SIEMENS

SIPROTEC 5
Sicherheit

V08.01

Handbuch

Vorwort

Open Source Software

Inhaltsverzeichnis

1 Einführung

2 Measures for System Hardening

3 Access Control in SIPROTEC 5 and DIGSI 5

4 Malware Protection

5 Communication Security

6 Certificate Management

7 Backup and Restore

8 Security Logging

9 Securely Resetting the Device Configuration

10 Security Patch Management

Literaturverzeichnis

Glossar

Stichwortverzeichnis

C53000-H5000-C081-2



HINWEIS

Beachten Sie zu Ihrer eigenen Sicherheit die Warn- und Sicherheitshinweise in diesem Dokument, sofern vorhanden.

Haftungsausschluss

Änderungen und Irrtümer vorbehalten. Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden.

Dokumentversion: C53000-H5000-C081-2.03

Ausgabestand: 12.2019

Version des beschriebenen Produkts: V08.01

Copyright

Copyright © Siemens AG 2019. Alle Rechte vorbehalten.

Weitergabe sowie Vervielfältigung, Verbreitung und Bearbeitung dieses Dokuments, Verwertung und Mitteilung des Inhaltes sind unzulässig, soweit nicht schriftlich gestattet. Alle Rechte für den Fall der Patenterteilung, Geschmacks- oder Gebrauchsmustereintragung sind vorbehalten.

Marken

SIPROTEC™, DIGSI™, SIGRA™, SIGUARD™, SAFIR™ SICAM™ und MindSphere™ sind Marken der Siemens AG. Jede nicht autorisierte Verwendung ist unzulässig. Alle anderen Bezeichnungen in diesem Dokument können Marken sein, deren Verwendung durch Dritte für ihre eigenen Zwecke die Rechte des Eigentümers verletzen kann.

Vorwort

Zweck des Handbuchs

Dieses Handbuch beschreibt die Sicherheitsmerkmale zu den SIPROTEC 5-Geräten sowie DIGSI 5, z.B:

- Grundlegend sichere Konfiguration
- Sicherheitsbezogene Geräteeinstellungen, Parameter für Security-Funktionen und Standardwerte
- Maßnahmen zur Systemhärtung
- Matrix zur Kommunikationsschnittstelle
- Anweisungen für sicherheitsbewusstes Verhalten, z.B. Systemsicherung und Systemwiederherstellung
- Erläuterungen zu sicherheitsspezifischen Protokoll- und Audit-Meldungen, möglichen Ursachen und geeigneten Gegenmaßnahmen. Diese Informationen können als Basis für ein sicheres Design und einen sicheren Betrieb des gesamten Systems verwendet werden.

HINWEIS

Die Systemmerkmale aus einer systemspezifischen Vernetzung und die Konfiguration von Produkten in einem System sind in diesem Handbuch nicht beschrieben.

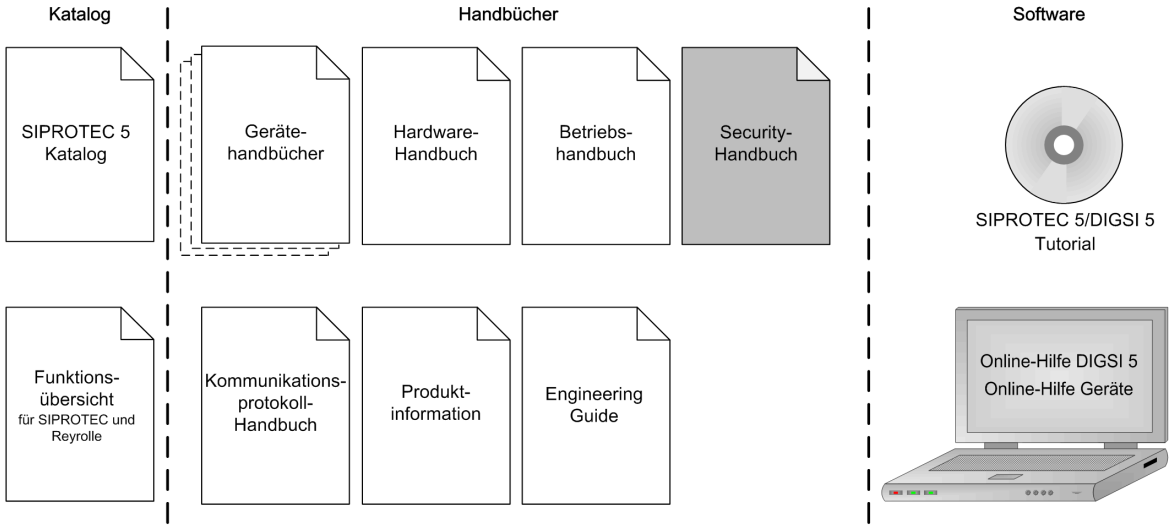
Zielgruppe

Schutzingenieure, Inbetriebsetzer, Personen, die mit der Einstellung, Prüfung und Wartung von Automatik-, Selektivschutz- und Steuerungseinrichtungen betraut sind sowie Betriebspersonal in elektrischen Anlagen und Kraftwerken.

Gültigkeitsbereich

Dieses Handbuch ist gültig für Produkte von SIPROTEC 5 und DIGSI 5 mit Hardware- und Firmware-Version V08.01.

Weiterführende Dokumentation



[dw_pref_sip5_security, 1, de_DE]

- Security-Handbuch
  Das Security-Handbuch beschreibt die Sicherheitsmerkmale von SIPROTEC 5-Geräten und DIGSI 5.
- Gerätehandbücher
  Gerätehandbücher beschreiben die Funktionen und Applikationen eines spezifischen SIPROTEC 5-Gerätes. Das gedruckte Handbuch und die Geräte-Online-Hilfe haben dieselbe Informationsstruktur.
- Hardware-Handbuch
  Das Hardware-Handbuch beschreibt die Hardware-Bausteine und Gerätekombinationen der SIPROTEC 5-Gerätefamilie.
- Betriebshandbuch
  Das Betriebshandbuch beschreibt die Grundprinzipien und -prozeduren des Gerätebetriebs und die Montage der Geräte für die SIPROTEC 5-Gerätefamilie.
- Kommunikationsprotokoll-Handbuch
  Das Kommunikationsprotokoll-Handbuch enthält eine Beschreibung der Protokolle zur Kommunikation innerhalb der SIPROTEC 5-Gerätefamilie und zu übergeordneten Leitstellen.
- Produktinformation
  Die Produktinformation enthält allgemeine Informationen über betriebsvorbereitende Bedingungen. Dieses Dokument wird mit jedem SIPROTEC 5-Gerät ausgeliefert.
- Engineering Guide
  Der Engineering Guide beschreibt die wesentlichen Schritte beim Engineering mit DIGSI 5. Zusätzlich erfahren Sie im Engineering Guide, wie Sie eine projektierte Konfiguration in ein SIPROTEC 5-Gerät laden und die Gerätefunktionalität des SIPROTEC 5-Gerätes aktualisieren.
- Online-Hilfe DIGSI 5
  Die Online-Hilfe DIGSI 5 enthält ein Hilfepaket für DIGSI und CFC.
  Das Hilfepaket für DIGSI 5 enthält die Beschreibung des Grundbetriebs von Software, der DIGSI-Prinzipien und der Editoren. Das Hilfepaket für CFC enthält eine Einführung in die CFC-Programmierung, Grundbeispiele für die CFC-Handhabung und ein Referenzkapitel mit allen für die SIPROTEC 5-Gerätefamilie verfügbaren CFC-Bausteinen.
- SIPROTEC 5/DIGSI 5 Tutorial
  Das Tutorial auf der DVD enthält eine kurze Information über wichtige Produktmerkmale, detaillierte Informationen zu den einzelnen Fachgebieten sowie Betriebssequenzen mit praxisorientierten Aufgaben und einer kurzen Erläuterung.

