

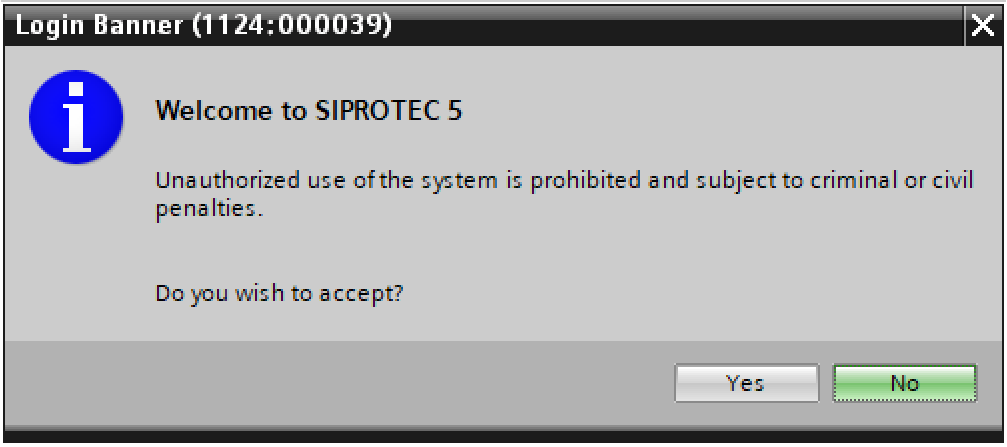
1331.23941.102 Message: Unauthorized use of the system is prohibited and subject to criminal or civil penalties.

[sc_banner setting, 1, en_US]

Figure 3-19 Configuration of Banner Setting

The maximum message length is 128 characters. If you enable the **Banner setting** feature, the message cannot be empty. You can define the content yourself, for example:

- System usage may be monitored, recorded, and subject to audit.
- Unauthorized use of the system is prohibited and subject to criminal or civil penalties.
- Use of the system indicates consent to monitoring and recording.



Login Banner (1124:000039)

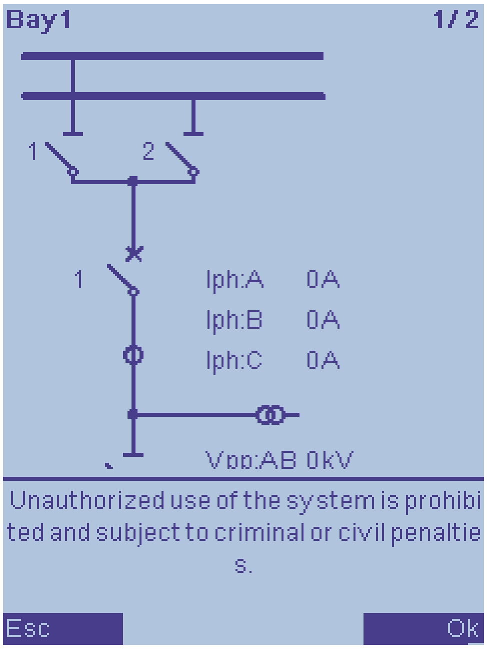
Welcome to SIPROTEC 5

Unauthorized use of the system is prohibited and subject to criminal or civil penalties.

Do you wish to accept?

[sc_banner-pop, 2, en_US]

Figure 3-20 Banner Message in DIGSI 5



Iph:A 0A
Iph:B 0A
Iph:C 0A
Vpp:AB 0kV

Unauthorized use of the system is prohibited and subject to criminal or civil penalties.

[sc_Banner HMI, 1, --_--]

Figure 3-21 Banner Message on the Device Display

If you click **Yes** in DIGSI 5 or press the softkey **Ok** on the device operation panel, the login process continues. Otherwise, the login process is denied.

4 Malware Protection

4.1 Overview

The SIPROTEC 5 devices are based on the VxWorks operating system for which no special antivirus program is known to be available. Furthermore, the SIPROTEC 5 devices are equipped with an internal firewall for protection from attacks over the network. In order to enhance the standard level of protection, the firewall is enabled by default.

You can only load digitally signed firmware files into the devices and protect the devices from executing manipulated or corrupted firmware files. The device only accepts signed firmware files and signed hardware configurations. The signing is applied securely at the Siemens production facilities with the Siemens-internal public-key infrastructure for products.

In addition, viruses are usually transmitted by E-mail, while surfing on the Internet, or through usage of infected removable storage media. SIPROTEC 5 devices are not susceptible to these infection paths.

The authentication between DIGSI 5 and the device using digital certificates prevents applications other than DIGSI 5 from being able to access or modify the device configuration. You can find more information about how to issue your own certificates to authorize the DIGSI 5 installations and interact with your SIPROTEC 5 devices in chapter *6.5 DIGSI 5 Client Authentication*.

4.2 Malware Protection for Engineering Software

The PC-based engineering software application for SIPROTEC relays – DIGSI 5, is installed using a signed installer to protect its integrity. Siemens regularly tests and reports the compatibility of new antivirus patterns with the latest DIGSI versions. These reports, which also include the results of the Microsoft Windows patch-compatibility verification, are available in the Internet on a monthly basis. Furthermore, every release of DIGSI 5 is tested against a multitude of antivirus scanners before delivery.

DIGSI software is also tested for compatibility with whitelisting application solutions, wherein only approved software is allowed to be executed; malware that might have infected the system after activation of the whitelisting protection are prevented from executing. The advantage of the whitelisting application for protected and isolated substation networks is that it alleviates the pressure to immediately update antivirus patterns for newly discovered malware.

These steps help to ensure secured and reliable operations of SIPROTEC 5 devices and DIGSI 5 in the target environment.

4.3 Integrity Verification of the Downloaded File

You can also verify the integrity of all SIPROTEC firmware and software files which are available for download on the Siemens-supported portal. For each downloadable firmware and software file, the corresponding SHA-256 fingerprint is published in the Internet[12].

Tools such as Certutil in Microsoft Windows can be used for the following purposes:

- Generate the SHA-256 fingerprint for the file you download.
- Check if the SHA-256 fingerprint is identical to the published fingerprint, that is verifying the file integrity.

[12] *http://www.siemens.com/gridsecurity* -> **Product security** -> **Downloads** -> **Software**

5 Protection against DoS Attacks

5.1 Traffic Limiter

The traffic limiter works on the IP-connection level. Currently, only IP-based TCP, UDP and ICMP connections are supported.

The traffic limiter checks the connections over a 1-second interval.

If the connections have the same IP address, port, and protocol type, and the number of the specific connections exceeds the maximum threshold value (see *Table 5-1*), these connections are dropped. If the number of the specific connections falls below the minimum threshold value, the device accepts these connections again.

If the number of all connections exceeds the total-amount threshold value, the device drops all connections.

Table 5-1 Threshold Values

CPU/Module Type	Min. Threshold Value[13]	Max. Threshold Value[13]	Sum Threshold Value
CP100 (Port J)	2400	4000	8000
CP300 (Port J)	2400	4000	8000
ETH-BB-2FO ETH-BD-2FO	2400	4000	8000
ETH-BA-2EL	300	500	1000

NOTE

Currently, a SIPROTEC 5 device can track 32 connections concurrently.

[13] The unit is frames per second

5.2 Overload Protection

The layer **Overload protection** works on the Ethernet driver level.

This layer counts the incoming Ethernet frames. If the number of frames exceeds the threshold (see *Table 5-2*), the layer stops processing the frames to the next layer of the stack.

This measure is used to ensure the device functionality and to prevent the network stack from disturbing the real-time protection functions by taking up too many CPU cycles.

In different CPUs (Port J) and communication modules, the layer **Overload protection** performs differently.

- CP150 (Port J), CP300 (Port J), ETH-YA-2EL, and ETH-YC-2FO

  The layer **Overload protection** checks the limit in a millisecond interval to ensure a minimum response-time for a potential overload. If the number of frames in a millisecond is larger than the threshold value, the whole device which is underload stops processing immediately.

  A leaky-bucket model is used to average the frames over a 250-ms interval.

- CP100 (Port J), ETH-BB-2FO, ETH-BD-2FO, and ETH-BA-2EL

  When a frame is coming in, the layer checks the limit based on the time between 2 interrupts caused by the network hardware.

Table 5-2 Threshold Values

CPU/Module Type	Threshold Value[14]
CP100 (Port J)	11000
CP150 (Port J) CP300 (Port J) ETH-YA-2EL ETH-YC-2FO	5632
ETH-BB-2FO ETH-BD-2FO	8000
ETH-BA-2EL	2500

[14] The unit is frames per second.

6 Communication Security

6.1 Applying Ethernet Access Restrictions

Via the security settings, you can restrict the access rights of a DIGSI 5 connection for each Ethernet interface, like port J, USB port, and Ethernet communication modules.

NOTE

- If the device has an Ethernet communication module, you can also use Port E, Port F, Port N, or Port P.
- No matter whether the USB-port access is restricted or not, there is no impact on secure resetting of device configuration service.

You can set the security settings in DIGSI 5 in the Project tree under **Safety and security** > **Network access security**.

You can set the following access rights:

- No access
  No DIGSI communication is possible via this interface.
- Read-only access
  You only have read access to the device via this interface.
- Read and write access
  Read and write access to the device is possible via this interface.

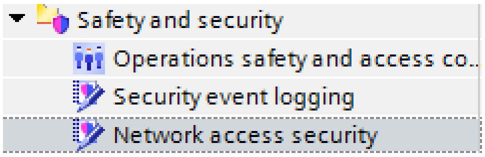
6.2 Configurations of IEC 61850 Secure MMS

Secure communication is a key requirement for substations according to IEC 62351. There are 2 main profiles for secure MMS, direct TLS connections, and end-to-end encryption. In the profiles, the encryption is part of the MMS connection layers.

SIPROTEC 5 devices support direct TLS connections.

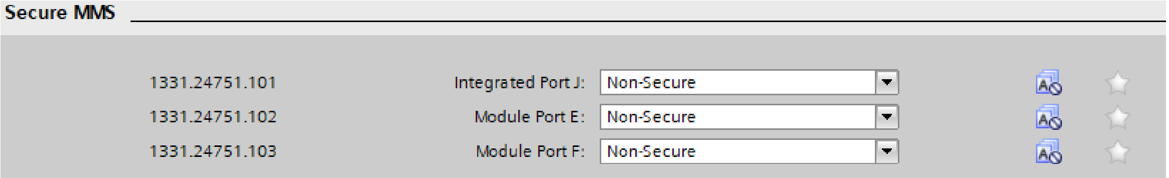
To configure direct TLS connections, proceed as follows:

- ✧ In the **Hardware and protocols** dialog, enable and configure IEC 61850.
- ✧ In the project tree, navigate to **Safety and security** > **Network access security**.



[sc_network_access_security, 1, en_US]

Each enabled IEC 61850 interface is listed with the default value ***Non-Secure***. The default setting is the default compatibility mode using TCP communication via the unsecure port 102.

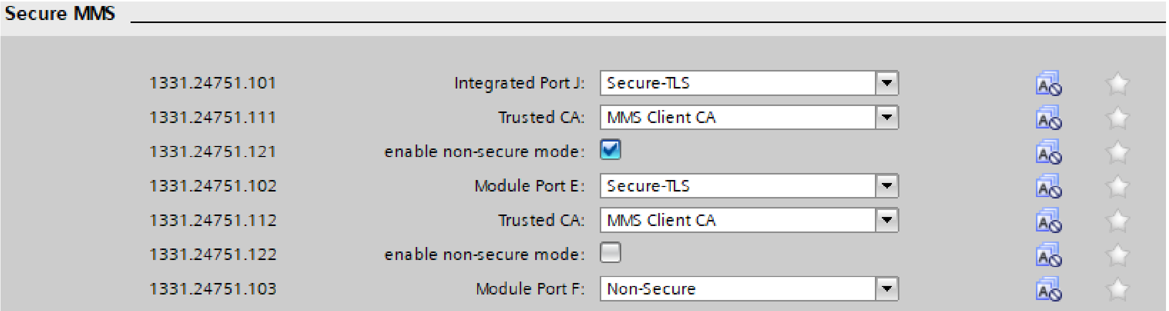


Secure MMS

1331.24751.101	Integrated Port J:	Non-Secure
1331.24751.102	Module Port E:	Non-Secure
1331.24751.103	Module Port F:	Non-Secure

[sc_Secure_MMS, 1, en_US]

- ✧ To enable the secure mode using secure TLS communication via port 3782, set the interface to ***Secure-TLS***.



Secure MMS

1331.24751.101	Integrated Port J:	Secure-TLS
1331.24751.111	Trusted CA:	MMS Client CA
1331.24751.121	enable non-secure mode:	☑
1331.24751.102	Module Port E:	Secure-TLS
1331.24751.112	Trusted CA:	MMS Client CA
1331.24751.122	enable non-secure mode:	☐
1331.24751.103	Module Port F:	Non-Secure

[sc_Secure_MMS_settings, 1, en_US]

- ✧ From the list box **Trusted CA**, select the trusted CA that the client uses for the incoming TLS connection.

  The list box shows the CAs that you add in the **DIGSI 5 CA store** via **Tools** > **Manage certificate authorities (CA)**.
- ✧ Set check box of **`enable non-secure mode`**.

  This check box enables unsecure communication via port 102 in parallel to the configured secure communication via port 3782.

After completing the security settings, to ensure that the mutual authentication of the underlying TLS channel can be configured and established properly, proceed as follows:

- ✧ Download the CSR file from the Web UI. For more information, refer to *7.2.3 Requested Certificates*.
- ✧ Sign the downloaded CSR file with the trusted CA.
- ✧ Upload the signed CSR file back to the device.

You can also use the EST to automatically get the MMS server certificates signed by the CA without downloading the CSR file and manually signing it. For more information on EST, refer to *7.3 Automatic Enrollment over Secure Transport*.

6.3 Security of Web Browser Interactions with Device

Apart from the use of the engineering tool DIGSI 5 for configuration and maintenance, SIPROTEC 5 devices provide a Web front end that can be used with a standard Web browser, as described in chapter **Operation Using a Browser-Based User Interface** of the *SIPROTEC 5 Operating Manual*.

NOTE

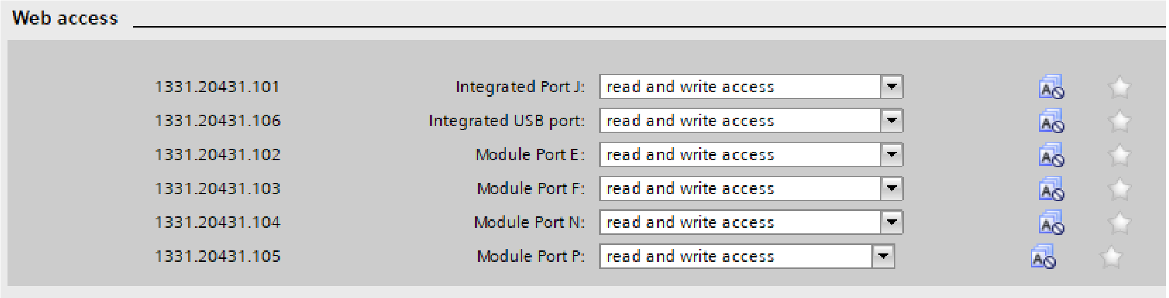
You can operate the SIPROTEC 5 device via DIGSI 5 and via the **browser-based user interface** in parallel.

Before operating the device via a Web browser, you first have to check the security settings. For more information refer to *6.1 Applying Ethernet Access Restrictions*.

To operate the device via the **browser-based user interface**, proceed as follows:

- Connect the SIPROTEC 5 device (for example Port J) to your PC using a network cable.

In order to improve the security of the connection, define the following access settings under **Network access security** in DIGSI:



Web access

1331.20431.101	Integrated Port J:	read and write access
1331.20431.106	Integrated USB port:	read and write access
1331.20431.102	Module Port E:	read and write access
1331.20431.103	Module Port F:	read and write access
1331.20431.104	Module Port N:	read and write access
1331.20431.105	Module Port P:	read and write access

[sc_web_access, 1, en_US]

Figure 6-1 Security Settings in DIGSI

NOTE

Note the IP address and the port number of the interface used for communication with the PC and the **browser-based user interface**. Make sure that the 12-digit IP address for the Web browser has been correctly set using the format ***.***.***.*** via DIGSI.

- Launch the Web browser on your PC.
- Enter the IP address of the device in the address line of the Web browser, followed by the port number 4443, for example https://172.16.60.60:4443, and confirm the entry using the ENTER key.

NOTE

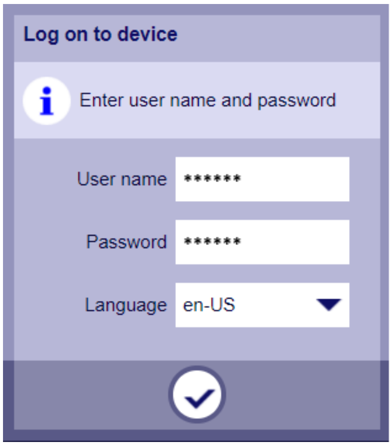
Some Web browsers may have problems connecting to the specified IP address of the device; in this case, delete the associated certificate in the Web browser.

The following login dialogs are available, depending on the security configuration of the SIPROTEC 5 device:

- Variant 1:
  If you have entered a connection password in DIGSI 5 under **Operations safety and access control**, the login dialog starts with the user name **Siprotec 5**. This user name cannot be changed. You must use the connection password configured in DIGSI.
- Variant 2:
  If you have configured the role-based access control (RBAC) in DIGSI 5 under **Operations safety and access control**, the login dialog starts with the request of the user name and password that you have configured on the authentication server.

- Variant 3:
  If you have not configured the role-based access control (RBAC) or the connection password, the login dialog starts with the user name **Siprotec 5**. This user name cannot be changed. The entry field for the password must be left empty.

Once the Web browser is successfully connected to the device, the following login dialog (for Variant 2) appears, for example:



Log on to device

Enter user name and password

User name ******

Password ******

Language en-US

[sc_web_monitor, 1, en_US]

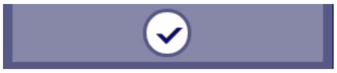
Figure 6-2 Login Dialog for the Browser-Based User Interface

- Enter the user name in the text box **User name**.
- Click in the text box **Password** and enter the password.
- Select a language.
  The language selection depends on the language set for the user interface of the device.