- SIPROTEC 5 Katalog
  Der SIPROTEC 5-Katalog beschreibt die SIPROTEC 5-Systemeigenschaften.
- Funktionsübersicht SIPROTEC und Reyrolle
  Die Funktionsübersicht liefert einen Überblick der Siemens Schutzgeräte sowie eine Geräteauswahltabelle.

Angaben zur Konformität

CE

Das Produkt entspricht den Bestimmungen des Rates der Europäischen Gemeinschaften zur Angleichung der Rechtsvorschriften der Mitgliedstaaten betreffend die elektromagnetische Verträglichkeit (EMV-Richtlinie 2014/30/EU) sowie elektrische Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen (Niederspannungsrichtlinie 2014/35/EU).

Diese Konformität ist das Ergebnis einer Bewertung, die durch die Siemens AG gemäß den Richtlinien in Übereinstimmung mit der Norm EN 60255-26 für die EMV-Richtlinie und der Norm EN 60255-27 für die Niederspannungsrichtlinie durchgeführt worden ist.

Das Gerät ist für den Einsatz im Industriebereich entwickelt und hergestellt.

Das Erzeugnis steht im Einklang mit den internationalen Normen der Reihe IEC 60255 und der nationalen Bestimmung VDE 0435.

Normen

IEEE Std C 37.90

Das Produkt ist im Rahmen der Technischen Daten UL-zugelassen.

Weitere Informationen zur UL-Datenbank finden Sie unter: *ul.com*

Das Produkt finden Sie unter der Zulassungsnummer (**UL File Number**) **E194016**.

c UL US
LISTED

IND. CONT. EQ.
69CA

Weitere Unterstützung

Bei Fragen zum System wenden Sie sich an Ihren Siemens-Vertriebspartner.

Customer Support Center

Unser Customer Support Center unterstützt Sie rund um die Uhr.

Siemens AG
Customer Support Center
Humboldtstraße 59
90459 Nürnberg
Germany
E-Mail: *support.energy@siemens.com*

Schulungskurse

Sie können das individuelle Kursangebot bei unserem Training Center erfragen:

Siemens AG
Siemens Power Academy TD
Humboldtstraße 59
90459 Nürnberg
Deutschland

Tel: +49 (911) 433-7415
Fax: +49 (911) 433-7929
E-Mail: *poweracademy@siemens.com*
Internet: *www.siemens.com/poweracademy*

Hinweise zu Ihrer Sicherheit

Dieses Dokument ist kein vollständiges Verzeichnis aller für einen Betrieb des Produkts erforderlichen Sicherheitsmaßnahmen. Es enthält aber Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise sind je nach Gefährdungsgrad wie folgt dargestellt:



GEFAHR

GEFAHR bedeutet, dass Tod oder schwere Verletzungen eintreten **werden**, wenn die angegebenen Maßnahmen nicht getroffen werden.

✧ Beachten Sie alle Hinweise, um Tod oder schwere Verletzungen zu vermeiden.



WARNUNG

WARNUNG bedeutet, dass Tod oder schwere Verletzungen eintreten **können**, wenn die angegebenen Maßnahmen nicht getroffen werden.

✧ Beachten Sie alle Hinweise, um Tod oder schwere Verletzungen zu vermeiden.



VORSICHT

VORSICHT bedeutet, dass mittelschwere oder leichte Verletzungen eintreten **können**, wenn die angegebenen Maßnahmen nicht getroffen werden.

✧ Beachten Sie alle Hinweise, um mittelschwere oder leichte Verletzungen zu vermeiden.

ACHTUNG

ACHTUNG bedeutet, dass Sachschäden entstehen **können**, wenn die angegebenen Maßnahmen nicht getroffen werden.

✧ Beachten Sie alle Hinweise, um Sachschäden zu vermeiden.



HINWEIS

ist eine wichtige Information über das Produkt, die Handhabung des Produktes oder den jeweiligen Teil der Dokumentation, auf den besonders aufmerksam gemacht werden soll.

Open Source Software

Dieses Produkt beinhaltet unter anderem auch Open Source Software, die von Dritten entwickelt wurde. Die in diesem Produkt enthaltene Open Source Software und die entsprechenden Open-Source-Software-Lizenzbedingungen finden Sie in der Readme_OSS. Die Open-Source-Software-Programme sind urheberrechtlich geschützt. Sie sind berechtigt, die Open Source Software gemäß den jeweiligen Open-Source-Software-Lizenzbedingungen zu nutzen. Bei Widersprüchen zwischen den Open-Source-Software-Lizenzbedingungen und den für das Produkt geltenden Siemens Lizenzbedingungen gelten in Bezug auf die Open Source Software die Open-Source-Software-Lizenzbedingungen vorrangig. Die Open Source Software wird unentgeltlich überlassen. Den Quelltext der Software können Sie – soweit die einschlägigen Open-Source-Software-Lizenzbedingungen dies vorsehen – gegen Zahlung der Versandkosten bei Ihrem Siemens Vertriebsbeauftragten zumindest bis zum Ablauf von 3 Jahren ab Erwerb des Produkts anfordern. Wir haften für das Produkt einschließlich der darin enthaltenen Open Source Software entsprechend den für das Produkt gültigen Lizenzbedingungen. Jegliche Haftung für die Nutzung der Open Source Software über den von uns für das Produkt vorgesehenen Programmablauf hinaus sowie jegliche Haftung für Mängel, die durch Änderungen der Open Source Software verursacht wurden, ist ausgeschlossen. Wir leisten keine technische Unterstützung für das Produkt, wenn dieses geändert wurde.