NOTE

If RBAC is active, access is possible only after a successful user name and password authentication check. For more information refer to *3.2 Role-Based Access Control (RBAC) in SIPROTEC 5*.

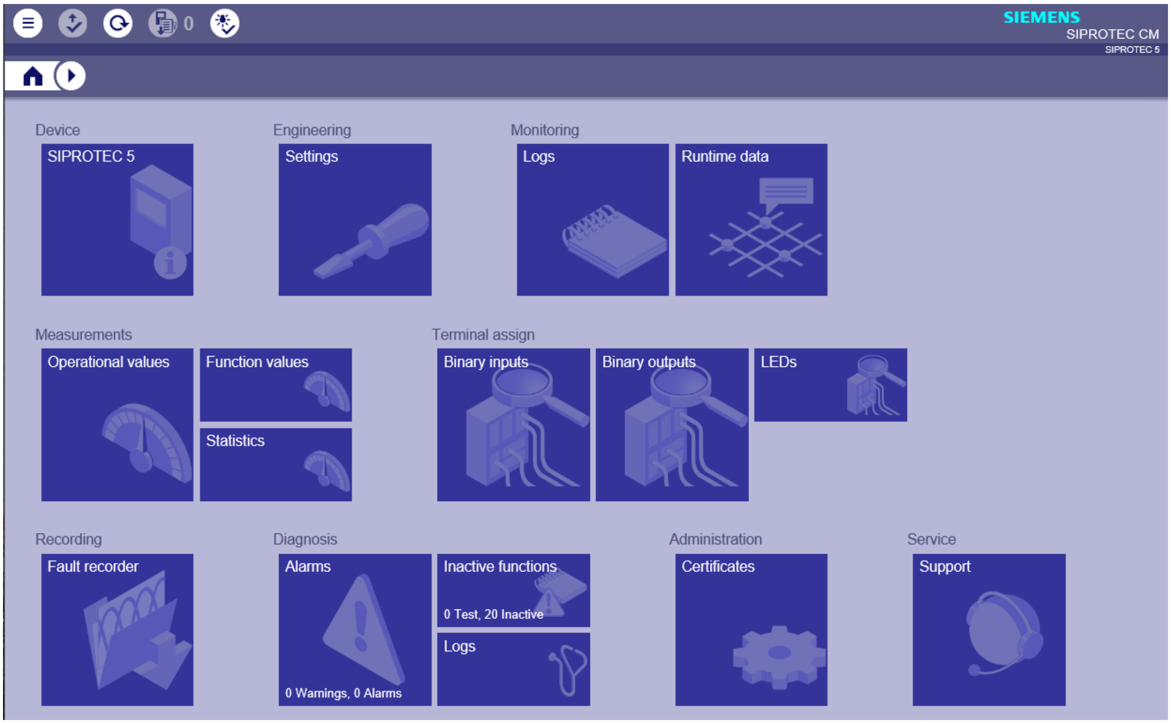
- Click the button with the checkmark.



[scwebmonitor_enter, 1, --_--]

Figure 6-3 Confirmation Button

After a successful login, the following buttons are available:



[sc_web_UI, 1, en_US]

Figure 6-4 Buttons for the Browser-Based User Interface

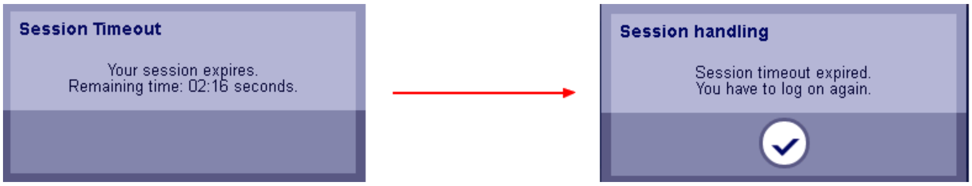
You can view the corresponding sections, or you can edit them by clicking the individual buttons.

Time-Out

NOTE

If you do not perform any action on the **browser-based user interface** within a defined time range, the Web browser disconnects from the device.

The following messages appear:



Session Timeout

Your session expires.
Remaining time: 02:16 seconds.

Session handling

Session timeout expired.
You have to log on again.

[sc_web_monitor_session_timeout, 1, en_US]

Figure 6-5 Time-Out

After a certain time has elapsed, you must log on to the device again using the Web browser.

6.4 DIGSI 5 Server Authentication

6.4.1 General Information

With the feature **DIGSI Server authentication**, you can use your own server certificates in a SIPROTEC 5 device for the secure communication between DIGSI 5 and the SIPROTEC 5 device.

When DIGSI 5 establishes a connection to the SIPROTEC 5 device, the device presents its server digital certificate to DIGSI 5 for authentication purposes. DIGSI 5 validates the signature and issued-by information of the server certificate with a customer CA which is listed in the tab **DIGSI 5 CA Cert store** or **Windows System CA Store**.

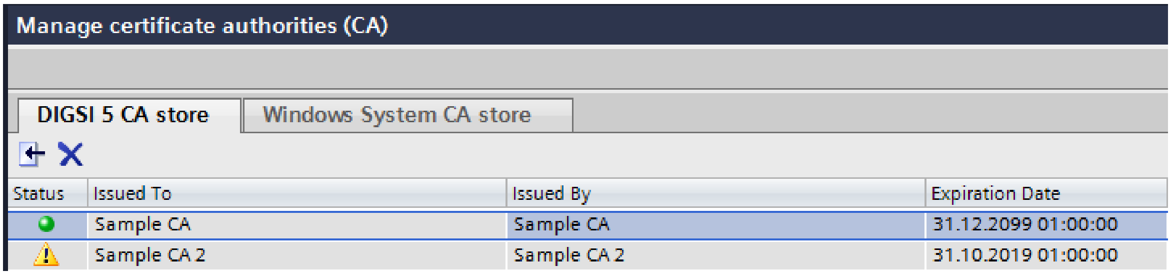
If you want your SIPROTEC 5 device to use your own server certificates instead of Siemens default certificates, then you need a Public Key Infrastructure (PKI) with an operational CA you can use to issue or digitally sign such client certificates. For more information on how to set up a PKI for your operational needs, refer to the *SICAM GridPass Manual* (*www.siemens.com/sicam-gridpass*).

6.4.2 Configurations in the DIGSI 5 CA Store

To use your own server certificates, you must first make DIGSI 5 aware of the corresponding issuing CA certificate.

To perform this step, you must add your issuing CA to the **DIGSI 5 CA store**. The **DIGSI 5 CA store** manages a list of CAs that can be used to validate the certificate chain corresponding to the device certificate.

You can access the **DIGSI 5 CA store** via the menu **Tools** > **Manage certificate authorities (CA)**:



Status	Issued To	Issued By	Expiration Date
●	Sample CA	Sample CA	31.12.2099 01:00:00
⚠	Sample CA 2	Sample CA 2	31.10.2019 01:00:00

[sc_manage_CA, 1, en_US]

There are 2 ways to add an existing CA to the **DIGSI 5 CA store**:

- Import the CA from the tab **Windows system CA store**
- Import the CA from a file

Import a CA from the Windows System CA Store

✧ If you have already installed your issuing CA in the operating system, you can import it from **Windows System CA store** in DIGSI 5. Open the tab **Windows System CA store** and select the CA you want to add to the **DIGSI 5 CA store**.

✧ Click the button ←.

Import a CA from a File

You can also import your issuing CA certificate from a file:

✧ Open the tab **DIGSI 5 CA store** and click the button ←.

A file browser is displayed.

✧ Select the CA file you want to import and confirm in order to import the CA file to the **DIGSI 5 CA store**.

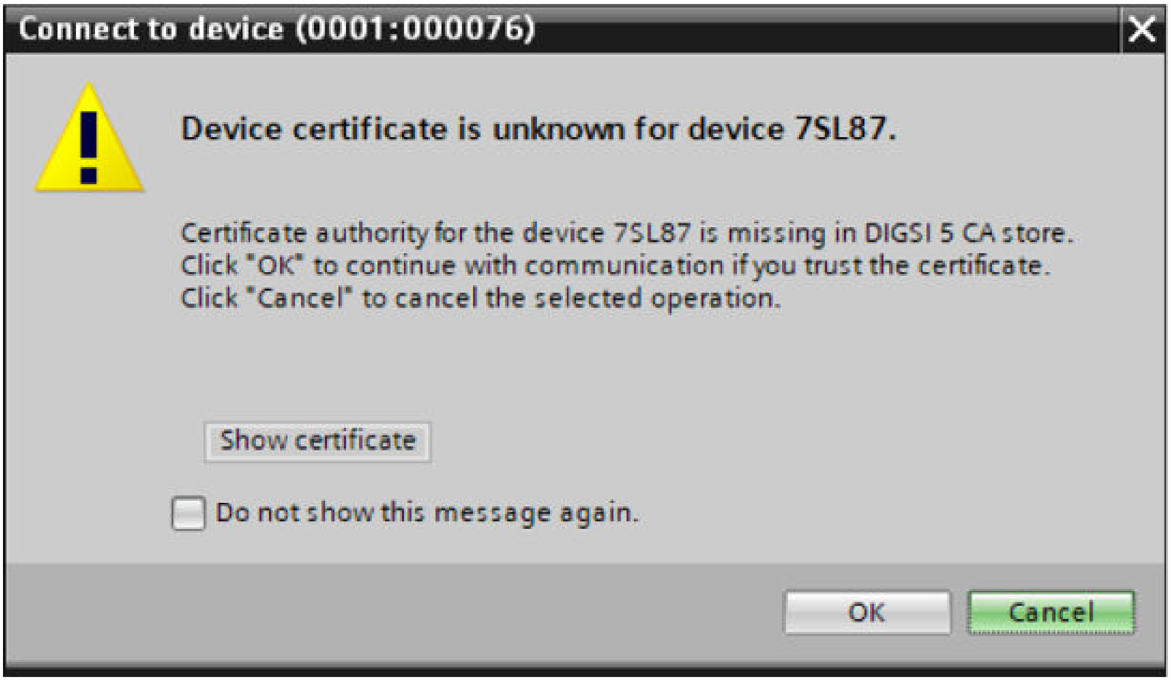
In either case, if the operation is successful, the imported CA is displayed in the list **DIGSI 5 CA store** with a status icon indicating the expiration state of the selected CA certificate:

Icon	Explanation
🟢	The expiration date of the CA lies more than 180 days in the future.
⚠	The CA expires within the next 180 days.
🔴	The CA has already expired and thus is not valid anymore.

NOTE

Currently, there is a limitation of 8 CAs that can be managed within the **DIGSI 5 CA store**. Before adding more CAs, remove unused CAs manually.

After the CA is imported, DIGSI 5 validates the server certificate when connecting to the device. If the authentication fails, DIGSI 5 shows the following message:



Connect to device (0001:000076)

Device certificate is unknown for device 7SL87.

Certificate authority for the device 7SL87 is missing in DIGSI 5 CA store.
Click "OK" to continue with communication if you trust the certificate.
Click "Cancel" to cancel the selected operation.

□ Do not show this message again.

[sc_DIGSI_auth_failure, 1, en_US]

Figure 6-6 Example of a DIGSI Authentication Failure

Delete a CA from the DIGSI 5 CA Store

✧ To remove a CA from the **DIGSI 5 CA store**, select the CA in the list and click the button ✕.

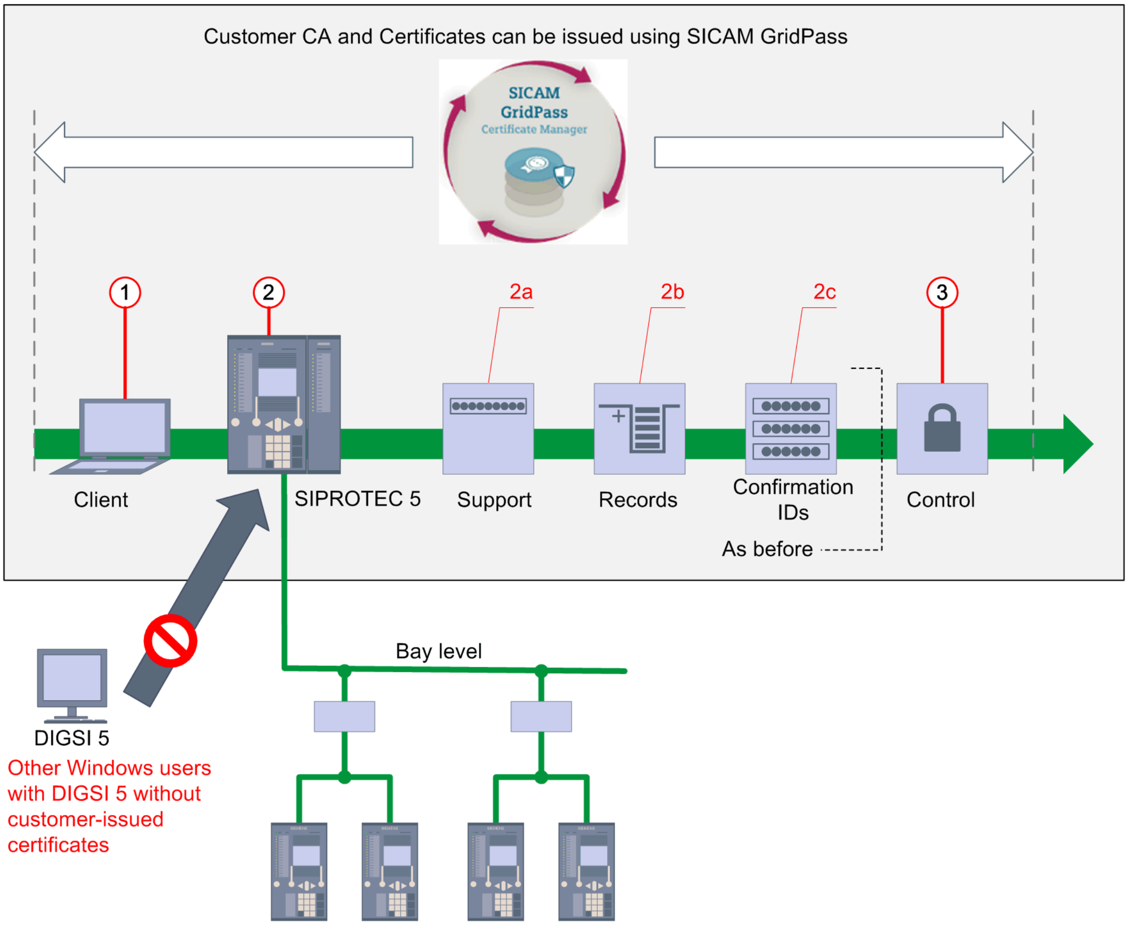
If the CA is already referenced within one or multiple devices in the open project, a warning appears when you try to remove it.

6.5 DIGSI 5 Client Authentication

6.5.1 General Information

With the new feature **DIGSI Client authentication**, you can use your own digital certificates in the DIGSI 5 program for the secure communication between DIGSI 5 and the SIPROTEC 5 device.

Once this feature is configured, a connection to a device using a standard DIGSI 5 version with the embedded default Siemens client certificate is not possible anymore. This prevents unauthorized Windows users with DIGSI 5 installations from accessing operational SIPROTEC 5 devices.


Customer CA and Certificates can be issued using SICAM GridPass
SICAM
GridPass
Certificate Manager
1
2
2a
2b
2c
3
Client
SIPROTEC 5
Support
Records
Confirmation IDs
Control
As before
Bay level
DIGSI 5
Other Windows users with DIGSI 5 without customer-issued certificates

[dw_schematic-representation_this_security-feature, 1, en_US]

Figure 6-7 Schematic Representation of the Security Feature

1 Installation of customer-issued client certificate in the Windows user account (client authorization)

2 Installation of the customer CA used to sign the DIGSI 5 client certificates in the device

New: Only DIGSI 5 installations that connect using certificates signed by customer CA are permitted

2a Device-side support for role-based access control including central user management and emergency access (works as before)

2b Recording of security-relevant events and alarms via Syslog and recording in non-volatile security logs in the device (works as before)

2c Confirmation IDs for safety-critical operations (works as before)

3 Mutually authenticated and encrypted communication between DIGSI 5 and the SIPROTEC 5 device

While establishing the connection with a SIPROTEC 5 device, DIGSI 5 presents its client digital certificate to the device for authentication purposes. If you want your DIGSI 5 installation to use your own client certificates instead of Siemens default certificates, then you need a PKI with an operational CA that you can use to issue or digitally sign such client certificates. For more information on how to setup a PKI for your operational needs, refer to the SICAM GridPass Manual (*www.siemens.com/sicam-gridpass*).

To use this DIGSI client authentication feature, you must first configure the Windows user accounts that are authorized to use DIGSI 5, and the SIPROTEC 5 devices accordingly.

To configure the new feature **DIGSI Client authentication**, proceed as follows:

- Setup a DIGSI 5 CA store.
- Configure the DIGSI 5 Client authentication security feature.
- Verify the configured CA via a Web browser.

You can find more information on these steps in the following chapters.

6.5.2 Configuration

6.5.2.1 Setup the DIGSI 5 CA Store

To use your own client certificates, you must first make DIGSI 5 aware of the corresponding issuing CA certificate.

6.5.2.2 Configuration of the DIGSI 5 Client Authentication Security Feature

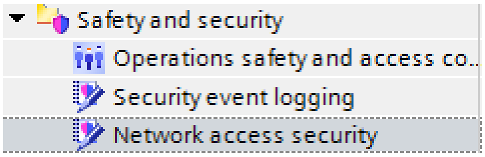
NOTE

If you have opened a project with a CA that is currently not part of this CA store, a configured CA will automatically be added to the DIGSI CA store. The same applies to online connections to an existing device.

You must configure your devices to only accept DIGSI 5 connection requests with your client certificates.

To configure the **DIGSI client authentication for a device**, proceed as follows:

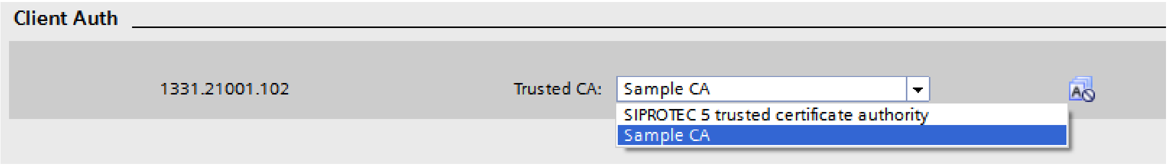
✧ In the project tree, select the respective device, navigate to **Safety and security** and select **Network access security**:



- Safety and security
  - Operations safety and access co..
  - Security event logging
  - Network access security

[sc_network_access_security, 1, en_US]

The following information is displayed:



Client Auth

1331.21001.102 Trusted CA: Sample CA

SIPROTEC 5 trusted certificate authority
Sample CA

[sc_client_authentication, 1, en_US]

✧ From the list box **Trusted CA**, select the CA that you use to issue your DIGSI 5 client certificates.