Mit DIGSI 5 haben Sie im Online-Modus die Möglichkeit, über das Hauptmenü **Open Source Software Information anzeigen** die Readme_OSS-Datei mit den Original-Lizenztexten und Copyright-Hinweisen aus dem Gerät auszulesen und anzeigen zu lassen.

Dazu sind folgende Schritte notwendig:

- Wechseln Sie in den Online-Modus.
- Wählen Sie das Gerät aus.
- Selektieren Sie **Online** in der Menüleiste.
- Klicken Sie auf **Open Source Software Information anzeigen**.



HINWEIS

Zum Auslesen der Readme_OSS-Datei muss auf dem Rechner ein PDF-Viewer installiert sein.

Um SIPROTEC 5-Geräte in Betrieb nehmen zu können, ist eine gültige DIGSI 5-Lizenz erforderlich.

Inhaltsverzeichnis

Vorwort ... **3**

Open Source Software ... **7**

1 Einführung ... **13**

1.1 Ziel ... 14

1.2 Beachtung von Normen ... 15

1.3 Sicherheitsanforderungen ... 16

2 Measures for System Hardening ... **17**

2.1 Übersicht ... 18

2.2 Vorgesehene Betriebsumgebung ... 19

2.3 Supported LAN Services ... 20

2.3.1 Verzeichnis der erforderlichen offenen Ports ... 20

2.3.2 Deaktivierung unnötiger System- und Kommunikationsdienste ... 20

2.3.3 Diagnose-Homepage ... 21

2.4 Maßnahmen zur Härtung ... 22

3 Access Control in SIPROTEC 5 and DIGSI 5 ... **23**

3.1 Access Control with Connection Password ... 24

3.1.1 Einleitung ... 24

3.1.2 Einstellung des Verbindungspasswortes ... 24

3.1.3 Authentifizierung und Verbindungspasswort während des Betriebs ... 25

3.1.4 Verbindungspasswort zurücksetzen und deaktivieren ... 25

3.2 Role-Based Access Control (RBAC) in SIPROTEC 5 ... 27

3.2.1 Übersicht ... 27

3.2.2 Hilfswerkzeuge ... 28

3.2.3 Einstellungen des RADIUS-Servers ... 28

3.2.4 Parameter für den RADIUS-Server ... 30

3.2.5 Anmeldeversuche ... 30

3.2.6 Benutzerpuffergröße ... 31

3.2.7 Sicherheitseinstellungen laden ... 31

3.2.8 Grundlegende Eigenschaften der Zuweisung von Rechten und unterstützten Rollen ... 33

3.2.9 Benutzernamen an der Bedieneinheit des Gerätes ... 36

3.2.10 Anmeldung am Gerät über die Bedieneinheit des Gerätes ... 37

3.3 Rollenbasierte Ansichten in DIGSI 5 ... 39

3.4 Notfallzugang ... 43

4 Malware Protection ... **45**

4.1 Übersicht ... 46

4.2 Malware-Schutz für Engineering-Software ... 47
4.3 Integritätsprüfung der heruntergeladenen Datei ... 48

5 Communication Security ... 49
5.1 Zugriffsbeschränkungen für Ethernet anwenden ... 50
5.2 DIGSI 5 Client-Authentifizierung ... 51
5.2.1 Allgemeine Informationen ... 51
5.2.2 Konfiguration ... 52
5.2.2.1 DIGSI 5 CA-Store einrichten ... 52
5.2.2.2 Konfiguration der Sicherheitsfunktion DIGSI 5 Client-Authentifizierung ... 53
5.2.2.3 Verifizierung der konfigurierten CA über einen Web-Browser ... 54
5.2.2.4 Unbefugter Zugriff mit DIGSI 5 auf SIPROTEC 5-Geräte ... 55
5.2.2.5 Wiederherstellung nach einer Sperrung über sicheres Zurücksetzen der Anmeldedaten ... 56
5.3 Sicherheit von Interaktionen zwischen Web-Browser und Gerät ... 58

6 Certificate Management ... 61
6.1 Einleitung ... 62
6.2 Zertifikate im Einsatz ... 64
6.3 Zertifizierungsstellen ... 65
6.4 Angeforderte Zertifikate ... 66

7 Backup and Restore ... 67
7.1 Allgemein ... 68
7.2 Archivieren und Dearchivieren eines Projekts ... 69

8 Security Logging ... 73
8.1 Übersicht ... 74
8.2 Unterstützte System- und Firmware-Versionen ... 75
8.3 Logged Security Events ... 76
8.3.1 Aufbau von Sicherheitsereignissen ... 76
8.3.2 Syslog-Ereignisse SIPROTEC 5 ... 76
8.4 Configuration ... 90
8.4.1 Übersicht ... 90
8.4.2 Windows Ereignisprotokoll ... 95
8.5 Auditberichte anzeigen ... 98

9 Securely Resetting the Device Configuration ... 101
9.1 Security Credentials and Configuration Reset ... 102
9.1.1 Herunterladen der Datei zum Rücksetzen der Sicherheitsanmeldedaten und Konfiguration (SCRF) ... 102
9.1.2 Sicherheitseinstellungen zurücksetzen ... 102
9.2 Secure Factory Reset ... 104
9.2.1 Herunterladen der Datei zum sicheren Zurücksetzen auf Werkseinstellungen (SFRF) ... 104
9.2.2 Zurücksetzen auf die Werkseinstellungen ... 104

10 Security Patch Management ... 107
10.1 Allgemein ... 108
10.2 SIPROTEC 5 Patch-Management ... 109
10.3 DIGSI 5 Patch-Management ... 110

Literaturverzeichnis **111**

Glossar **113**

Stichwortverzeichnis **115**

1 Einführung

1.1	Ziel	14
1.2	Beachtung von Normen	15
1.3	Sicherheitsanforderungen	16

1.1 Ziel

In der Vergangenheit waren Rechner funktionelle Inseln mit wenig oder gar keiner Anknüpfung an andere Geräte. Heute sind alle Rechen-Server, Desktop-Rechner und Automatisierungseinheiten miteinander verknüpft.

Einerseits schafft dieser Zustand neue Geschäftsmöglichkeiten. Andererseits können diese verknüpften Komponenten angegriffen werden, z.B. Anwendungen, die nicht für den Einsatz in stark vernetzten Umgebungen vorgesehen sind.

Der wichtigste Aspekt dieses Handbuches ist der wachsende Einsatz folgender Technologien:

- Rangierbare Standardprotokolle, z.B. IP und TCP
- Verbindung von in der Vergangenheit isolierten Netzwerken, z.B. Gegenstationen
- Standard-Software-Komponenten, z.B. OEM-Betriebssysteme (Original Equipment Manufacture - Originalhersteller) wie Windows

Das Handbuch bietet Empfehlungen für die sichere Inbetriebnahme und den sicheren Betrieb von SIPROTEC 5-Geräten in vernetzten Umgebungen.

1.2 Beachtung von Normen

Die von Siemens angebotenen Produkte und Technologien berücksichtigen die führenden Normen für die Cyber-Security. Die wesentlichen Grundlagen für sichere Infrastrukturen sind Normen und Richtlinien wie IEC 62443, IEC 62351, BDEW Whitepaper, IEEE 1686 und NERC CIP (Critical Infrastructure Protection).

1.3 Sicherheitsanforderungen

Die wichtigsten Sicherheitsanforderungen sind:

- Authentifizierung und Autorisierung der Benutzer
- Sicherstellung der Integrität der übertragenen Daten
- Schutz gegen Viren, Trojaner und andere Schadprogramme
- Sammlung und Speicherung von Protokolldateien
- Betrieb des Systems in einer geschützten Umgebung (physische Sicherheit)
- Jeder Benutzer erhält nur die Rechte, die für seine entsprechende Aufgabe erforderlich sind.
- Sicherstellung, dass eine Wiederherstellung nach einem Systemausfall ohne oder nur mit geringen Datenverlusten möglich ist
- Aktivierung nur der erforderlichen Dienste und Ports
- Die Netzlast kritischer Systeme ist begrenzt auf das Maß, mit dem die Systeme unter Volllast weiterarbeiten. So wird z.B. die Anzahl von Broadcasts in den Netzkomponenten begrenzt.

2 Measures for System Hardening

2.1	Übersicht	18
2.2	Vorgesehene Betriebsumgebung	19
2.3	Supported LAN Services	20
2.4	Maßnahmen zur Härtung	22

2.1 Übersicht

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt die Härtung bei der IT-Sicherheit als "[...] die Entfernung aller Software-Komponenten und -funktionen, die für die Erfüllung der gewünschten Aufgabe durch ein Programm nicht unbedingt erforderlich sind."
In der Praxis erfüllen Härtungsmaßnahmen folgende Ziele:

- Reduzierung der Möglichkeiten zur Ausnutzung von Schwachstellen
- Minimierung möglicher Angriffsmethoden
- Ausschluss eines Angreifers von verfügbaren Werkzeugen im Fall eines erfolgreichen Angriffs
- Minimierung der verfügbaren Rechte des Angreifers im Fall eines erfolgreichen Angriffs
- Erhöhung der Wahrscheinlichkeit der Entdeckung eines erfolgreichen Angriffs

Eine Reduzierung der Komplexität und der Wartungsarbeiten am System ist in diesem Sinne ein sekundäres Ziel der Härtung, das die Handhabbarkeit verbessert und somit Verwaltungsfehler minimiert.

2.2 Vorgesehene Betriebsumgebung

Siemens empfiehlt das Einspielen der zur Verfügung gestellten Sicherheitsupdates über die entsprechenden Werkzeuge und dokumentierten Vorgehensweisen, die mit dem Produkt verfügbar sind. Das Einspielen der Sicherheitsupdates über mehrere Produktinstanzen hinweg kann auch automatisch erfolgen, wenn dies im Funktionsumfang des Produkts enthalten ist.

Siemens empfiehlt die Validierung aller Sicherheitsupdates vor dem Einspielen und die Überwachung des Aktualisierungsvorgangs in der Zielumgebung durch geschultes Personal.

Als generelle Sicherheitsmaßnahme empfiehlt Siemens, den Netzwerkzugriff mit angemessenen Maßnahmen zu schützen (z.B. mit Firewalls, Segmentierung, VPN).

Siemens empfiehlt, die Umgebung gemäß den Betriebsrichtlinien zu konfigurieren, damit die Geräte in einer geschützten IT-Umgebung betrieben werden. Die empfohlenen Sicherheitsrichtlinien für sichere Unterstationen finden Sie unter *https://www.siemens.com/gridsecurity*.

Die folgenden Annahmen oder Randbedingungen gelten für die vorgesehene Betriebsumgebung, in denen die SIPROTEC 5-Geräte gemäß Empfehlungen in diesem Handbuch eingesetzt werden.

Tabelle 2-1 Annahmen oder Randbedingungen hinsichtlich Sicherheit

Annahmen und Randbedingungen
Die Kommunikation der Leitstelle mit dem SIPROTEC 5-Gerät erfolgt nicht direkt.
Remote-Ethernet-Verbindungen zu Unterstationen sind über VPN oder TLS gesichert.
Die Unterstation ist physikalisch gesichert (Sicherheitszone).
In den SIPROTEC 5-Geräten ist Role-Based Access Control (RBAC) aktiviert.
Der Zeit-Server ist konfiguriert und die Gerätezeit wurde synchronisiert.
Die DIGSI 5-Instanzen verwenden für den Aufbau der TLS-Verbindung zu SIPROTEC 5-Geräten von Ihrer CA zugelassene Client-Zertifikate. Weitere Informationen hierzu siehe Kapitel *5.2 DIGSI 5 Client-Authentifizierung*.
Das Protokoll OPC UA PubSub für die IoT-Konnektivität wird auf einem Kommunikationsmodul aktiviert, das keine andere prozesskritische Kommunikation unterstützt, z.B., GOOSE/SV.

2.3 Supported LAN Services

2.3.1 Verzeichnis der erforderlichen offenen Ports

Tabelle 2-2 Verzeichnis der erforderlichen offenen Ports

Dienst	Layer 4-Protokoll	Layer 7-Protokoll	Typischer Client	Client-Port	Typischer Server	Server-Port	Mainboard	Kommunikationsmodul
DIGSI 5-Protokoll zum Automation License Manager	TCP	DIGSI 5-Protokoll zum Automation License Manager	DIGSI 5-PC	4410 (Standardwert)	Automation License Manager auf einem separaten Server, d.h. lokalen Host	4410 (Standardwert)	–	–
DIGSI 5-Protokoll zu SIPROTEC 5	TCP	HTTPS	DIGSI 5-PC	>1024	SIPROTEC 5	443	X	X
Reporting/ IEC 61850/MMS	TCP	IEC 61850	IEC 61850-Client (z.B. SICAM PAS, SICAM A8000)	>1024	SIPROTEC 5	102	X	X
Zeitsynchronisation/SNTP	UDP	SNTP	SIPROTEC 5	123	SNTP-Server	123	X	X
Überwachung über Simple Network Management Protocol (SNMPv3)	UDP	SNMPv3	PC mit SNMP-Client (z.B. SICAM PAS/ 1703/DIGSI 5-PC/ Remote DIGSI 5-PC)	>1024	SIPROTEC 5	161	–	X
DNP3i	TCP	DNP3 TCP	SICAM PAS	20000 oder nächster freier Port	SIPROTEC 5	20000	–	X
Synchrophasor	TCP UDP	–	Phasor-Datenkonzentrator	>1024	SIPROTEC 5	4712 4713	–	X
MODBUS TCP	TCP	MODBUS	Stationsleitgerät	>1024	SIPROTEC 5	502	–	X
Thermobox	UDP	RTD	Thermobox	>1024	SIPROTEC 5	Kann konfiguriert werden	X	X
Syslog-Client	UDP	–	SIPROTEC 5	–	Syslog-Server	514	X	X
RADIUS-Client	UDP	–	SIPROTEC 5	–	RADIUS-Server	1812	X	X
OPC UA	TCP	MQTT	SIPROTEC 5	–	Broker	8883	–	X
Web-Dienst	TCP	HTTPS	Web Browser	–	SIPROTEC 5	4443	X	X