The list box shows the CAs that are currently imported in the **DIGSI 5 CA store** (see chapter *6.5.2.1 Setup the DIGSI 5 CA Store*). The default value of this list box is **SIPROTEC 5 trusted certificate authority**. If you have selected this value, the default behavior for the connection from DIGSI 5 to the SIPROTEC 5 device with Siemens issued DIGSI 5 client certificates is activated.

Load these settings to the device for them to take effect.

NOTE

To verify the configured CA via the user interface, navigate to **Settings** > **Security** > **Client Auth** > **TrustedCA**.

✧ To establish a communication with the device, a client certificate issued by the selected CA must be installed on the DIGSI PC.

If there are several client certificates to select from, you are asked to select one. If there is no client certificate installed on the DIGSI 5 PC, a respective error message is shown. You can reset the device configurations via the USB port and start the operations again.

Additional Operations for Products in Old Firmware Versions

To increase the security of TLS connections, from firmware version 7.30, Siemens introduces TLS 1.2 in SIPROTEC 5 products and disallows connections that are based on TLS 1.0. To avoid potential protocol-downgrade-attacks and other TLS 1.0 vulnerabilities, Microsoft also disables TLS 1.0 by default in major Windows operating systems.

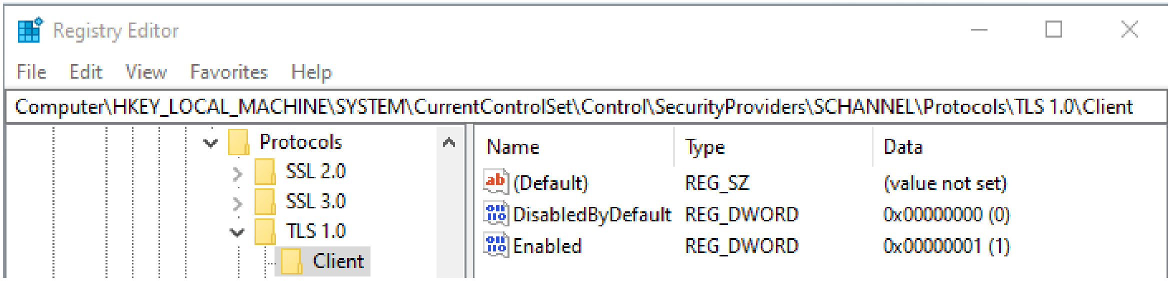
So, if the firmware versions of your SIPROTEC 5 devices are lower than V7.30, to establish connections between the devices and DIGSI 5, enable TLS 1.0 in your operating system first.

For example, for the Windows 10 Enterprise edition, you can turn on TLS 1.0 in **Registry Editor** with the following steps:

✧ Open regedit.exe and navigate to the key location **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols**.

✧ Under the key **TLS 1.0**, select the subkey **Client**.

If there is no such key and subkey, create them.



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client

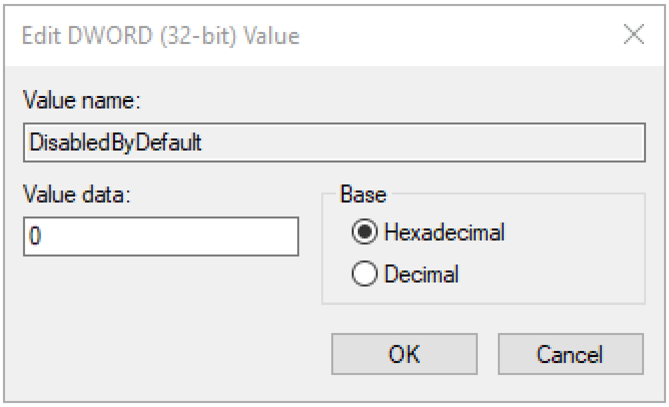
Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_DWORD	0x00000000 (0)
Enabled	REG_DWORD	0x00000001 (1)

[sc_Registry_Editor_EN, 1, en_US]

Figure 6-8 Key and Subkey for TLS 1.0

✧ Set **`DisabledByDefault`** to ***0*** and **`Enabled`** to ***1***.

For the data type DWORD, value ***0*** means off while ***1*** means on.



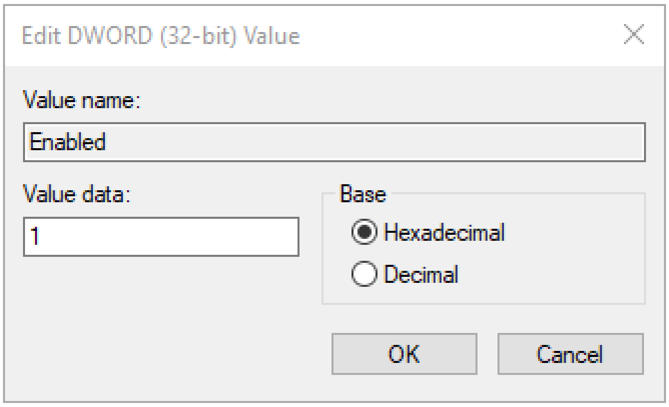
Value name: DisabledByDefault

Value data: 0

Base
● Hexadecimal
○ Decimal

[sc_DWORD_Disable, 1, en_US]

Figure 6-9 Value Data for TLS 1.0 – 1



Edit DWORD (32-bit) Value

Value name: Enabled

Value data: 1

Base

● Hexadecimal

○ Decimal

[sc_DWORD_Enable, 1, en_US]

Figure 6-10 Value Data for TLS 1.0 – 2

✧ Restart the computer to apply the changes.

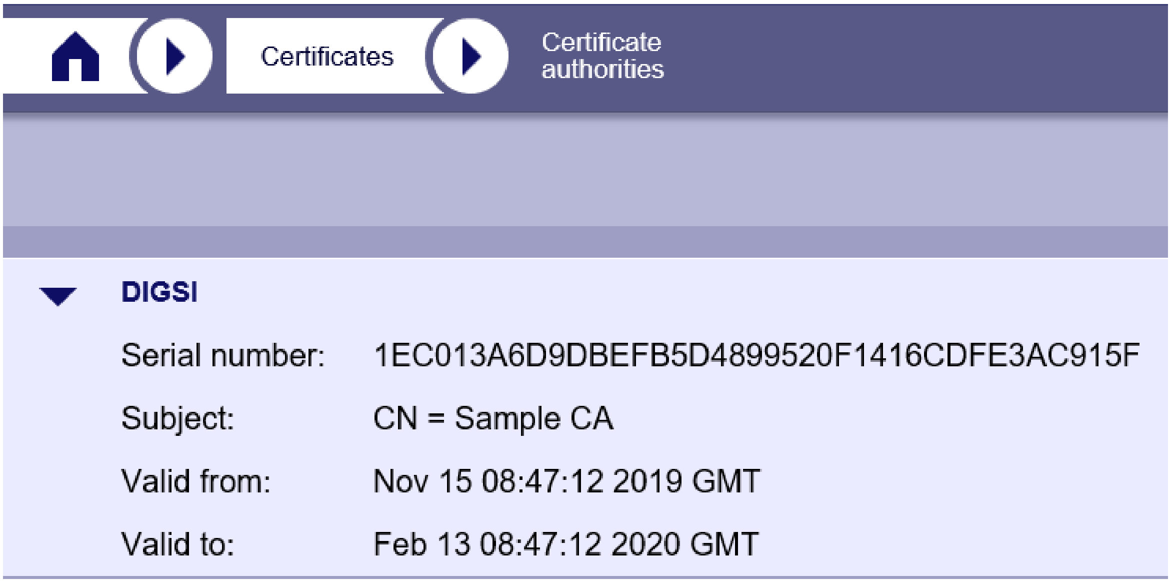
6.5.2.3 Verification of Configured CA via a Web Browser

You can check the configuration of the **DIGSI client authentication** via a Web browser.

To check the settings, proceed as follows:

✧ Open the Web browser and login to a device that has been configured to only accept connection requests from DIGSI 5 installations that use your own CA-issued certificates (and not Siemens default certificates).

✧ Navigate to **Certificates** > **Certificate authorities**.



DIGSI

Serial number: 1EC013A6D9DBEFB5D4899520F1416CDFE3AC915F

Subject: CN = Sample CA

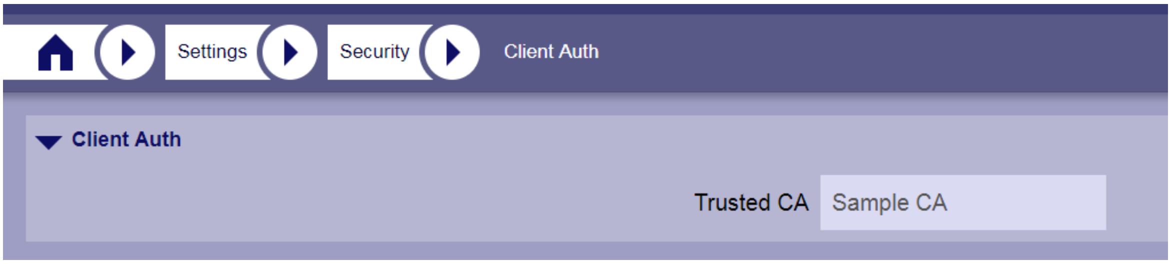
Valid from: Nov 15 08:47:12 2019 GMT

Valid to: Feb 13 08:47:12 2020 GMT

[sc_CerAuth., 1, en_US]

✧ Navigate to **Settings** > **Security** > **Client Auth**.

The configured customer-specific CA can also be checked in the **Client Auth** settings page as follows:



Client Auth

Trusted CA: Sample CA

[sc_settings_ClientAuth, 1, en_US]

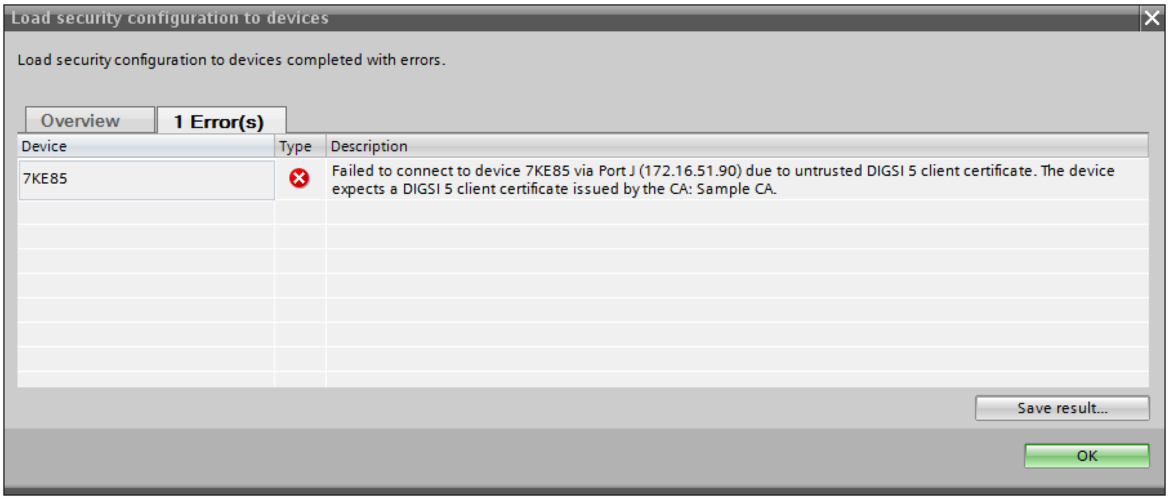
If you have selected the **SIPROTEC 5 trusted certificate authority**, the value for **Trusted CA** is **Default**.

6.5.2.4 Unauthorized DIGSI 5 Access to SIPROTEC 5 Devices

With the configuration of a Trusted certificate authority (CA), a valid client certificate signed by that CA needs to be available within the Windows system CA store in order to be able to establish a secure connection to the SIPROTEC 5 device.

No Valid Certificate

If no valid client certificate is available, DIGSI 5 will not be able to connect to the SIPROTEC 5 device. Instead, an error message will be displayed indicating the expected client certificate:



Load security configuration to devices

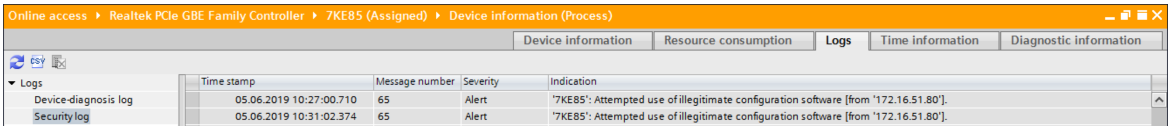
Load security configuration to devices completed with errors.

Overview | 1 Error(s)

Device	Type	Description
7KE85	☒	Failed to connect to device 7KE85 via Port J (172.16.51.90) due to untrusted DIGSI 5 client certificate. The device expects a DIGSI 5 client certificate issued by the CA: Sample CA.

[sc_unauthorized_DIGSI_access, 1, en_US]

This unauthorized access attempt additionally results in an entry in the security log:

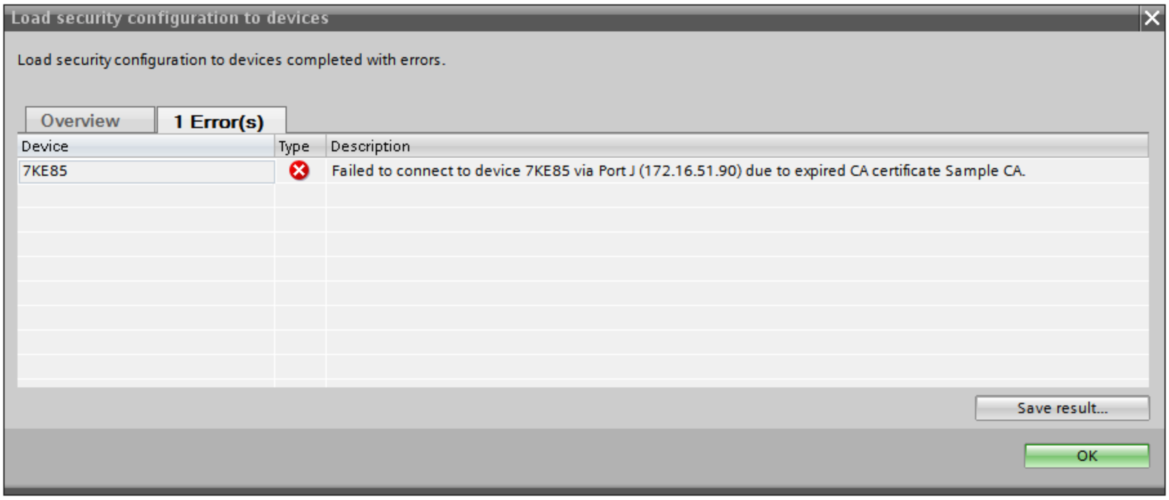


Time stamp	Message number	Severity	Indication
05.06.2019 10:27:00.710	65	Alert	'7KE85': Attempted use of illegitimate configuration software [from '172.16.51.80'].
05.06.2019 10:31:02.374	65	Alert	'7KE85': Attempted use of illegitimate configuration software [from '172.16.51.80'].

[sc_unauthorized_DIGSI_access_security_log, 1, en_US]

Expired Certificate

If the configured Trusted CA has expired before its renewal, the following error message is displayed while trying to connect to the SIPROTEC 5 device:



Load security configuration to devices completed with errors.

Device	Type	Description
7KE85	⊗	Failed to connect to device 7KE85 via Port J (172.16.51.90) due to expired CA certificate Sample CA.

[sc_unauthorized_DIGSI_access_message, 1, en_US]

In order to recover from an unintentional lockout, refer to chapter *6.5.2.5 Recover from Lockout via Secure Credential Reset*.

6.5.2.5 Recover from Lockout via Secure Credential Reset

With the configuration of a Trusted CA, a valid client certificate signed by the CA needs to be available within the Windows system CA store in order to be able to establish a secure connection to the SIPROTEC 5 device.

If the Trusted CA expires before its renewal or if the appropriate client certificate is not available anymore in the Windows system CA store, DIGSI will not be able to communicate with the SIPROTEC 5 device anymore. Recovering from that scenario is only possible by resetting access credentials via a USB connection.

NOTE

The setting of the parameter `Integrated Port USB` has no impact on this recovery.

Prerequisite for recovering is that you have downloaded the **Security Credentials and Configuration Reset File** (SCRF file) from the device first.

Downloading SCRF File

To do this, proceed as follows:

- ✧ Select the device in the project tree and select **Online** → **Security** → **Download credentials reset file...**.
- ✧ For recommendations related to the handling of SCRF files see also *10.1.1 Downloading the Secure Credential and Configuration Reset File (SCRF)*.

Recover from a Lockout

To recover from a lockout, this SCRF file can be uploaded to the device via USB without having a valid client certificate.

To do this, proceed as follows:

- ✧ Select the device in the project tree and select **Online** → **Security** → **Reset access credentials...**.

This operation resets the client certificate validation settings in the device to factory defaults, thereby allowing DIGSI 5 installations with inbuilt Siemens client certificates to be able to communicate with the device.

NOTE

As consequence, all security relevant settings will be set to their default values!

6.6 IEEE 802.1X Certificate Authentication

For versions 8.30 and higher, with the **IEEE 802.1X** certificate authentication feature, SIPORTEC 5 devices support IEEE 802.1X port-based network access control via Ethernet communication modules, for example, port E, port F, port N, or port P.

If this feature is activated, working with a 802.1X authenticator such as a router or a switch, a SIPROTEC 5 device takes the role of 802.1X supplicant. This feature provides a secure, certificate-based access control of your network access. It permits or denies network connection to SIPROTEC 5 devices based on the certificate-based mutual authentication. It only allows authenticated devices access your network, and prevents illegal devices or clients from accessing and hacking your network.

The ECC (Elliptic Curve Cryptography) digital-signature algorithm not the RSA (Rivest-Shamir-Adleman) algorithm is used in the digital certificates in this feature.