Weitere Informationen zu den unterstützten Kommunikationsprotokollen finden Sie im SIPROTEC 5-Handbuch Kommunikationsprotokolle.

2.3.2 Deaktivierung unnötiger System- und Kommunikationsdienste

Nach Empfang der gelieferten Geräte müssen Sie die Geräte zuerst initialisieren. Erst danach sind die Geräte betriebsbereit.

Standardmäßig ist nur die Verbindung zu DIGSI 5 im Gerät aktiviert. Alle andere Ethernet-Dienste und -Ports sind im Gerät standardmäßig deaktiviert und können mit DIGSI 5 aktiviert werden. Durch die sichere Standardkonfiguration gibt es keine offene Schnittstelle für mögliche Angreifer und im Netzwerk sind nur die Dienste aktiviert, die auch verwendet werden.

Nicht erforderliche Dienste können Sie im Gerät jederzeit mit DIGSI 5 deaktivieren.

2.3.3 Diagnose-Homepage

Siemens empfiehlt, die Dienste der Diagnose-Homepage für Handlungen auf dem Mainboard und den Kommunikationsmodulen nach der Inbetriebnahme zu deaktivieren, da die Diagnose-Dienste weder HTTPS noch die Zugriffskontrolle unterstützen. Weitere Informationen zur Homepage siehe DIGSI 5 Online-Hilfe.

2.4 Maßnahmen zur Härtung

Folgende Maßnahmen zur Systemhärtung kommen zur Anwendung:

- Härtung des Windows-Systems
  Die Härtung des Windows-Systems muss gemäß dem Handbuch System Hardening for Substation Automation and Protection (Systemhärtung für Stationsautomatisierung und Schutz) erfolgen. Dieses Handbuch finden Sie auf *https://www.siemens.com/gridsecurity* unter **Downloads Cyber Security** → **Manuals** → **Secure Substation - Manual**.
- Deinstallation oder Deaktivierung unnötiger Software-Komponenten, z.B. Meldungssimulation und Prüfwerkzeuge für Datenfluss
- Deaktivierung unnötiger System- und Kommunikationsdienste, z.B. Fernbedienung und Fernwartung
- Deaktivierung unnötiger Benutzerkonten
- Aktivierung von Einstellungen zur Verbesserung der Sicherheit
- Beschränkung der Rechte von Benutzern und Programmen



HINWEIS

Eine Sammlung der Härtungsanleitungen für verschiedene Betriebssysteme, Server-Dienste und Standardapplikationen finden Sie z.B. beim Center for Internet Security unter *http://www.cisecurity.org*.

3 Access Control in SIPROTEC 5 and DIGSI 5

3.1	Access Control with Connection Password	24
3.2	Role-Based Access Control (RBAC) in SIPROTEC 5	27
3.3	Rollenbasierte Ansichten in DIGSI 5	39
3.4	Notfallzugang	43

3.1 Access Control with Connection Password

3.1.1 Einleitung

SIPROTEC 5-Geräte unterstützen die Benutzerauthentifizierung und Funktionen für den Zugriffsschutz auf sicherheitsrelevante Handlungen und Funktionen. Sie können zwischen der zentralen Role-Based Access Control (RBAC) und dem gerätespezifischen DIGSI 5-Verbindungspasswort wählen.

Wenn Sie die RBAC-Funktion nicht nutzen möchten, dann richten Sie die Geräte so ein, dass eine Benutzerauthentifizierung mit Abfrage des Passworts erfolgt.

Wenn RBAC deaktiviert ist, können Sie zusätzlich Bestätigungscodes einrichten, um unbeabsichtigte sicherheitskritische Aktionen auf dem Gerät zu verhindern. Weitere Informationen zum Bestätigungscode siehe SIPROTEC 5 Betriebsanleitung.

3.1.2 Einstellung des Verbindungspasswortes

Das Verbindungspasswort erfüllt den NERC-CIP-Standard (North American Electric Reliability Critical Infrastructure Protection) und besteht aus folgenden Teilen:

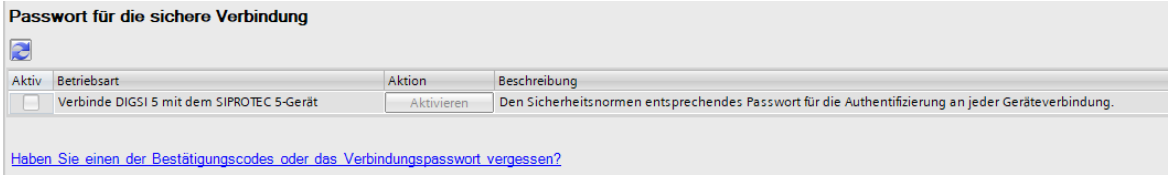
- Kleinbuchstaben
- Großbuchstaben
- Ziffern
- Sonderzeichen, z.B. %, &, $

Das Verbindungspasswort ist 8 bis 24 Zeichen lang. DIGSI 5 prüft die Länge bei der Eingabe.

Standardmäßig ist das Verbindungspasswort leer. Bei der Eingabe eines neuen Verbindungspasswortes werden die vorhandenen Zeichen versteckt mit Sternchen gezeigt. Geben Sie das Passwort zur Bestätigung 2 Mal ein. Diese Bestätigung vermeidet fehlerhafte Eintragungen.

HINWEIS

Das Deaktivieren des Verbindungspasswortes bedeutet, dass alle Benutzer über DIGSI 5 oder die Browserbasierte Benutzeroberfläche ohne Authentifizierung unbeschränkten Zugriff auf das Gerät haben. Wenn Sie dies verhindern wollen, setzen Sie das Verbindungspasswort im Gerät.