Before configuring this feature, make sure that the following prerequisites are met:

- Set the network redundancy protocol of the port to ***Line Mode***.
- Available CAs are imported in the **DIGSI 5 CA store** (see chapter *6.5.2.1 Setup the DIGSI 5 CA Store*).

NOTE

If RBAC is enabled, only users in the role of a **SECADM** or an **Administrator** can configure the **IEEE 802.1X** certificate authentication feature.

NOTE

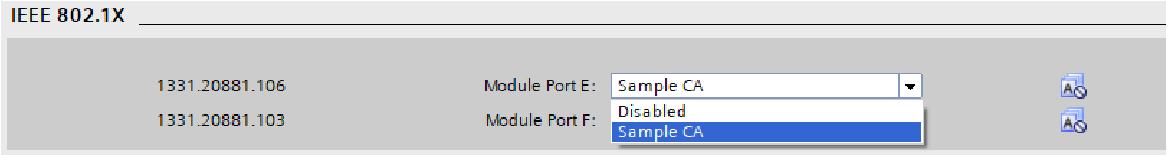
If the **IEEE 802.1X** certificate authentication feature and RBAC are both enabled, Siemens recommends activating the emergency account to ensure that SCRF and SFRF can be downloaded under specific conditions.

Configuration in DIGSI 5

To configure the **IEEE 802.1X** certificate authentication feature for a device, proceed as follows:

✧ In the project tree, select the target device, navigate to **Safety and security** and select **Network access security**.

The following information is displayed:



IEEE 802.1X

1331.20881.106 Module Port E: Sample CA

1331.20881.103 Module Port F:

Disabled
Sample CA

[sc_DIGSI_802.1x, 2, en_US]

✧ From the list box of a module port, select the CA that you use to verify the **IEEE 802.1X** server certificate.

The default value of this list box is ***Disabled***.

✧ Load the security settings to the device for them to take effect.

Upload of the IEEE 802.1x Certificate via the Browser-Based User Interface

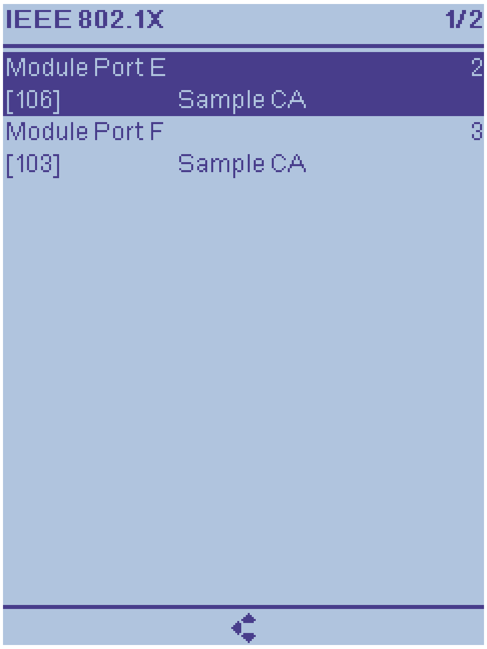
✧ In order for the IEEE 802.1X protocol to take effect, you must sign and upload the certificate manually.

For more information on how to upload the **IEEE 802.1X** certificate to a device, refer to chapter *7.2.4 Example: Uploading a Certificate to a Device*.

Status Verification of the IEEE 802.1X Certificate in a Device

To verify the status of the **IEEE 802.1X** certificate in a device, proceed as follows:

✧ In the device, navigate to **Main menu** > **Settings** > **Security** > **IEEE 802.1X**.



IEEE 802.1X 1/2

Module Port E 2
[106] Sample CA

Module Port F 3
[103] Sample CA

[sc_HMI_802.1X, 2, en_US]

NOTE

To disable the **IEEE 802.1X** certificate feature in a device, disable this feature on the router or switch side first.

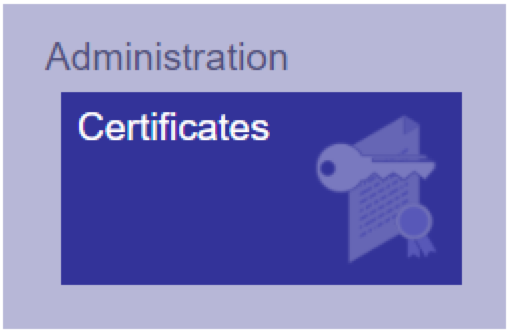
7 Certificate Management

7.1 Introduction

In some cases, you must manage the digital certificates.
The **Certificate Management** feature makes the following operations possible:

- Checking current certificates
- Downloading CSR (Certificate Signing Request) files
- Uploading certificates
- Deleting certificates

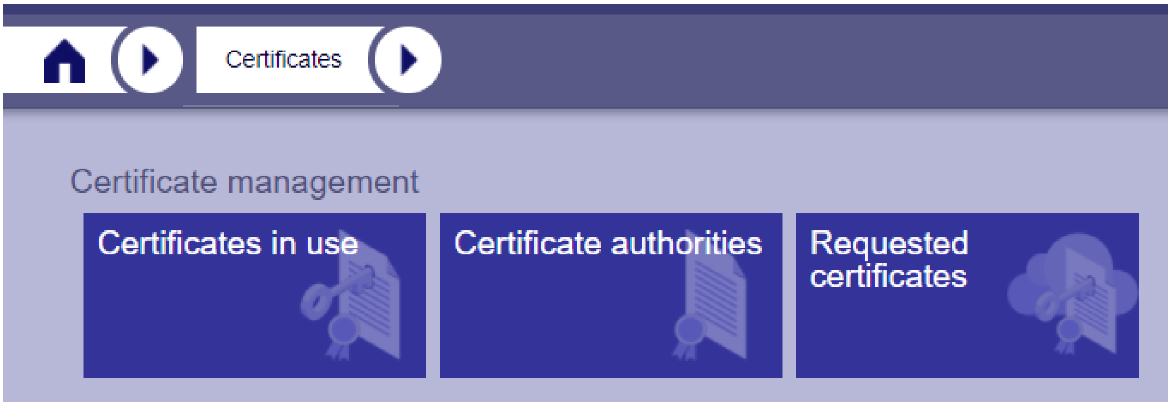
You can do all these operations only via the **browser-based user interface**.
If the RBAC is enabled, you can see the **Certificates** button only with the role **SECADM** or **Administrator**. Once the RBAC is disabled, all users have read and write access to the certificates with password ***111111***.



[sc_certificates_button, 2, en_US]

If you click the **Certificates** button, the following sections are available:

- Certificates in Use
- Certificate Authorities
- Requested Certificates



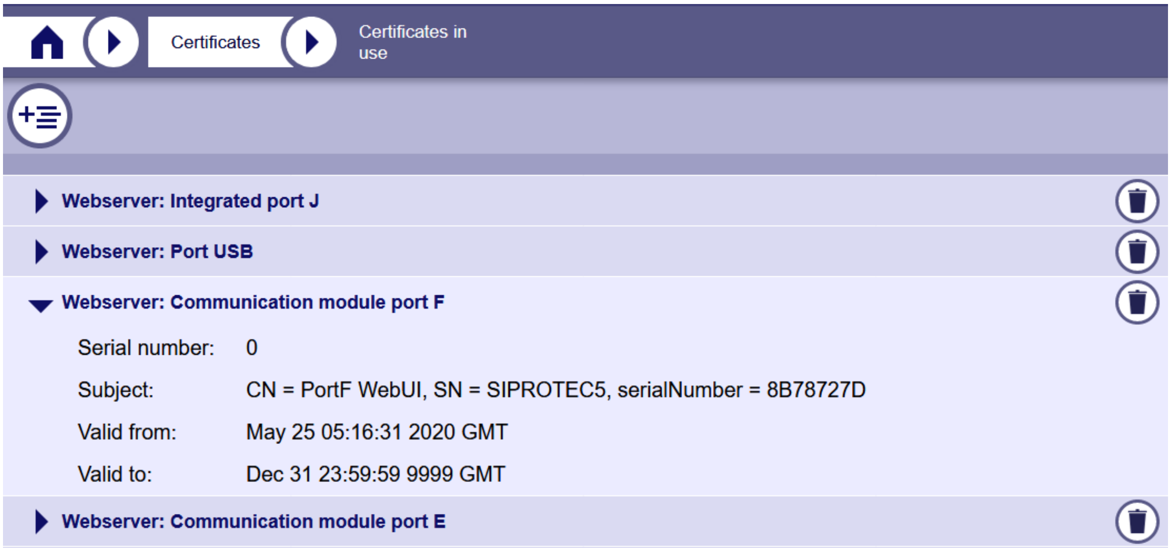
[sc_CM, 3, en_US]

For more information on these sections, refer to the following chapters.

7.2 Manual Management

7.2.1 Certificates in Use

Certificates that are currently used in the device are displayed in the **Certificates in Use** section. You can also upload or delete certificates in this section.


Certificates
Certificates in use
Webserver: Integrated port J
Webserver: Port USB
Webserver: Communication module port F
Webserver: Communication module port E

Serial number: 0
Subject: CN = PortF WebUI, SN = SIPROTEC5, serialNumber = 8B78727D
Valid from: May 25 05:16:31 2020 GMT
Valid to: Dec 31 23:59:59 9999 GMT

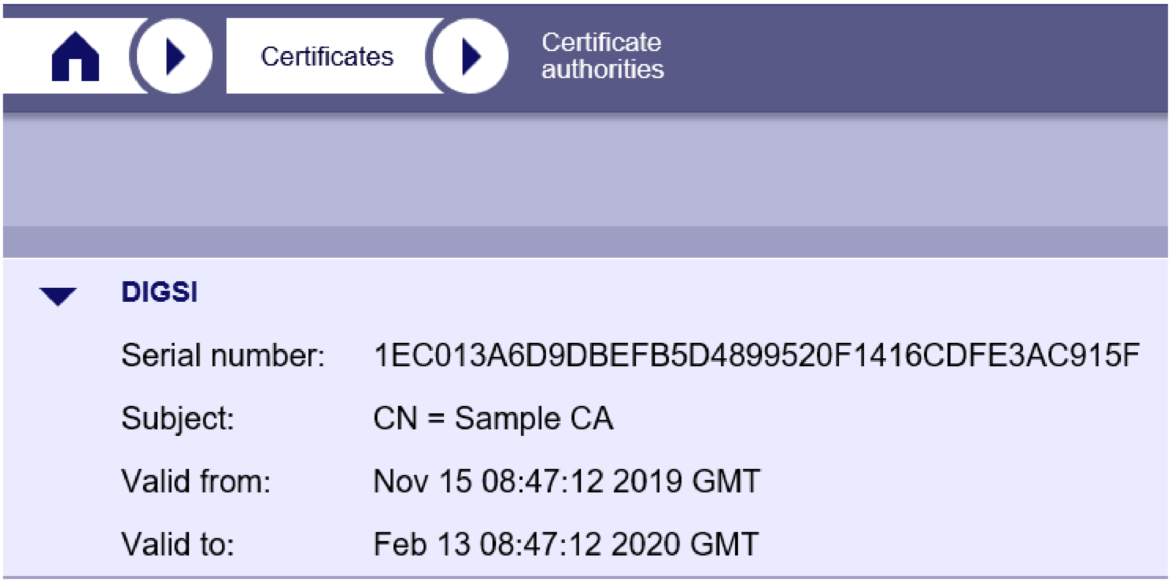
[sc_certificates, 2, en_US]

NOTE

Only certificates in the .pem format are accepted when uploading certificates to the devices.
For enhanced security, Siemens recommends replacing the default certificate with your own certificate.

7.2.2 Certificate Authorities

If you have imported your CAs in the **DIGSI 5 CA store** in DIGSI 5 and have loaded the CAs to the device, you can view the CAs in the **Certificate Authorities** section with the **browser-based user interface**.



DIGSI

Serial number: 1EC013A6D9DBEFB5D4899520F1416CDFE3AC915F

Subject: CN = Sample CA

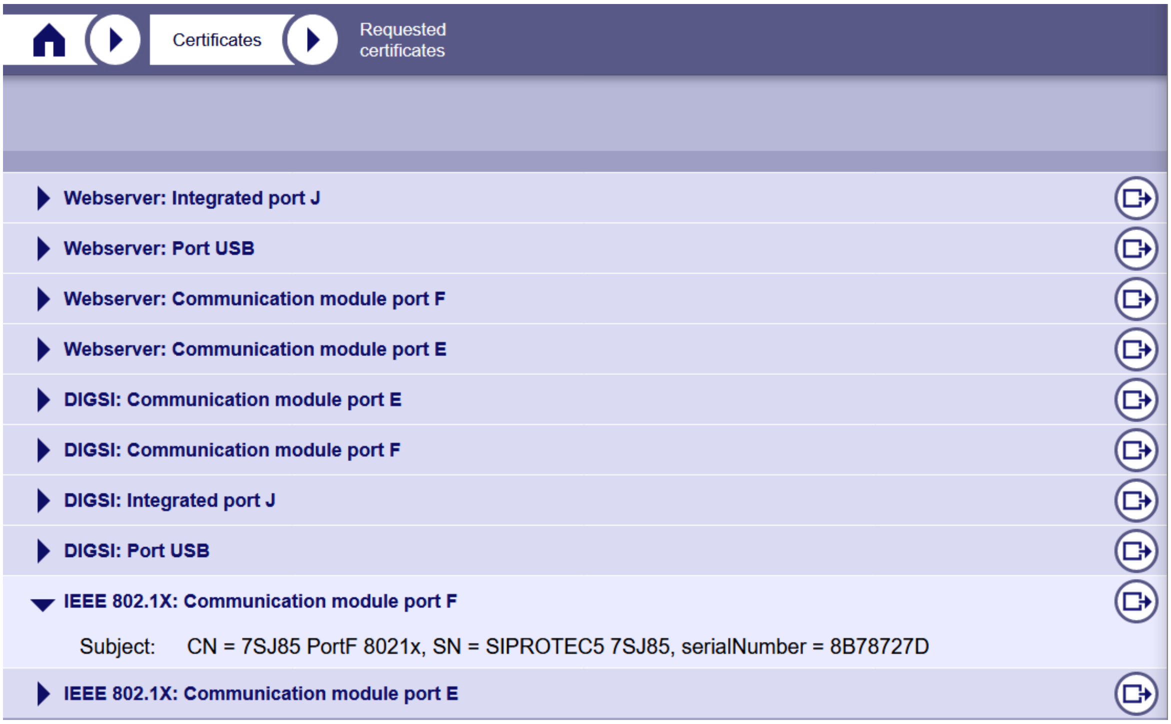
Valid from: Nov 15 08:47:12 2019 GMT

Valid to: Feb 13 08:47:12 2020 GMT

[sc_CerAuth., 1, en_US]

7.2.3 Requested Certificates

Once you enable a certificate-related feature in DIGSI 5 and load it to the device, the device generates a corresponding CSR file automatically. Such CSR files are listed in the **Requested Certificates** section.
With the export button, you can download a CSR file to your local PC for signing.



- Webserver: Integrated port J
- Webserver: Port USB
- Webserver: Communication module port F
- Webserver: Communication module port E
- DIGSI: Communication module port E
- DIGSI: Communication module port F
- DIGSI: Integrated port J
- DIGSI: Port USB
- IEEE 802.1X: Communication module port F

  Subject: CN = 7SJ85 PortF 8021x, SN = SIPROTEC5 7SJ85, serialNumber = 8B78727D
- IEEE 802.1X: Communication module port E

[sc_crt_export, 2, en_US]

7.2.4 Example: Uploading a Certificate to a Device

The IEEE 802.1X certificate is used as an example to show the complete certificate-uploading processes.

To upload the certificate to the device, proceed as follows:

Make sure the **IEEE 802.1X** feature is enabled in the device and the Web browser is successfully connected to the device. For more information of the **IEEE 802.1X** feature, refer to *6.6 IEEE 802.1X Certificate Authentication*.

✧ Unfold the **IEEE 802.1X** item under **Certificates** > **Requested Certificates**.

✧ Click the export button and save the downloaded file (.csr) to a folder.

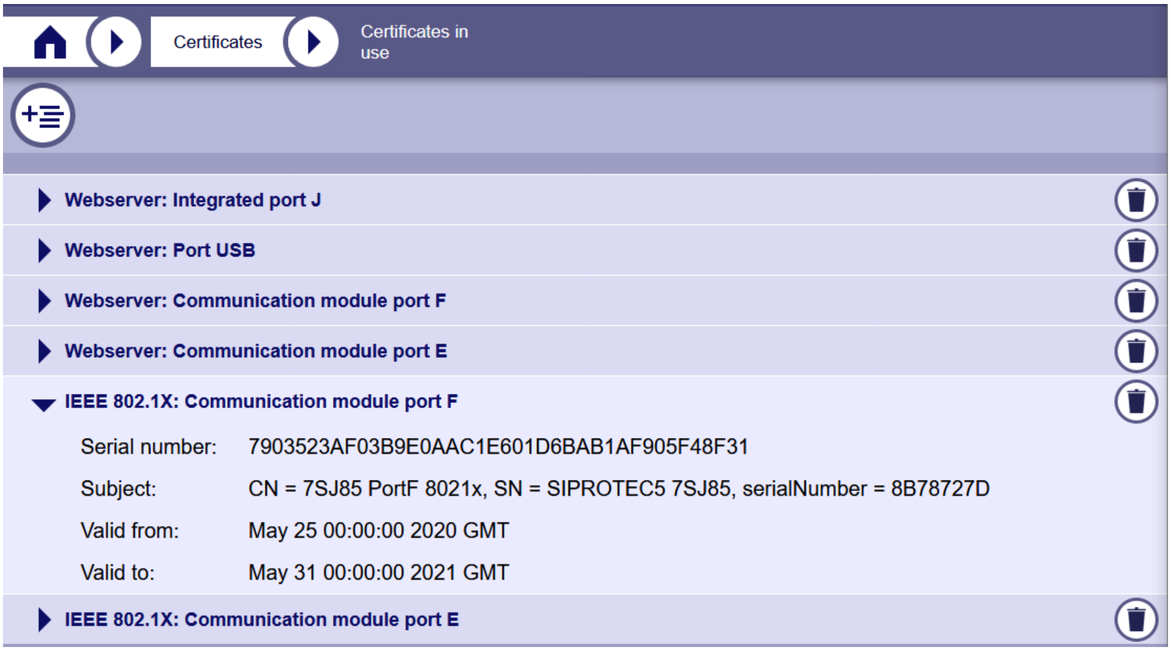
✧ Sign the downloaded CSR file with SICAM GridPass in your local PC.
For more information on how to sign a CSR file with SICAM GridPass, refer to the SICAM GridPass Manual *www.siemens.com/sicam-gridpass*.