[sc_ConntPsw, 1, de_DE]

Bild 3-1 Einstellfenster für das Verbindungspasswort

Nach Eingabe eines neuen Verbindungspasswortes leitet DIGSI 5 dieses automatisch an das Gerät weiter.

Die Initialisierung des Verbindungspasswortes ist nur über die USB-Schnittstelle auf der Vorderseite oder über eine Ethernet-Schnittstelle des Gerätes möglich. In beiden Fällen wird das eingegebene Verbindungspasswort sicher über das TLS-Protokoll an das Gerät übertragen. Das Verbindungspasswort wird weder im DIGSI 5-Projekt noch woanders auf dem Windows-PC gespeichert. Es wird als Hash-Wert mit Salt im Gerät hinterlegt.

Ein weiterer Zugang zum Gerät (über DIGSI 5 oder die browserbasierte Benutzeroberfläche) ist nach dem Initialisieren des Verbindungspasswortes nur möglich, wenn Sie das korrekte Verbindungspasswort in den Dialog von DIGSI 5 eingeben, während die Verbindung mit dem Gerät hergestellt wird. Dieses Vorgehen verhindert einen nicht autorisierten Zugriff. Siemens empfiehlt, das Verbindungspasswort nach der Initialisierung zu überprüfen.

Sie können das Verbindungspasswort online über eine Ethernet-Verbindung ändern. Nach Eingabe des bisherigen Verbindungspasswortes und wiederholter Eingabe des neuen Verbindungspasswortes wird die Änderung im Gerät übernommen.

3.1.3 Authentifizierung und Verbindungspasswort während des Betriebs

Der 1. Ablauf zwischen DIGSI 5 und dem Gerät ist ein Authentifizierungsverfahren basierend auf dem TLS 1.2-Protokoll, in dem digitale Zertifikate zwischen DIGSI 5 und dem Gerät ausgetauscht werden. Dieses Verfahren gewährleistet, dass nur DIGSI 5 vollen technischen Zugang zu einem SIPROTEC 5-Gerät haben kann. Wenn andere Anwendungen zugreifen wollen, werden sie blockiert.

Nach der TLS-Authentifizierung fragt das SIPROTEC 5-Gerät das Verbindungspasswort ab, wenn Sie im Gerät ein Verbindungspasswort eingestellt haben.

Für den Zugriff auf das Gerät müssen Sie das richtige Verbindungspasswort eingeben. Die Eingabe eines falschen Passworts wird im Sicherheitsmeldepuffer aufgezeichnet. Bei fünfmaliger falscher Eingabe des Verbindungspasswortes wird der Zugriff auf das Gerät 5 Minuten lang blockiert. Auch diese Handlungen werden im Sicherheitsmeldepuffer des Gerätes aufgezeichnet.

Ein Sitzungsmanager in DIGSI 5 überwacht 30 Minuten lang alle Passwörter und die für die Identifikation relevanten Eingaben.

3.1.4 Verbindungspasswort zurücksetzen und deaktivieren

Wenn Sie die Einstellung des Verbindungspasswortes vor der Deaktivierung vergessen, müssen Sie es zurücksetzen.

Verbindungspasswort für Geräte mit Anzeige zurücksetzen

Gehen Sie wie folgt vor:

- ✧ Wechseln Sie im Hauptmenü des Gerätes zum Menü **Gerätefunktionen**.
- ✧ Rufen Sie den Menüeintrag **Sicherheit** → **PW zurücksetzen** auf.
- ✧ Bestätigen Sie das Rücksetzen des Passwortes mit dem Softkey **Ok**.

  – oder –
- ✧ Brechen Sie den Vorgang mit **Verlass.** ab.
- ✧ Geben Sie den Bestätigungscode **222222** ein und bestätigen Sie mit **Enter**.
- ✧ Geben Sie folgenden Tastaturkurzbefehl als Recovery-Code ein:
  <1>, <2>, <3>, <4>, <5>, <6>, <FN>+<1>, <FN>+<2>, <FN>+<3>, <FN>+<4>, <FN>+<5> und <FN>+<6>



HINWEIS

Beachten Sie, dass die Zeitüberschreitung zwischen den Tastenaktionen 1 s beträgt.

Verbindungspasswort für Geräte ohne Anzeige oder Geräte im Fallback-Modus zurücksetzen

Gehen Sie wie folgt vor:

- ✧ Schalten Sie das Gerät spannungslos.
- ✧ Entfernen Sie die Batterie des Gerätes und warten Sie 2 Minuten.
- ✧ Setzen Sie die Batterie in das Gerät ein.
- ✧ Schließen Sie das Gerät an die Spannungsversorgung an.

Das Verbindungspasswort ist zurückgesetzt.

Verbindungspasswort am Gerät deaktivieren

Gehen Sie wie folgt vor:

- ✧ Wechseln Sie im Hauptmenü des Gerätes zum Menü **`Gerätefunktionen`**.
- ✧ Rufen Sie den Menüeintrag **`Sicherheit`** → **`PW ein/ausschalt.`** auf.
- ✧ Geben Sie den Bestätigungscode **222222** ein.
- ✧ Deaktivieren Sie das Verbindungspasswort.



HINWEIS

Wenn die Gerätebatterie nicht mehr funktioniert oder entnommen wurde, wird das Verbindungspasswort nach dem Neustart des Gerätes deaktiviert.

Verbindungspasswort in DIGSI 5 deaktivieren

Gehen Sie wie folgt vor:

- ✧ Geben Sie in DIGSI 5 das korrekte Verbindungspasswort ein.

DIGSI 5 wird mit dem Gerät verbunden.

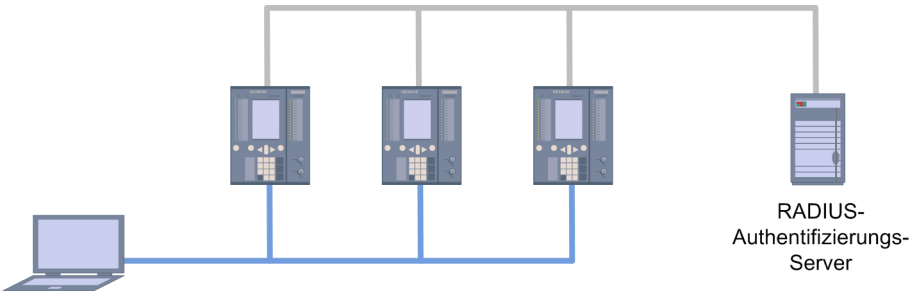
- ✧ Navigieren Sie zu **Gerät** -> **Sicherheit** → **Betriebssicherheits- und Zugriffskontrolle**.
- ✧ Entfernen Sie die Markierung für die Betriebsart **Verbinde DIGSI 5 mit dem SIPROTEC 5-Gerät** im Bereich **Passwort für die sichere Verbindung**.

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

3.2.1 Übersicht

Die RBAC-Funktion kann aktiviert werden, um den sicheren Zugriff auf ein SIPROTEC 5-Gerät zur Durchführung sicherheitsrelevanter Handlungen und Funktionen zu gewährleisten. Nach der Aktivierung werden alle Benutzer bei jedem Zugriffsversuch über ihre zentral verwalteten Benutzerkonten eindeutig authentifiziert.

Alle SIPROTEC 5-Geräte können an einen RADIUS[1]-Server angeschlossen werden, bei dem die Benutzerkonten und Autorisierungsdaten zentral verwaltet werden. RADIUS ist ein Client/Server-Protokoll. Die Client-Implementierung ist in der Firmware des SIPROTEC 5-Gerätes integriert.



[dw_authentication_server, 1, de_DE]

Bild 3-2 Authentifizierungsserver

Wenn sich ein Benutzer anmeldet, sendet das SIPROTEC 5-Gerät den Benutzernamen und das Passwort an den RADIUS-Server. Dieser prüft die Zugangsdaten des Benutzers und sendet bei erfolgreicher Authentifizierung die dem jeweiligen Benutzer zugeordneten Rollen an das SIPROTEC 5-Gerät zurück.

SIPROTEC 5-Geräte unterstützen RBAC mit vordefinierten, normbasierten Rollen. Benutzerkonten werden Rollen zugeordnet und diese Rollen erhalten Rechte entsprechend ihrer Funktionen. Die Zuweisung zwischen Benutzern und Rollen ist in der Konfiguration für den RADIUS-Server festgelegt. Die Zuweisung von Rechten zu Rollen ist in den Sicherheitseinstellungen des SIPROTEC 5-Gerätes vordefiniert.

SIPROTEC 5-Geräte erfüllen folgende Anforderungen:

- Standardrollen und Zuweisung von Rollen zu Rechten gemäß der Normen IEC 62351-8 und IEEE 1686
- Standardrollen und -rechte der Empfehlungen des BDEW-Whitepaper
- Zentrale Verwaltung von Benutzerkonten, Rollen und Verantwortungsbereichen (Area of Responsibility, AoR) auf einem RADIUS-Server
- Offline-/Notfallzugang zum Benutzerkonto bei Unerreichbarkeit des RADIUS-Servers

Sie können RBAC für ein SIPROTEC 5-Gerät mit DIGSI 5 aktivieren oder deaktivieren. Weitere Informationen hierzu siehe Kapitel *3.2.3 Einstellungen des RADIUS-Servers*.



HINWEIS

Wenn RBAC deaktiviert ist, können Sie das Gerät mit dem Verbindungspasswort gegen unbefugten Zugriff schützen und mit Bestätigungscodes können Sie ungewollte sicherheitskritische Aktionen verhindern. Weitere Informationen hierzu siehe Kapitel *3.1.4 Verbindungspasswort zurücksetzen und deaktivieren*.

1 RADIUS: Remote Authentication Dial-In User Service

3.2.2 Hilfswerkzeuge

RADIUS-Server

Die Hauptaufgaben des RADIUS-Servers sind die Benutzerauthentifizierung und die Verwaltung der Benutzerzugriffsrechte. Bei der Authentifizierung mit einem eindeutigen Benutzernamen und Passwort prüft der RADIUS-Server die Angaben des sich verbindenden Benutzers auf Richtigkeit.

Wenn der Benutzer eindeutig identifiziert wurde, weist die Autorisierung die Zugriffsrechte zu. Der Benutzer erhält die jeweiligen Zugriffsrechte auf Daten oder Dienste des SIPROTEC 5-Gerätes. Außerdem werden alle Zugriffsversuche für spätere Analysen aufgezeichnet (Audit-Trail).

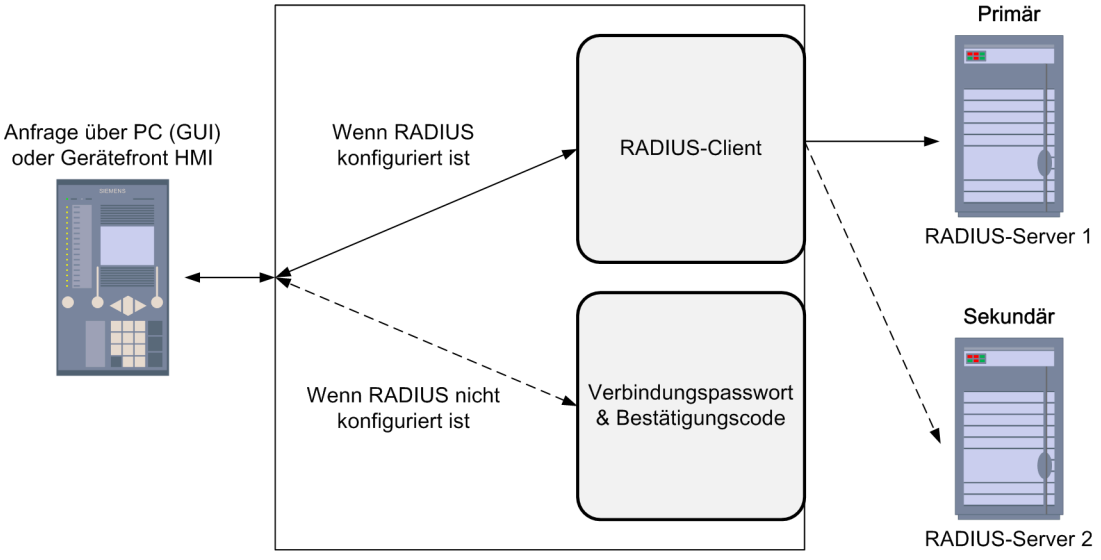
Folgende Informationen werden aufgezeichnet:

- Verbindungsversuche
- Benutzername und Rolleninformationen
- Zeitpunkt der Anmeldung

Weitere Informationen zu aufgezeichneten Sicherheitsereignissen siehe Kapitel *8.3.2 Syslog-Ereignisse SIPROTEC 5*.

3.2.3 Einstellungen des RADIUS-Servers

Vor der Aktivierung von RBAC müssen Sie folgende Einstellungen über DIGSI 5 vornehmen. Sie können bis zu 2 RADIUS-Server aktivieren.