✧ Save the signed file as .pem.

✧ Click the upload button in the **Certificates in Use** section.

✧ In the **Upload Certificate** dialog, click the **Select a file** button.

✧ Select the signed IEEE 802.1X certificate and click the upload button.



Webserver: Integrated port J

Webserver: Port USB

Webserver: Communication module port F

Webserver: Communication module port E

IEEE 802.1X: Communication module port F

Serial number: 7903523AF03B9E0AAC1E601D6BAB1AF905F48F31
Subject: CN = 7SJ85 PortF 8021x, SN = SIPROTEC5 7SJ85, serialNumber = 8B78727D
Valid from: May 25 00:00:00 2020 GMT
Valid to: May 31 00:00:00 2021 GMT

IEEE 802.1X: Communication module port E

[sc_upload_suc, 2, en_US]

Once the IEEE 802.1X certificate is successfully loaded to the device, you can see the certificate listed in the **Certificates in Use** section.

7.3 Automatic Enrollment over Secure Transport

When a considerable number of users are distributed across the network for various devices, it becomes a real challenge for security administrators to maintain the validity of each certificate for each service where the PKI is used. To solve these issues, Siemens provides the **Automatic enrollment over secure transport** (EST) feature which is developed based on RFC 7030 and IEC 62351-9 standards.

The EST client in all devices points to a single EST server. Then, the request for certificate renewal is forwarded to the administration interface of the single EST server.

Siemens provides the state-of-the-art **EST Server** application and functionality in SICAM GridPass to maintain the certificate signing requests (CSRs) files and certificate revocation lists (CRLs) in your network.

NOTE

For more information about GridPass, refer to the SICAM GridPass Manual (*www.siemens.com/sicam-gridpass*).

To configure the EST server settings, navigate to **Project** > **Target device** > **Safety and security** > **Automatic certificate management** in DIGSI 5.

7.3.1 EST Server Configuration

In a typical application with EST, the EST server is located outside of the substations and centrally controls different requests that are sent by these substations. Therefore, the transport layer of the EST requests is over a secure TLS channel with mutual authentications. This characteristic of the TLS channel requires an initial customer PKI where the private key of the CA is available and is usable for signing the requests. So, it is impossible to use the default Siemens CA for the EST client.

To set the customer CA for the EST and TLS connection, the customer CA must be available in the **DIGSI CA store**. For more information, refer to *6.5.2.1 Setup the DIGSI 5 CA Store*.

At the first trust of the TLS connection, the following processes are necessary:

- Export the requests of the EST client certificate from the browser-based user interface manually for signature.
- Sign the exported file with the CA which is used for the EST communication.
- Import the EST client certificate to the device with a CA signature to establish validity.

For more information, refer to *7.2.4 Example: Uploading a Certificate to a Device*.

After this initial step is done and trust is established between the EST client and the EST server, the EST client manages all further certificate renewal for the selected protocols and the EST client itself.

Setting Name	Range	Default Value	Remark
IP address	0.0.0.0 to 255.255.255.255	–	–
Server port	1 to 65535	8085	Increments of 1
Module port	All Ethernet communication module	Port J	–
Trusted CA	CAs that are currently imported in the DIGSI 5 CA store	First selection in the selection list	The Trusted CA is the CA that issues the EST server certificate.

7.3.2 Enrollment Configuration

In the **Auto.enroll** zone, check the option where you want the certificates to be managed automatically by the EST server:

- DIGSI 5

  The certificates that are used for the communication between DIGSI 5 and the device are managed automatically.

- Web UI

  The certificates that are used for the communication between the browser-based user interface and the device are managed automatically.

- IEEE 802.1 x

  The certificates that are used for the IEEE 802.1x supplicant are managed automatically.

- SyslogTLS

  The certificates that are used for the communication between the device and the syslog server are managed automatically.

- Secure MMS

  The certificates that are used for the communication between the device and the MMS client are managed automatically.

NOTE

Regardless of whether the certificates are managed manually or automatically, the browser-based user interface is the only way to view them.

For V8.80 and higher versions, EST is only available in modular devices.

8 Backup and Restore

8.1 General

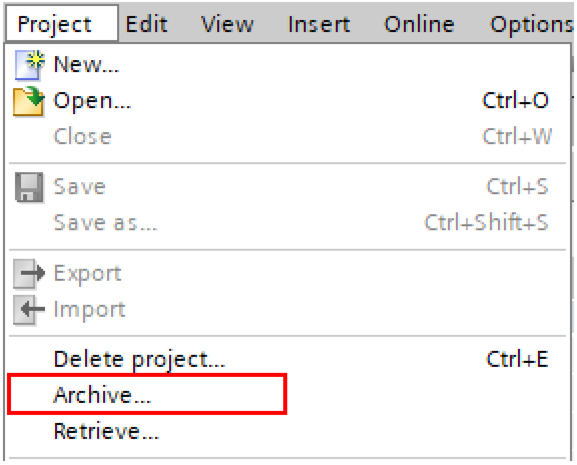
DIGSI 5 manages the components of a system and all project data associated to the system. Projects are structured as folders in Windows. If the presetting is left unchanged, you can find the project folders under **My Files\Automation**. For each project, a folder with the name of the project is created.

8.2 Archiving or Retrieving a Project

In order to save a project as a backup file and retrieve it later, you can archive the project created in DIGSI 5 with the same name or any other name in the desired location. After archiving any currently opened project in DIGSI 5, you can continue working on the project without closing it. If necessary, you can always retrieve the archived version of the project and start working on it at any time.

Archiving a Project

✧ In the **Project** menu, click **Archive...**.

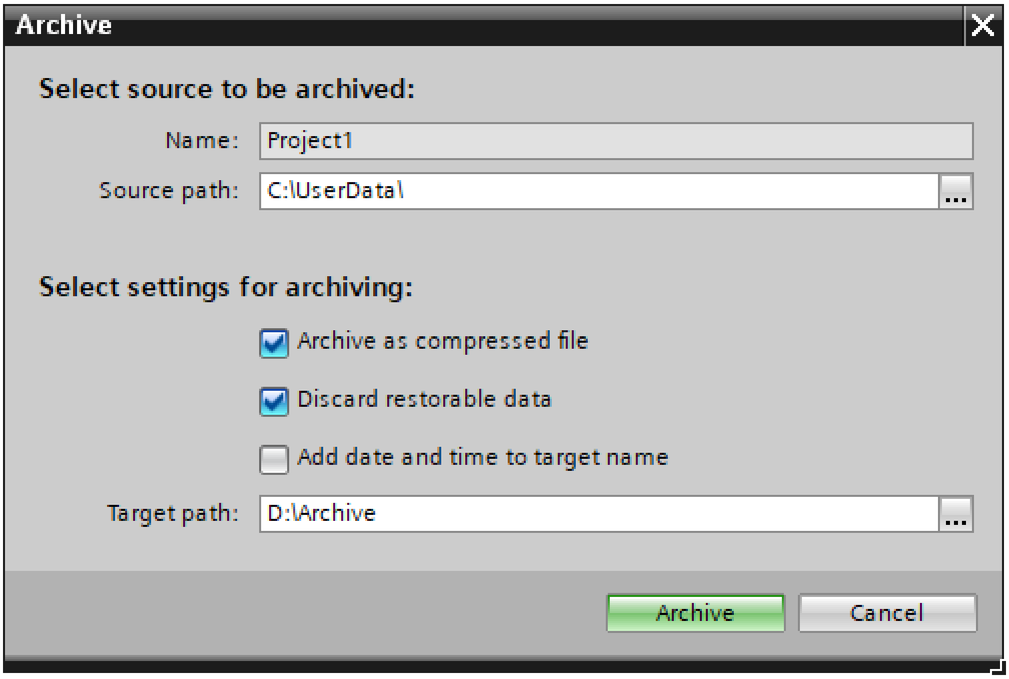


[sc_project_menu, 1, en_US]

Figure 8-1 Archive Menu Item

The **Archive** dialog opens with the default file name.

✧ If necessary, enter the new archive path.


Archive

Select source to be archived:

Name: Project1

Source path: C:\UserData\

Select settings for archiving:

☑ Archive as compressed file

☑ Discard restorable data

□ Add date and time to target name

Target path: D:\Archive

[sc_archive_project, 1, en_US]

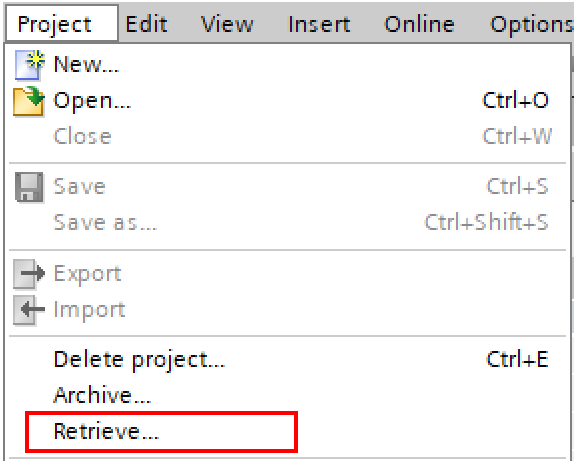
Figure 8-2 Archive Dialog

✧ Click **Archive**.
A progress dialog appears and displays the archive status.

The archived project file is saved in the desired location with the file extension **.dz5**.

Retrieving an Archived Project

✧ In the **Project** menu, click **Retrieve...**.



[sc_project_menu_2, 1, en_US]

Figure 8-3 Retrieve Menu Item

✧ Select the archived project with the file extension **.dz5** from the respective folder.

✧ Select the target directory in which you want to save the retrieved project.

The retrieved project is opened in DIGIS 5.

9 Security Logging

9.1 Overview

SIPROTEC 5 devices and DIGSI 5 provide a security audit trail function which chronologically acquires and categorizes security-relevant events according to the origin and severity.

When a security-related event occurs, the SIPROTEC 5 device spontaneously sends the event to 1 or 2 external syslog-servers without a conformation via UDP or TLS while DIGSI 5 sends such an event to the Windows Event Log. This action allows security-related events to be recorded from various transformer stations with the requirements of standards and guidelines, such as IEEE 1686, IEC 62443, and the BDEW White Paper.

For the device, logging is started centrally on 1 or 2 self-selected syslog servers. Combining different protocol data that the devices use gives you a general overview of the device network. You can analyze and monitor this data. This action allows safety-critical events to be logged and related changes to be tracked. You can also track attacks on the operated devices by the log data.

A later readout of the logged security-related events from the security event buffer which is in the device is possible. The logs are in English.

You can view the collected log data in the security log locally on the device display, irrespective of the current operating mode of the device. The alarm and safety-critical indications are stored chronologically in the security log. You cannot modify or delete these entries.

For a full list of recorded security events, refer to *9.3.1 Configuration of Security Logging*.

NOTE

On the syslog servers, Siemens recommends protecting the received security-events from unauthorized read or write access with the role Auditor.

9.2 Environment

Supported System and Firmware Versions

The following table shows the system and firmware versions that support syslog:

System	Devices	Versions	Interfaces
SIPROTEC 5	Modular devices Non-modular devices	V07.50 and higher	• Port J • Port E • Port F • Port P • Port N
	Compact devices	V08.70 and higher	Port F

Supported Communication Protocols and Operating Modes

All alarms and warning indications are available as temporary indications. With the **Security logging** function enabled, the security-related alarms and warning indications are sent to supervision systems (such as control centers) via supported communication protocols under supported operating modes.

- Supported operating modes
  - Simulation mode
  - Process mode
  - Commissioning mode
  - Fallback mode

9.3 Configuration

9.3.1 Configuration of Security Logging

If you have started DIGSI 5 and connected it to a device, select **Safety and security** > **Security event logging** in the project tree. The **Sec. Ev. Logg.** menu item contains the setting options for a central syslog server. You can activate up to 2 syslog servers.

Capacity Utilization of the Syslog Server

In the **General** area, with the adjustable parameter **Security log cap. warn.**, you determine from which utilization of the security log on a warning indication is issued. A warning threshold of 80 % means that the set capacity limit has been reached after approx. 1600 entries in the security log. Further warning indications are issued when the capacity limits of 85 %, 90 %, 95 %, and 98 % are reached.

The security logs are organized as a ring buffer. If the entries of the security logs exceeds the 100 % capacity limit, the oldest entries are automatically overwritten and the capacity utilization is reset to 0 %. When you read the security log using DIGSI 5, the capacity utilization is reset to 0 %. The warning indications remain in the device. You must apply all settings with DIGSI 5.

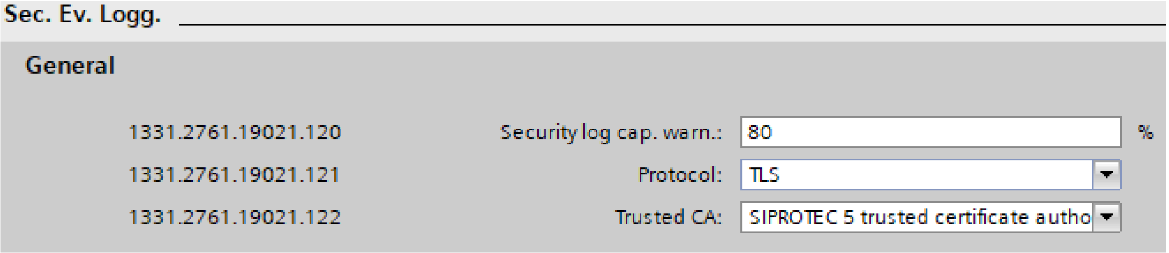
If you downgrade the firmware to a version lower than V07.50, the device-internal log size decreases from the current value of 2048 entries to 500 entries. The older firmware supports only 500 entries in another format. In this case, the most recent 500 entries are taken from the current/syslog-capable device status and format are applied to the older firmware-appropriate format. The rest of the entries is lost.

After the downgrade, the content of the internal log with its 2048 entries is deleted. In the meanwhile, a message that a firmware downgrade has taken place is logged as the most recent entry in the ported log.

Transmission Protocol

The parameter `Protocol` lets you select via which protocol the logs are transmitted. Currently, the protocols UDP and TLS are supported.

Additionally, if you select the protocol ***TLS***, you must also select the server CA that you trust for the transmission.



Sec. Ev. Logg.

General

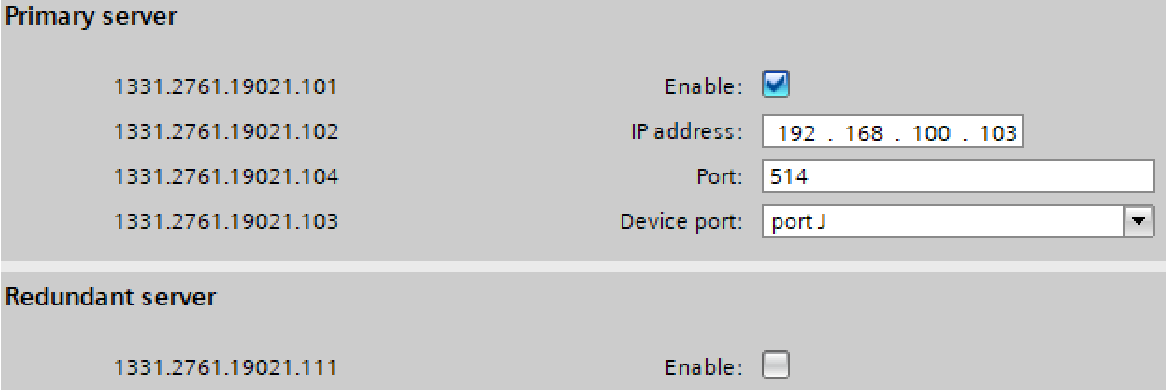
1331.2761.19021.120	Security log cap. warn.:	80	%
1331.2761.19021.121	Protocol:	TLS	
1331.2761.19021.122	Trusted CA:	SIPROTEC 5 trusted certificate autho	

[sc_syslog_TLS, 1, en_US]

Figure 9-1 Transmission Protocol TLS Selected

Syslog Server Information

To establish a connection between the SIPROTEC 5 device and a syslog server that is used to log the security-related events, define the following parameters in DIGSI 5.



Primary server

1331.2761.19021.101	Enable:	☑
1331.2761.19021.102	IP address:	192 . 168 . 100 . 103
1331.2761.19021.104	Port:	514
1331.2761.19021.103	Device port:	port J

Redundant server

1331.2761.19021.111	Enable:	□

[sc_Primary log server, 1, en_US]

Activate logging under **Primary server** and/or **Redundant server**. The following parameters are for the connection to the syslog server:

Parameter Names	Descriptions
IP address	IP address of the to be connected syslog server
Port	Port number of the to be connected syslog server
Device port	Device port, through which the SIPROTEC 5 device logs the events to the syslog server

For more information about the supported security events, refer to *9.4 Logged Security Events*.

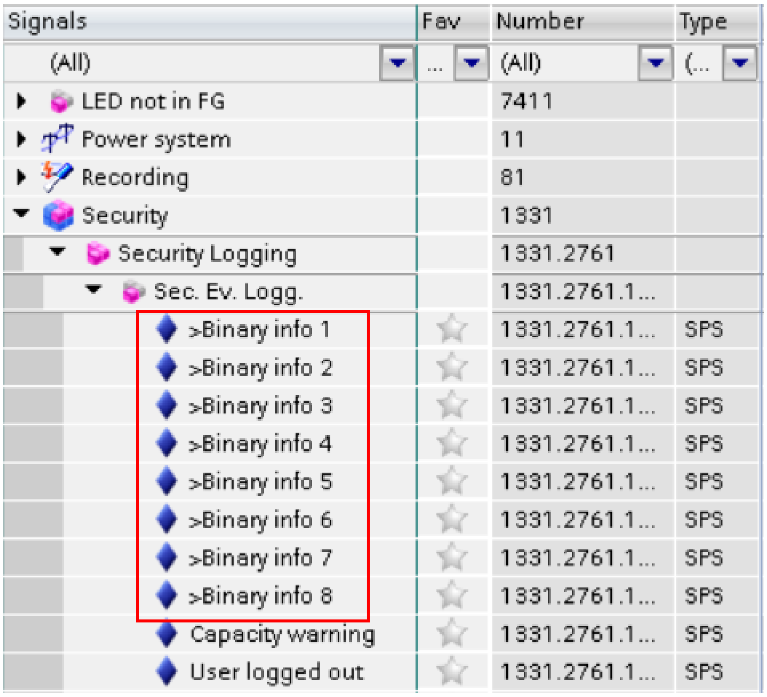
9.3.2 Checking the Used Syslog Servers

On the device display, you can check the information of the used syslog servers via **Main** > **Settings** > **Security** > **Security Logging** > **Sec. Ev. Logging**.

9.3.3 Customizable Logged Events

For versions 8.80 and higher, DIGSI 5 provides 8 binary input signals for logging of the user-defined events. These logged user-defined events are of the severity level *Event*.

You can see these signals via **Project** > **Target device** > **Information routing** > **Security** > **Security Logging** > **Sec. Ev. Logg.** in DIGSI 5. You can double-click the signal names to rename the signals.



Signals	Fav	Number	Type
(All)	...	(All)	(...
LED not in FG		7411	
Power system		11	
Recording		81	
Security		1331	
Security Logging		1331.2761	
Sec. Ev. Logg.		1331.2761.1...	
>Binary info 1	☆	1331.2761.1...	SPS
>Binary info 2	☆	1331.2761.1...	SPS
>Binary info 3	☆	1331.2761.1...	SPS
>Binary info 4	☆	1331.2761.1...	SPS
>Binary info 5	☆	1331.2761.1...	SPS
>Binary info 6	☆	1331.2761.1...	SPS
>Binary info 7	☆	1331.2761.1...	SPS
>Binary info 8	☆	1331.2761.1...	SPS
Capacity warning	☆	1331.2761.1...	SPS
User logged out	☆	1331.2761.1...	SPS

[sc_user-defined events, 1, en_US]

Figure 9-2 Customizable Logged Events

9.4 Logged Security Events

9.4.1 Logged Content

When **Primary server** and/or **Redundant server** is activated, the following items are logged in the security log and forwarded to the servers:

- Actions
  - Successful logout of a user, even after a certain period
  - Successful login of a user
  - Change or delete the connection password
  - Update or restore the firmware version in the device
  - Update the configuration in the device
  - Change the operating mode of the device
  - Change the date and time
  - Change or overwrite state value entries by the logged-on user
  - Switching operations by the registered user
  - View the audit log in the device
- Potential errors
  - Number of entries with correct or incorrect passwords
  - Unsuccessful login attempt by typing 3 wrong passwords
  - Reboot or restart the device
- Other entries
  - Capacity warning of the security log

The following table shows which type of message (including format) and which action is expected.

Event/Alarm Summary	Description
Syslog message severity: WARNING	
Successful remote and local login	The content of the events for the successful login depends on whether RBAC is active or not and on the location from which the login is made: Remotely (for example, DIGSI 5) or locally (on-site operation).
Manual logoff	The events for the manual logout are logged in the Audit Trail and transmitted using syslog UDP. The content of the indication depends on whether RBAC is active or not.
Logoff determined by time	The content of the indication depends on whether RBAC is active or not.
Forcing control operations	Events for control operations initiated locally or remotely. For example: • Changing the position of the poles • Tripping/closing operations in relation to the primary equipment • Command operations in relation to the primary equipment • Mode-change operations in relation to the primary equipment • Start/cancellation of the switching sequence • Change in coil position • Control of sequential voltages/target voltages • Control of the switching authority • Controlling the winding selection

Event/Alarm Summary	Description
Downloading the configuration	Events relating to downloading the protection configuration to a PC
Uploading the configuration	Events relating to uploading the protection configuration from a PC to a device
Configuration change	Events that display a change in the current configuration, for example, from changing a parameter
Firmware change	Events relating to uploading the device firmware in the device
AuditLog access	Events relating to displaying and downloading the audit trails of the device
Change in time and date	Event that displays the changes in the current date/time configuration.
Syslog message severity: ALARM	
Security management	Events that display changes in the current security configuration for the following elements: • User management • User authentication • Secure communication • Settings for security supervision (logging)
Login failed	Events for a failed login attempt If RBAC is active, the failed logins are logged after 3 attempts for one user name within the configured time frame. Afterward, each additional incorrect attempt for the same user name is logged as well until the maximum number of login attempts has been reached. Once the number of login attempts has been exhausted, the login for that user name is blocked for the configured time span. That is, additional login attempts for that user name are refused and logged, regardless of whether the combination of user name and password is correct or not. Once the blocking time has elapsed, the counter for the blocked user name is reset. The counter for this user name is also reset if a successful login attempt occurs for this user name or if the time span has elapsed without reaching the maximum number of login attempts.
Product restart	Events upon restarting the device. Booting or restarting the device by removing the power supply or by using a device-internal restart mechanism, for example, a reset button, switch-on sequence, or access to software, is logged.
Invalid configuration and firmware	Events upon detection of an invalid configuration or firmware, for example, a SIPROTEC 5 device signature check

NOTE

The use of a confirmation ID is not logged. Only security-related events are logged.

9.4.2 Structure of a Security-Log Entry

A security-log entry is built up with the following elements:

Element	Description
Severity (level)	Severity levels: • Event • Alarm
Date	Date when the event is logged

Element	Description
Time	Time when the event is logged • T Time • hh:mm:ss.ttt Time when the event is created • +hh:mm Time deviation from GMT
IP address or port name	IP address or port name of the product or subcomponent that generates the log entry
Module name	The name of the product module that generates the log entry
BOM	Byte order mark for UTF8 encoding
Product name	The name of the product that generates the log entry
Indication text	The message part of a syslog event Depending on the event, the indication text can contain variable additional information (%A1%, %A2%, %A3%, and %A4%).

9.4.3 Syslog Events SIPROTEC 5

NOTE

The **browser-based user interface** does not support displaying security logs.

Severity Level Event

The following table shows syslog messages at the severity level ***Event***.

Table 9-1 Syslog Messages at Severity Level Event

Event	Additional Information	
Storage capacity of the security audit decreased below the set threshold of %A1% entries.	%A1%	Threshold of the storage capacity set by users or the default value ***80***
User %A1% initiated a remote session from %A2% in the role(s) of %A3%.	%A1%	Account ID
	%A2%	IP address of the remote workstation
	%A3%	Role(s) which are assigned to the user and separated with commas in the list
User %A1% changed the settings related to user authentication: %A2% server: IP address [set to value %A3%].	%A1%	Account ID
	%A2%	Protocol (RADIUS, LDAP)
	%A3%	IP address
A user initiated a remote session from %A1%.	%A1%	IP address of the remote workstation
User %A1% initiated a local session in the role(s) of %A2%.	%A1%	Account ID
	%A2%	Role(s) which are assigned to the user and separated with commas in the list
User %A1% logged out.	%A1%	Account ID
A user terminated an interactive session.	–	–

Event	Additional Information	
The interactive session with user %A1% was terminated due to time-out (%A2%).	%A1%	Account ID
	%A2%	Time-out threshold set by the user or the default value (10 minutes) for the user inaction After this duration, the existing user-interactive session is terminated.
A user-interactive session was terminated due to time-out (%A1%).	%A1%	Time-out threshold set by the user or the default value (10 minutes) for the user inaction After this duration, the existing user-interactive session is terminated.
Password protection in the type of %A1% was disabled.	%A1%	Phrase, which clearly identifies the purpose of the password. For example, for the SIPROTEC 5 connection password, this is ***connection password***.
Password protection in the type of %A1% was modified.	%A1%	Phrase, which clearly identifies the purpose of the password. For example, for the SIPROTEC 5 connection password, it is ***connection password***.
User %A1% created an account %A2% in the role(s) of %A3% (%A4%-managed account).	%A1%	Account ID of the user that performs the activity
	%A2%	Account ID that is affected by the activity
	%A3%	Roles assigned to the user
	%A4%	Account type
User %A1% modified password of the account %A2% (%A3%-managed account).	%A1%	Account ID of the user that performs the activity
	%A2%	Account ID that is affected by the activity
	%A3%	Account type
User %A1% deleted the account %A2% (%A3%-managed account).	%A1%	Account ID of the user that performs the activity
	%A2%	Account ID that is affected by the activity
	%A3%	Account type
A user manually overwrote the real data.	–	–
A user manually overwrote the real data from %A1%.	%A1%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
User %A1% manually overwrote the real data.	%A1%	Account ID
User %A1% manually overwrote the real data from %A2%.	%A1%	Account ID
	%A2%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
A user executed the control operation %A1%. Additional information: %A2%	%A1%	Type of carried-out control operation, for example, circuit-breaker deactivated
	%A2%	Additional information about the control operation, for example, <FG.FN.FB.signalname of circuit breaker as stated in the DIGSI 5 operational log>
A user executed a control operation from %A1%: %A2%. Additional information: %A3%	%A1%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out. If a PC software is used, then it is the IP address of the PC.
	%A2%	Type of carried-out control operation, for example, circuit-breaker deactivated
	%A3%	Additional information about the control operation, for example, <FG.FN.FB.signalname of circuit breaker as stated in the DIGSI 5 operational log>

Event	Additional Information	
User %A1% executed a control operation: %A2%. Additional information: %A3%	%A1%	Account ID
	%A2%	Type of carried-out control operation, for example, circuit-breaker deactivated
	%A3%	Additional information about the control operation, for example, <FG.FN.FB.signalname of circuit breaker as stated in the DIGSI 5 operational log>
User %A1% executed a control operation from %A2%: %A3%. Additional information: %A4%	%A1%	Account ID
	%A2%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
	%A3%	Type of carried-out control operation, for example, circuit-breaker deactivated
	%A4%	Additional information about the control operation, for example, <FG.FN.FB.signalname of circuit breaker as stated in the DIGSI 5 operational log>
Configuration settings were downloaded from %A1%.	%A1%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
User %A1% downloaded configuration settings from %A2%.	%A1%	Account ID
	%A2%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
Configuration settings were uploaded from %A1%.	%A1%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
User %A1% uploaded configuration settings from %A2%.	%A1%	Account ID
	%A2%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
Configuration settings were changed.	–	–
Configuration settings were changed from %A1%.	%A1%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
User %A1% changed the configuration settings.	%A1%	Account ID
User %A1% changed the configuration settings from %A2%.	%A1%	Account ID
	%A2%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
Firmware in version %A1% was uploaded from %A2%.	%A1%	Version of firmware uploaded
	%A2%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.

Event	Additional Information	
User %A1% uploaded the firmware file from %A2%.	%A1%	Account ID
	%A2%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
Audit log was viewed.	–	–
Audit log was downloaded from %A1%.	%A1%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
User %A1% viewed the audit log.	%A1%	Account ID
User %A1% viewed the audit log from %A2%.	%A1%	Account ID
	%A2%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
A change to time/date was carried out from %A1%.	%A1%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
User %A1% changed the time/date.	%A1%	Account ID
User %A1% changed the time/date from %A2%.	%A1%	Account ID
	%A2%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
Authentication of the primary %A1% server %A2% failed.	%A1%	Protocol (RADIUS, LDAP)
	%A2%	IP address
%A1% is changed from off to on.	%A1%	Name of the binary input (BI) You can rename the BI in DIGSI 5. For more information, refer to *9.3.3 Customizable Logged Events*.
%A1% is changed from on to off.	%A1%	Name of the binary input (BI) You can rename the BI in DIGSI 5. For more information, refer to *9.3.3 Customizable Logged Events*.
Port %A1%: CH1: %A2% CH2: %A3%	%A1%	Communication port E, port F, port N, or port P
	%A2%	Link status ***up*** or ***down***
	%A3%	Link status ***up*** or ***down***
Port J: %A1%	%A1%	Link status ***up*** or ***down***
Successful certificate enrollment for %A1% from %A2%	%A1%	Certificate name
	%A2%	IP address
Failed certificate enrollment for %A1% from %A2%	%A1%	Certificate name
	%A2%	IP address

Severity Level Alarm

The following table shows syslog messages at the severity level ***Alarm***.

Table 9-2 Syslog Messages at Severity Level Alarm

Alarm	Additional Information	
When logging on with account %A1% (%A2%-managed account) from %A3%, 3 incorrect password entries in succession were attempted.	%A1%	Account ID
	%A2%	Account types: • For product-managed (local) user accounts, account types are the product names. • For RADIUS users, the account type is ***RADIUS***.
	%A3%	%A3% can be one of the following information: • User-identifiable name of the product where login attempts are detected • If a remote workstation is used, %A3% is the IP address of the remote workstation. • Device operation panel
3 incorrect password entries in succession were attempted while logging on with account %A1% (%A2%-managed account) from %A3%.	%A1%	Account ID
	%A2%	Account types: • For product-managed (local) user accounts, the account type is ***LOCAL***. • For RADIUS users, the account type is ***RADIUS***. • For LDAP users, the account type is ***LDAP***.
	%A3%	It can be one of the following information: • User-identifiable name of the product where login attempts were detected • If a remote workstation is used, %A3% is the IP address of the remote workstation. • Device operation panel
Repeated attempts to log on with account %A1% (%A2%-managed account) from %A3%	%A1%	Account ID
	%A2%	Account types: • For product-managed (local) user accounts, the account type is ***LOCAL***. • For RADIUS users, the account type is ***RADIUS***. • For LDAP users, the account type is ***LDAP***.
	%A3%	It can be one of the following information: • User-identifiable name of the product where login attempts were detected • If a remote workstation is used, %A3% is the IP address of the remote workstation. • Device operation panel

Alarm	Additional Information	
Account %A1% (%A2%-managed account) will be blocked in the next %A3% minutes due to too many unsuccessful login attempts from %A4%.	%A1%	Account ID
	%A2%	Account types: ● For product-managed (local) user accounts, the account type is ***LOCAL***. ● For RADIUS users, the account type is ***RADIUS***. ● For LDAP users, the account type is ***LDAP***.
	%A3%	The configured number of minutes during which the account remains blocked
	%A4%	It can be one of the following information: ● User-identifiable name of the product where login attempts were detected ● If a remote workstation is used, %A3% is the IP address of the remote workstation. ● Device operation panel
Restart initiated with action: %A1%	%A1%	Additional information on the exact action which triggered the restart, for example, configuration update, firmware update
Restart initiated from %A1% with action: %A2%	%A1%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out If a PC software is used, then it is the IP address of the PC.
	%A2%	Additional information on the exact action which triggered the restart, for example, settings download
User %A1% initiated a restart with action: %A2%.	%A1%	Account ID
	%A2%	Additional information on the exact action which triggered the restart, for example, configuration update, firmware update
User %A1% initiated a restart from %A2% with action: %A3%.	%A1%	Account ID
	%A2%	User-identified remote workstation (for example, engineering tool) with which the modifications are initiated to be carried out. If a PC software is used, then it is the IP address of the PC.
	%A3%	Additional information on the exact action which triggered the restart, for example, settings download
Attempted use of illegitimate configuration software from %A1%	%A1%	IP address of the PC where the unauthorized SW was detected
Attempted download of invalid firmware file(s) from %A1%	%A1%	Source of the unauthorized configurations, for example, IP address of the PC
Attempted download of unauthorized configuration settings from %A1%	%A1%	Source of the unauthorized configurations, for example, IP address of the PC
Attempted download of unauthorized firmware file(s) from %A1%	%A1%	Source of the unauthorized firmware file(s), for example, IP address of the PC
Attempted download of invalid configuration settings from %A1%	%A1%	Source of the invalid configurations, for example, IP address of the PC
Attempted download of invalid configuration settings	–	–
Time-synchronization message is outside of the internal clock.	–	–

Alarm	Additional Information	
%A1%: hardware deviation %A2%: CFG: %A3% HW: %A4%	%A1%	Device name
	%A2%	Slot number or port name
	%A3%	Hardware information, for example, IO type If the hardware is not configured in DIGSI 5, %A3% is **missing**.
	%A4%	Hardware information, for example, IO type If there is no hardware, %A4% is **missing**.

9.5 Viewing the Logs

9.5.1 Windows Event Logs

Overview

As per the cybersecurity standard IEEE 1686, DIGSI 5 must log the security events in the Windows event log and these logs can be viewed via the **Event Viewer**. A node named **DIGSI 5** is displayed in the **Event Viewer**. A group named **DIGSI 5 SECAUD** is displayed under the **Groups** > **Local Users and Groups** node in the **Computer Management** window on your computer.

The events are logged for the following operations performed in DIGSI 5:

- Opening DIGSI 5
- Closing DIGSI 5
- Loading a configuration to the device
- Loading a firmware to the device
- Updating DAF (Device Attribute File) into the device
- Refreshing the device data
- Updating the configurations from the target device
- Copying the online device to the project

Viewing Windows Event Log Entries

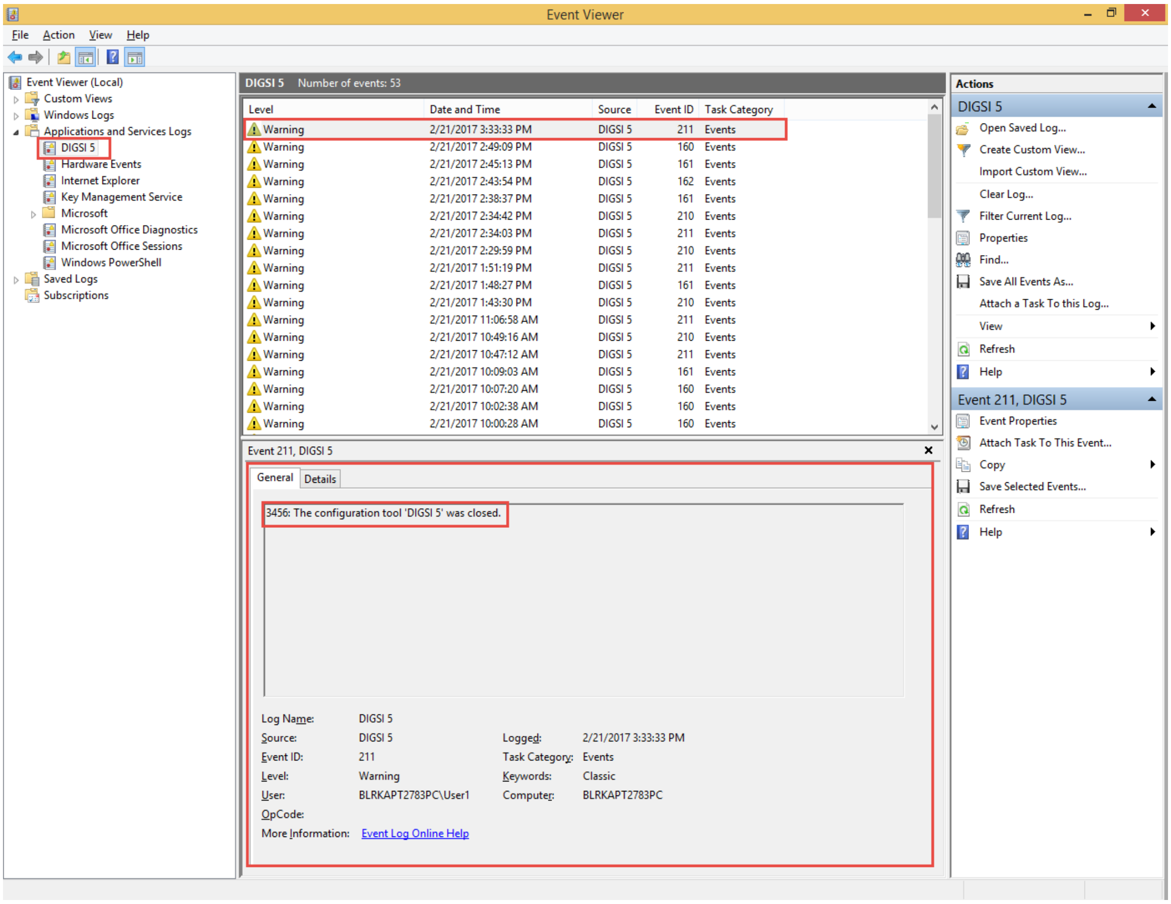
To view the entries of the Windows event log, proceed as follows:

✧ Click **Start** > **Control Panel** > **Administrative Tools** > **Event Viewer**.

- or -

✧ Select **Start** > **Run...** and enter **eventvwr** in the dialog.

✧ Click **OK**.
The **Event Viewer** dialog is displayed.



DIGSI 5 Number of events: 53

Level	Date and Time	Source	Event ID	Task Category
Warning	2/21/2017 3:33:33 PM	DIGSI 5	211	Events
Warning	2/21/2017 2:49:09 PM	DIGSI 5	160	Events
Warning	2/21/2017 2:45:13 PM	DIGSI 5	161	Events
Warning	2/21/2017 2:43:54 PM	DIGSI 5	162	Events
Warning	2/21/2017 2:38:37 PM	DIGSI 5	161	Events
Warning	2/21/2017 2:34:42 PM	DIGSI 5	210	Events
Warning	2/21/2017 2:34:03 PM	DIGSI 5	211	Events
Warning	2/21/2017 2:29:59 PM	DIGSI 5	210	Events
Warning	2/21/2017 1:51:19 PM	DIGSI 5	211	Events
Warning	2/21/2017 1:48:27 PM	DIGSI 5	161	Events
Warning	2/21/2017 1:43:30 PM	DIGSI 5	210	Events
Warning	2/21/2017 11:06:58 AM	DIGSI 5	211	Events
Warning	2/21/2017 10:49:16 AM	DIGSI 5	210	Events
Warning	2/21/2017 10:47:12 AM	DIGSI 5	211	Events
Warning	2/21/2017 10:09:03 AM	DIGSI 5	161	Events
Warning	2/21/2017 10:07:20 AM	DIGSI 5	160	Events
Warning	2/21/2017 10:02:38 AM	DIGSI 5	160	Events
Warning	2/21/2017 10:00:28 AM	DIGSI 5	160	Events

Event 211, DIGSI 5

3456: The configuration tool 'DIGSI 5' was closed.

Log Name:	DIGSI 5		
Source:	DIGSI 5	Logged:	2/21/2017 3:33:33 PM
Event ID:	211	Task Category:	Events
Level:	Warning	Keywords:	Classic
User:	BLRKAPT2783PC\User1	Computer:	BLRKAPT2783PC
OpCode:			
More Information:	Event Log Online Help		

[sc_event_viewer, 1, en_US]

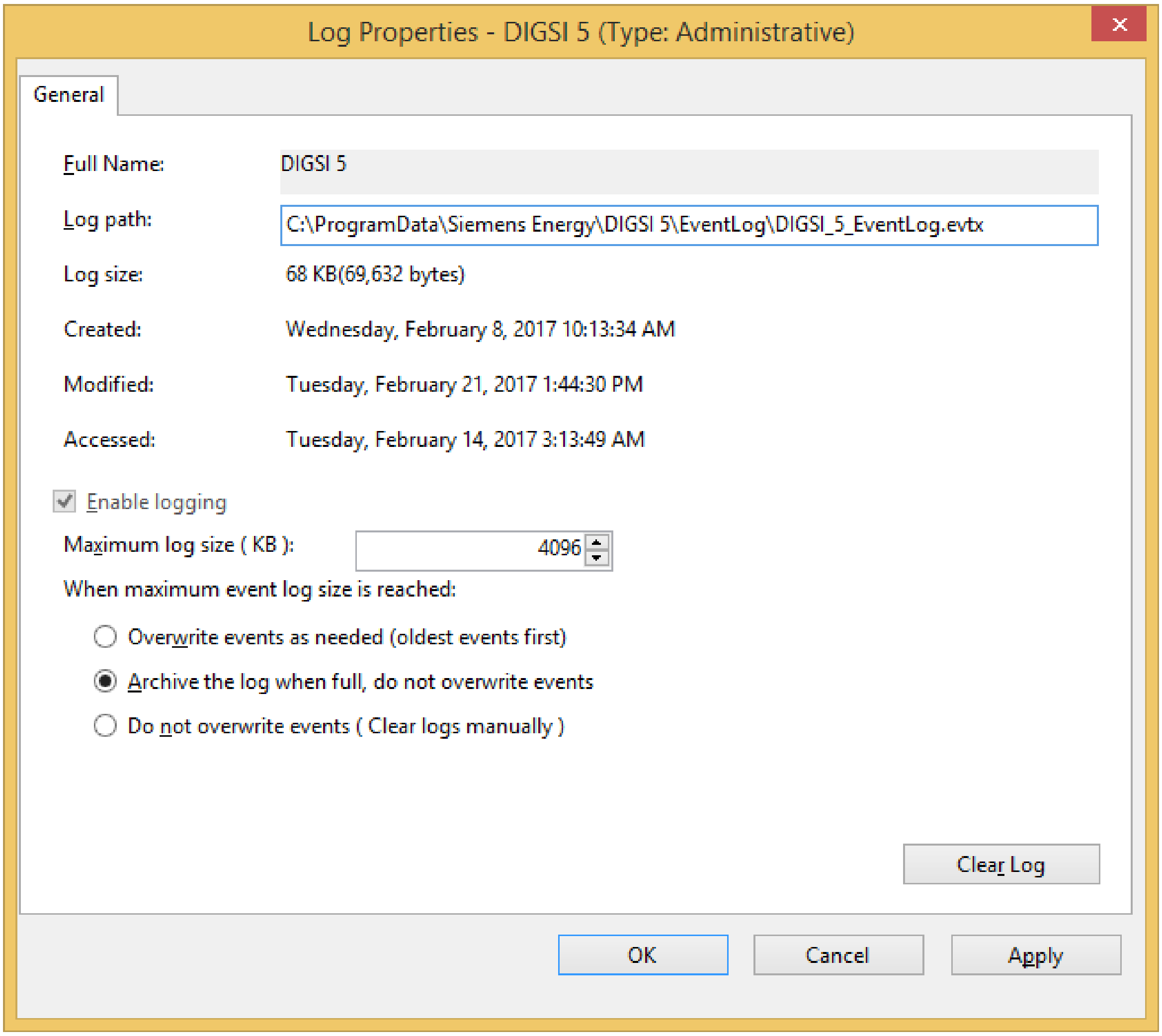
Figure 9-3 Event Viewer

The **General** tab displays the event properties and provides more information about the event logged. The event ID displayed in the figure is the process ID of the DIGSI instance for which the event is logged.

Viewing Log Properties – DIGSI 5

✧ In the **Event Viewer** window, under the **Applications and Services Logs** folder, right-click the **DIGSI 5** node and select **Properties** from the context menu.

The **Log Properties - DIGSI 5** dialog is displayed.



Full Name: DIGSI 5

Log path: C:\ProgramData\Siemens Energy\DIGSI 5\EventLog\DIGSI_5_EventLog.evtx

Log size: 68 KB(69,632 bytes)

Created: Wednesday, February 8, 2017 10:13:34 AM

Modified: Tuesday, February 21, 2017 1:44:30 PM

Accessed: Tuesday, February 14, 2017 3:13:49 AM

☑ Enable logging

Maximum log size (KB): 4096

When maximum event log size is reached:

○ Overwrite events as needed (oldest events first)

● Archive the log when full, do not overwrite events

○ Do not overwrite events (Clear logs manually)

[sc_event_viewer_properties, 1, en_US]

Figure 9-4 Event Viewer - DIGSI 5 Log Properties

By default, the event logs are saved in the following location:

`C:\ProgramData\Siemens Energy\DIGSI 5\EventLog\DIGSI_5_EventLog.evtx`

The maximum log-size capacity is 4096 KB.

If the maximum log size is reached, the option **Archive the log when full, do not overwrite events** is selected by default.

You can select the desired option as per your requirement.

9.5.2 Viewing Audit Logs

The access to areas of the device with restricted access rights is recorded in the security log. Unsuccessful and unauthorized access attempts are also recorded. Up to 2048 indications can be stored in the security log.

The logged indications are preconfigured and cannot be changed. You cannot delete the logs which are organized as a ring buffer. If you want to archive security-relevant information without loss of information, you must regularly view the logs.

Viewing Security Logs in DIGSI 5

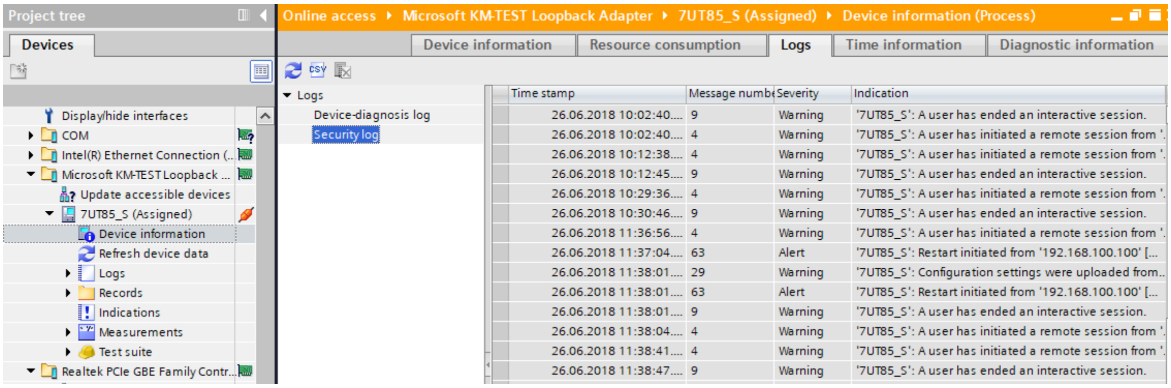
To access the security logs of your SIPROTEC 5 device in DIGSI 5, proceed as follows:

- In the project-tree window, navigate to **Project** > **Online access** > **Device** > **Device Information** > **Logs** > **Security logs**.

  The device must be in **Online access**.

- Click the button in the headline to refresh the contents.

  The state of the security logs that are last loaded from the device is displayed.



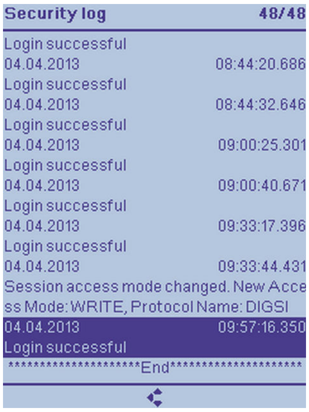
Time stamp	Message numb	Severity	Indication
26.06.2018 10:02:40....	9	Warning	'7UT85_S': A user has ended an interactive session.
26.06.2018 10:02:40....	4	Warning	'7UT85_S': A user has initiated a remote session from '.
26.06.2018 10:12:38....	4	Warning	'7UT85_S': A user has initiated a remote session from '.
26.06.2018 10:12:45....	9	Warning	'7UT85_S': A user has ended an interactive session.
26.06.2018 10:29:36....	4	Warning	'7UT85_S': A user has initiated a remote session from '.
26.06.2018 10:30:46....	9	Warning	'7UT85_S': A user has ended an interactive session.
26.06.2018 11:36:56....	4	Warning	'7UT85_S': A user has initiated a remote session from '.
26.06.2018 11:37:04....	63	Alert	'7UT85_S': Restart initiated from '192.168.100.100' [...
26.06.2018 11:38:01....	29	Warning	'7UT85_S': Configuration settings were uploaded from..
26.06.2018 11:38:01....	63	Alert	'7UT85_S': Restart initiated from '192.168.100.100' [...
26.06.2018 11:38:01....	9	Warning	'7UT85_S': A user has ended an interactive session.
26.06.2018 11:38:04....	4	Warning	'7UT85_S': A user has initiated a remote session from '.
26.06.2018 11:38:41....	4	Warning	'7UT85_S': A user has initiated a remote session from '.
26.06.2018 11:38:47....	9	Warning	'7UT85_S': A user has ended an interactive session.

[sc_secmld, 2, en_US]

Figure 9-5 Viewing the Security Logs in DIGSI 5

Viewing Security Logs via the Device Operation Panel

- With the device operation panel, navigate to **Main** > **Test & diagnosis** > **Logs** > **Security log**.
- You can browse within the displayed indication list using the navigation keys (up/down) on the device operation panel.



```
Security log                     48/48
Login successful
04.04.2013                08:44:20.686
Login successful
04.04.2013                08:44:32.646
Login successful
04.04.2013                09:00:25.301
Login successful
04.04.2013                09:00:40.671
Login successful
04.04.2013                09:33:17.396
Login successful
04.04.2013                09:33:44.431
Session access mode changed. New Acce
ss Mode: WRITE, Protocol Name: DIGSI
04.04.2013                09:57:16.350
Login successful
********************End*********************
```

[sc_seclog, 1, en_US]

Figure 9-6 Viewing the Security Log on the Device Operation Panel

10 Resetting the Device Configuration

10.1 Security Credentials and Configuration Reset

10.1.1 Downloading the Secure Credential and Configuration Reset File (SCRF)

NOTE

Backup and store the SCRF at a secure location when commissioning the device, because anyone is able to use this file.

Only the user accounts which are assigned with the role SECADM or Administrator have the authority to download the SCRF from a device.

Downloading the SCRF File

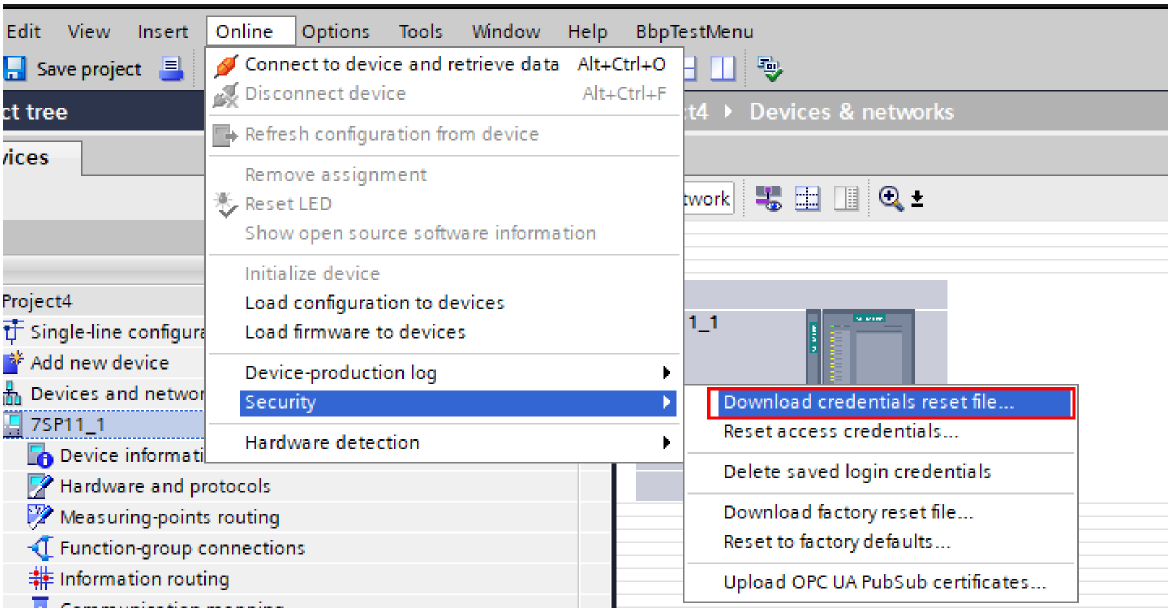
✧ Connect the SIPROTEC 5 device to a PC using a network cable.

✧ Start DIGSI 5.

✧ Select the device and activate the RBAC feature.

✧ Open the **Online** menu item.

✧ Select **Security** -> **Download credentials reset file...**.


Edit
View
Insert
Online
Options
Tools
Window
Help
BbpTestMenu
Save project
ct tree
vices
Project4
Single-line configura
Add new device
Devices and networ
7SP11_1
Device informati
Hardware and protocols
Measuring-points routing
Function-group connections
Information routing
Connect to device and retrieve data Alt+Ctrl+O
Disconnect device Alt+Ctrl+F
Refresh configuration from device
Remove assignment
Reset LED
Show open source software information
Initialize device
Load configuration to devices
Load firmware to devices
Device-production log
Security
Hardware detection
t4 ▸ Devices & networks
twork
1_1
Download credentials reset file...
Reset access credentials...
Delete saved login credentials
Download factory reset file...
Reset to factory defaults...
Upload OPC UA PubSub certificates...

[sc_download_scrf, 2, en_US]

Figure 10-1 Downloading the SCRF File

✧ Select a storage location on the PC, such as D:\Siprotec5SecurityData.

✧ Confirm the action with **OK**.

10.1.2 Resetting Security Settings

If the connection to the authentication server is broken or the emergency access has not been configured, you can reset the device security settings to regain interactive access to the devices where RBAC is activated.

Before resetting the security settings, you need to consider the following points:

- Each device has a unique SCRF.
  An SCRF file can only be used to reset the security settings of the device from which the SCRF is downloaded.
- You must handle the SCRF with care at all times and prevent unauthorized access to these files.
  Because regardless the assigned role(s), everyone can reset the security settings of a device by uploading the SCRF file into the device. For this reason, the SCRF must be effectively deleted from the PC after resetting.
- The SCRF can always be used to reset the security settings.

How to Reset Security Settings

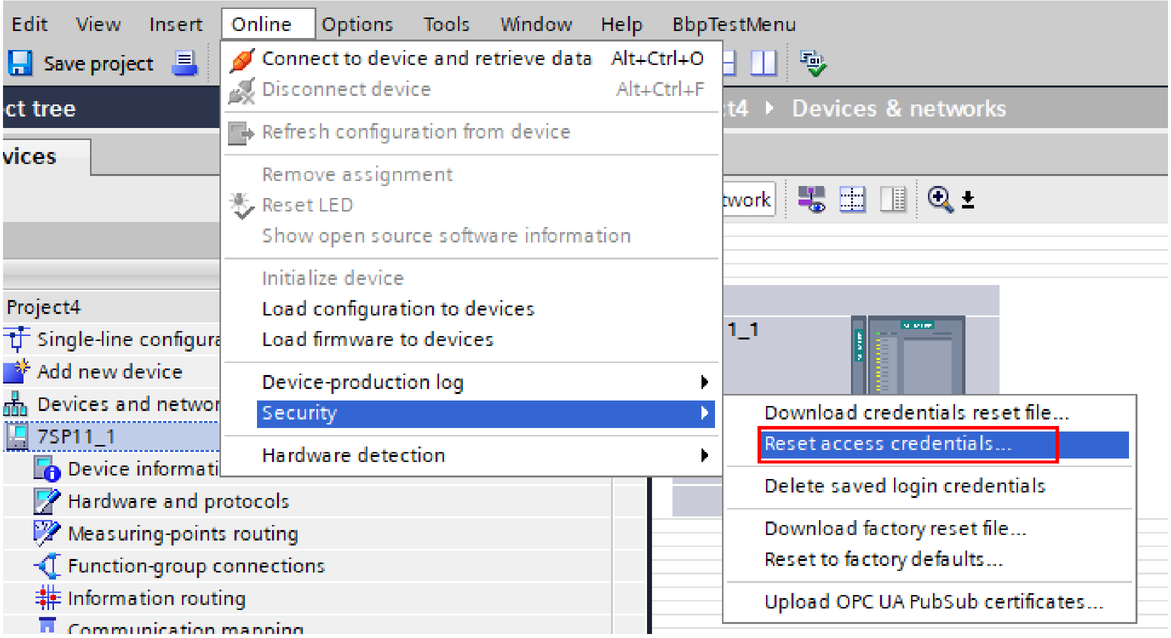
✧ Save the SCRF on the PC.

✧ Connect the SIPROTEC 5 device to a PC using a network cable.

✧ Start DIGSI 5.

✧ Select the device and open the **Online** menu item.

✧ Select **Security** > **Reset access credentials...**.



[sc_upload_scrf_en, 1, en_US]

Figure 10-2 Uploading the SCRF File

✧ Transfer the SCRF file to the device.

When successful, DIGSI shows an information and all security settings are inactive in the SIPROTEC 5 device.

NOTE

On the device operation panel and the browser-based user interface, the security settings will not be refreshed after the SCRF is successfully uploaded. To refresh the settings, a reboot is needed. But to avoid impacting the protection functions, the device does not restart automatically. You can select to restart the device according to the actual situation.

10.2 Secure Factory Reset

10.2.1 Downloading the Secure Factory Reset File (SFRF)

To return a SIPROTEC 5 device to its factory default state, you must first download the signed SFRF file from the device.

NOTE

Backup and store the SFRF file at a secure location when commissioning the device, because anyone is able to use this file.

The security administrator role is required for configuring the factory default state.

Downloading the SFRF File

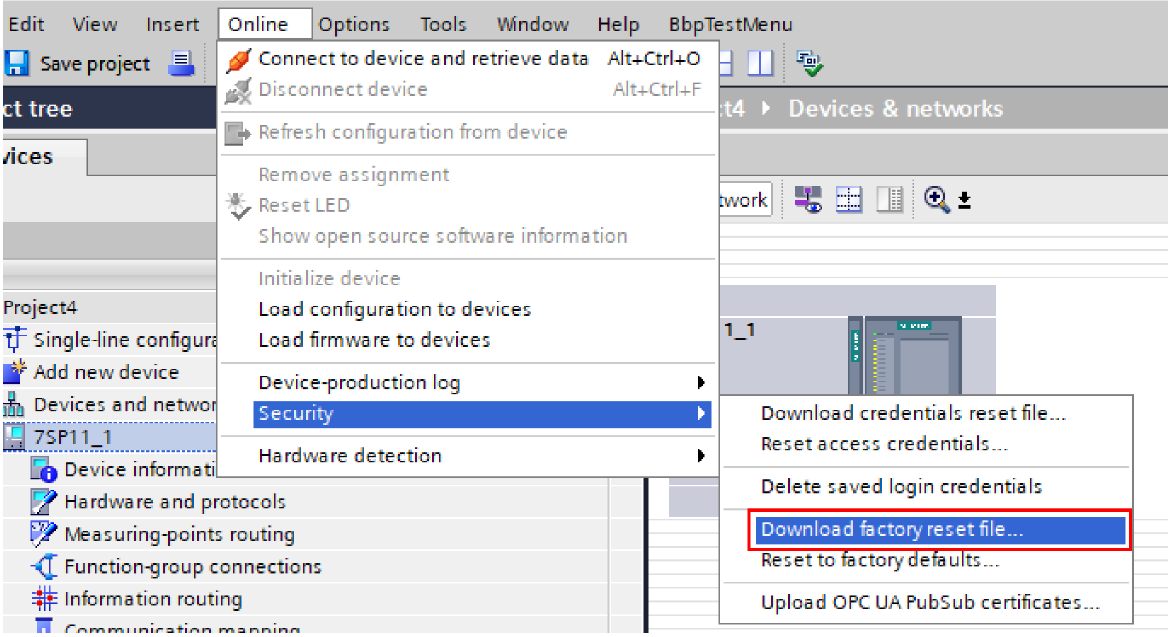
✧ Connect the SIPROTEC 5 device to a PC using a network cable.

✧ Start DIGSI 5.

✧ Select the device and activate the RBAC feature.

✧ Select the device and open the **Online** menu item.

✧ Select **Security** > **Download factory reset file...**.



[sc_download_sfrf, 2, en_US]

Figure 10-3 Downloading the SFRF File

✧ Select a storage location on the PC, for example, D:\Siprotec5SecurityData.

✧ Confirm the action with **OK**.

✧ Back up and store the signed SFRF file at a secure location.

10.2.2 Resetting to the Factory Default State

If the factory default state must be restored, you can restore this state by uploading the SFRF file into the device.

Before resetting the security settings, you need to consider the following points:

- Each device has a unique SFRF.
  An SFRF file can only be used to reset the security settings of the device from which the SCRF is downloaded.
- You must handle the SFRF with care at all times and prevent unauthorized access to these files.
  Because regardless the assigned role(s), everyone can reset a device to its factory default state by uploading the SFRF into it. For this reason, the SFRF must be effectively deleted from the PC after resetting.
- The SFRF can always be used to reset the SIPROTEC 5 device to its factory default state.

How to Reset to Factory Defaults

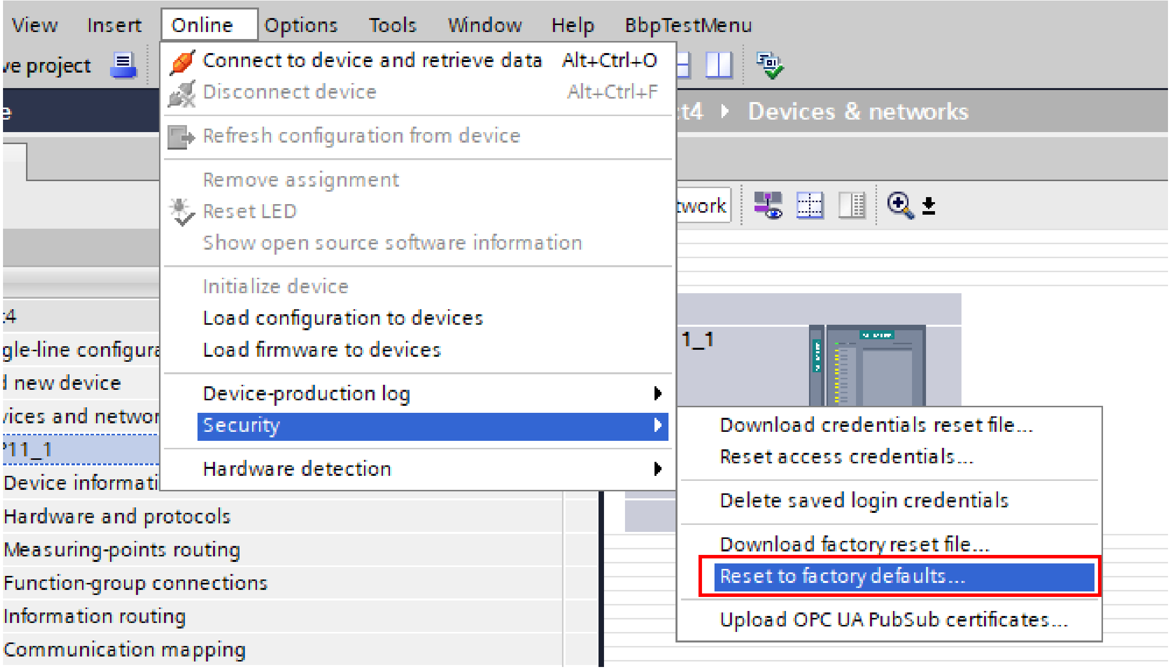
✧ Save the SFRF on the PC.

✧ Connect the SIPROTEC 5 device to a PC using a network cable.

✧ Start DIGSI 5.

✧ Select the device and open the **Online** menu item.

✧ Select **Security** > **Reset to factory defaults...**.


View
Insert
Online
Options
Tools
Window
Help
BbpTestMenu
ve project
Connect to device and retrieve data Alt+Ctrl+O
Disconnect device Alt+Ctrl+F
Refresh configuration from device
Remove assignment
Reset LED
Show open source software information
Initialize device
Load configuration to devices
Load firmware to devices
Device-production log
Security
Hardware detection
t4 ▸ Devices & networks
twork
1_1
:4
gle-line configura
l new device
vices and networ
'11_1
Device informati
Hardware and protocols
Measuring-points routing
Function-group connections
Information routing
Communication mapping
Download credentials reset file...
Reset access credentials...
Delete saved login credentials
Download factory reset file...
Reset to factory defaults...
Upload OPC UA PubSub certificates...

[sc_SFRF, 1, en_US]

✧ Transfer the SFRF file to the device.

After restarting the device, the factory default settings are restored.

NOTE

All data on the device as well as the security and protection settings are cleared upon loading the SFRF file.

11 Security Patch Management

11.1 General

The patch-management process is in accordance to chapter 2.1.1.3 of the *BDEW Whitepaper Guidelines*.

The overall system should allow the patching of all system components during normal system operation. Installation of a patch should be possible without interruption of normal system operations and with little impact on the availability of the system. For example, a complete shutdown of the primary generation, transmission or distribution systems should not be necessary to install updates on secondary systems. Preferentially, the patches will be installed on passive redundant components first. After a switchover process (change of the active component in the redundant system) and a subsequent test, the patch will be installed on the remaining components.

A patch-management process for the entire system should be supported. This process should manage the testing, installation, and documentation of security patches and system updates. In general, it should be possible that the operational crew who administers the systems also installs the patches and updates. Installation and uninstallation of patches and updates should be authorized by the system owner and should not be performed automatically.

11.2 SIPROTEC 5 Patch Management

To ensure that the SIPROTEC 5 devices use the latest firmware, you can download and update all firmware files for these devices individually.

When updating a firmware, the concerned device is not operational. If you cannot accept an interruption of normal operations, use redundant systems to ensure uninterrupted operations.

For the SIPROTEC 5 product development, Siemens has a patch-management process under which all firmware releases, as well as the accompanying enhancements, are documented in a traceable manner.

11.3 DIGSI 5 Patch Management

You can update the DIGSI 5 installations with maintenance releases and hotfixes.

For the DIGSI 5 development, Siemens has a patch-management process. All included releases, enhancements, and software-error fixes are documented in a traceable manner. Security updates for the third-party components used by DIGSI 5 (for example, Windows operating system) are also tested within this framework and released for DIGSI 5. Siemens offers updates free of charge.

From V3.00 on, DIGSI 5 can indicate if a disabled device driver has been installed. The system operator or the service technician responsible for the system maintenance usually performs the corresponding installation. You can find more information on security vulnerability-related updates to SIPROTEC 5 in *www.siemens.com/cert/advisories*.

12 Data Privacy Considerations

Siemens considers data privacy aspects related to power systems operations while designing and developing the SIPROTEC 5 products. The consideration is reflected in the following technical measures which are realized in the SIPROTEC 5 products.

Table 12-1 Data Privacy Considerations

Requirements	Remarks
Access control to personal data in the products	The security log contains information on security-relevant operations. If you activate RBAC in the device, this logged information also indicates the login name of the person who carried out the operations. Access control in the device ensures that the security log can only be accessed by authenticated and authorized users that are in the role of a SECAUD or an Administrator.
Compulsory use of passwords	Accessing to the security log which logs the person-identifiable information (PII) compulsorily requires the user in the role of a SECAUD or an Administrator to logon to the device with the correct password.
Proportionate encryption of data in rest and data in motion	The way that the SIPROTEC 5 device provides data encryption is the state-of-the-art in the protection device market.
Automatic log-off functions	After a deterministic time of inactivity, the device automatically logs off the logged-on users.
Deletion possibility	You can delete the security-log entries from the device by resetting the device to factory defaults. You can delete the local user cache by deactivating the local user cache feature in the device. You can find more information in chapter *3.2.4 User Cache Size*.
Two-factor authentication, if necessary	The device is not intended for direct access from a remote location, for example, over the Internet or other unprotected networks. Therefore, two-factor authentication is not necessary. But in two-factor authentication systems such as RSA SecureID, a physical token generator generates one-time passwords (OTP) for the centrally managed account of a user. These OTPs can be used to log on to SIPROTEC 5 devices.
Additional information on product-specific measures	PII is only captured and stored in the security log if RBAC is enabled. The login information (user name, password, and role) of the already logged-on users is locally stored in the device only if you enable the RBAC user-cache feature. You can delete all PII by the following steps: ● Firstly, delete the local user cache by deactivating the local user cache feature in the device. ● Secondly, delete the log entries from the device by resetting the device to factory defaults.

NOTE

Siemens advises you to consider the responsibilities of your organization towards fulfilling the GDPR requirements. For more information, refer to article 25 **Data protection by design and by default** of the GDPR *https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf*.

A Appendix

A.1 Signals for Security

DIGSI 5 provides the following signals to help you investigate security-related activities.

No.	Information	Purpose
DIGSI 5 path: Target project > **Information routing** > **Security** > **Security Logging** > **Sec. Ev. Logg.**		
_:2761:19021:501	>Binary info 1	These binary input signals are for the logging of user-defined events. For more information, refer to *9.3.3 Customizable Logged Events*.
_:2761:19021:502	>Binary info 2	
_:2761:19021:503	>Binary info 3	
_:2761:19021:504	>Binary info 4	
_:2761:19021:505	>Binary info 5	
_:2761:19021:506	>Binary info 6	
_:2761:19021:507	>Binary info 7	
_:2761:19021:508	>Binary info 8	
_:2761:19021:300	Capacity warning	If you route this signal, once the stored log entries increase to the set threshold of the parameter **Security log cap. warn.**, the signal is issued.
_:2761:19021:301	User logged out	A user terminates an interactive session.
_:2761:19021:302	User log. out (time-out)	An interactive session is terminated due to timeout.
_:2761:19021:303	Login failed	Login failed.
_:2761:19021:304	Login failed - blocked	A user is blocked due to multiple failed login-attempts.
_:2761:19021:305	User logged in	A user logs on successfully.
_:2761:19021:306	Subst. process data	A user manually overwrites the real data.
_:2761:19021:307	Control operation	A user takes a control operation.
_:2761:19021:308	Download conf.	Configurations have been downloaded from the device.
_:2761:19021:309	Upload configuration	Configurations have been uploaded to the device.
_:2761:19021:310	Configuration changed	Device configurations have been changed.
_:2761:19021:311	Firmware update	The device firmware has been updated.
_:2761:19021:312	Password changed	The password of an account has been changed.
_:2761:19021:313	Password deleted	The password of an account has been deleted.
_:2761:19021:314	Security log viewed	The audit log has been viewed.
_:2761:19021:315	Security log downl.	The audit log has been downloaded from the device.
_:2761:19021:316	Date/time changed	The date or time of the device has been changed.
_:2761:19021:319	Device reboot	The device has been rebooted.
_:2761:19021:320	Inv. firmw/config. upl.	The uploaded configurations or firmware settings are invalid, for example, the SIPROTEC 5 device signature is invalid.
_:2761:19021:321	Time synchr. failure	Time synchronization failed.

No.	Information	Purpose
DIGSI 5 path: Target project > **Information routing** > **Device**		
_:321	Cyber Security state	This indicates the status of a login that is established with a connection password: • *Login blocked* The **Connection password** is blocked as a user enters wrong connection passwords for more than 5 times. • *Login reactivated* The **Connection password** is activated again. For more information on the **Connection password**, refer to *3.1 Access Control with Connection Password*.
_:322	Cyber-security event	This signal group contains the following signals: • *PW change OK* Succeed to change the connection password • *PW change not OK* Failed to change the connection password • *Login OK* Succeed to log on • *Login not OK* Failed to log on • *PW activation OK* Succeed to activate the password • *PW activation not OK* Failed to activate the password • *PW deactivation OK* Succeed to deactivate the password • *PW deactivation n. OK* Failed to deactivate the password

Literature

/1/ *DIGSI 5 Online Help*
C53000-D5040-C001

/2/ *System Hardening for Substation Automation and Protection*
E50417-H8940-C619

/3/ *SIPROTEC 5, Operation*
C53000-D5040-C003

Glossary

Index