[dw_connection_radius-server, 2, de_DE]

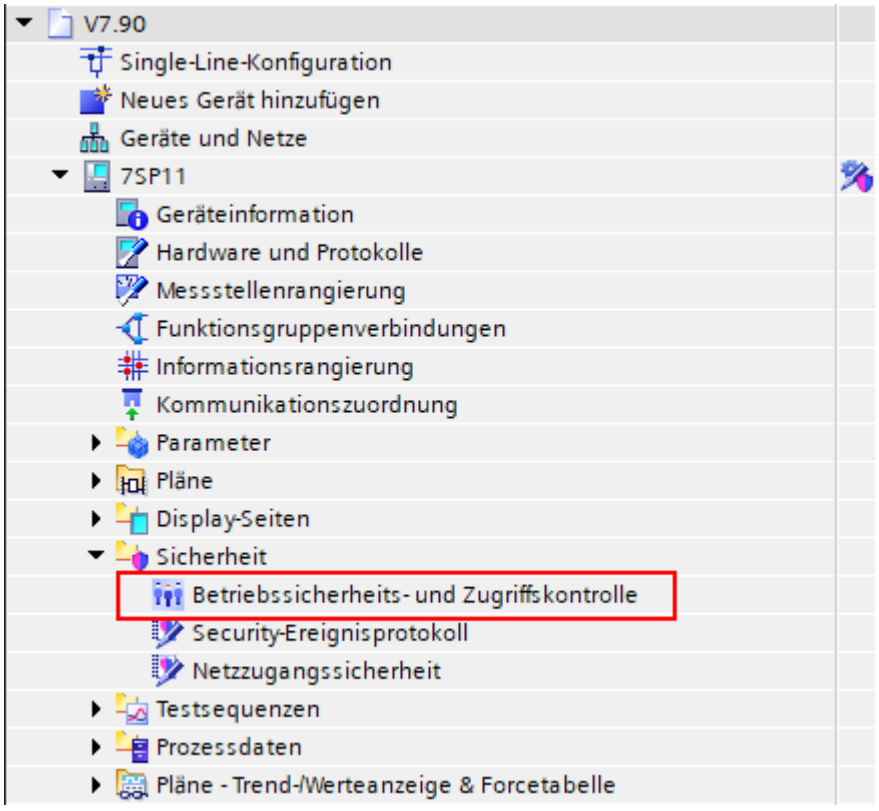
Bild 3-3 Verbindung zwischen Gerät und RADIUS-Server

RBAC aktivieren

✧ Öffnen Sie ein Projekt in DIGSI 5.

✧ Öffnen Sie in der Projektnavigation den Menüeintrag **Sicherheit**.

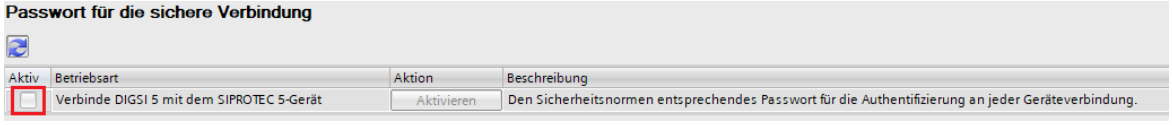
✧ Doppelklicken Sie auf den Menüeintrag **Betriebssicherheits- und Zugriffskontrolle**.



[sc_project-tree_rbac, 2, de_DE]

Bild 3-4 Projektnavigation

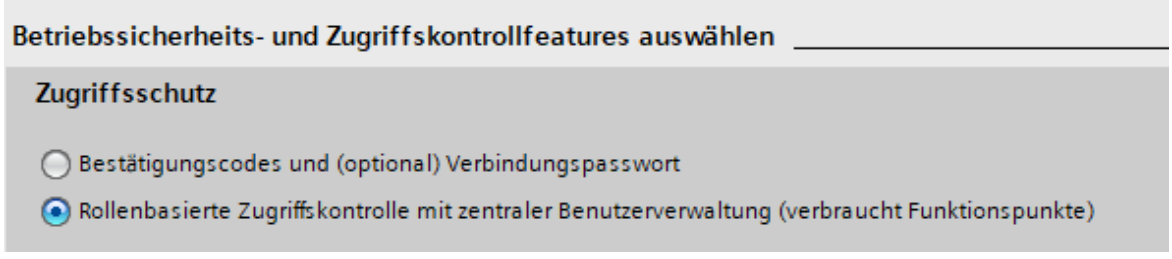
✧ Wenn das Verbindungspasswort im Bereich **Bestätigungscodes und Verbindungspasswort** aktiviert ist, muss es deaktiviert werden.



[sc_Deactivate_connection_password, 1, de_DE]

Bild 3-5 Verbindungspasswort deaktivieren

✧ Aktivieren Sie die RBAC-Funktion.



[sc_rbac_select, 3, de_DE]

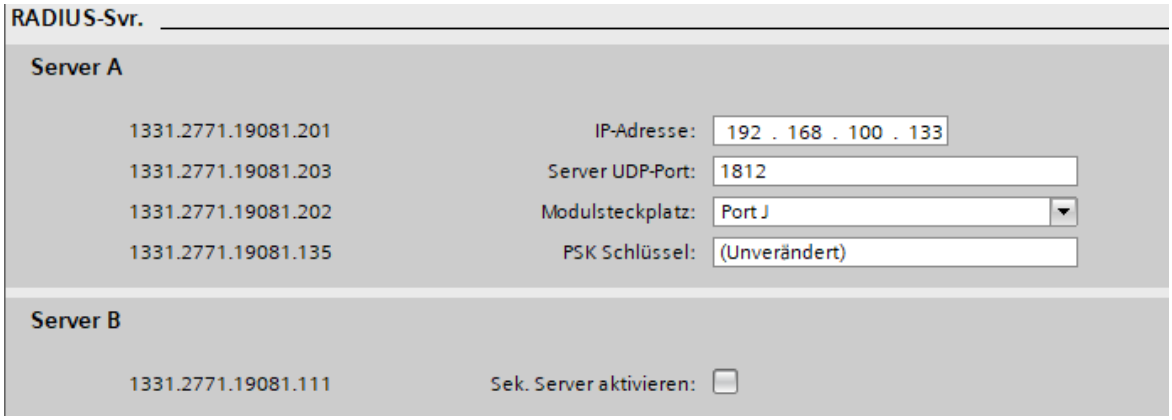
Bild 3-6 RBAC einschalten

HINWEIS

Beachten Sie, dass es nach der Aktivierung von RBAC kein Notfallkonto mehr gibt.

3.2.4 Parameter für den RADIUS-Server

Nehmen Sie zum Aufbau einer Verbindung zwischen dem SIPROTEC 5-Gerät und einem als Authentifizierungsserver fungierenden RADIUS-Server folgende Einstellungen in DIGSI 5 vor.



[sc_radius-server, 2, de_DE]

Bild 3-7 Konfigurationsbeispiel eines RADIUS-Servers in DIGSI 5

Parameter einstellen

- ✧ Geben Sie die **IP-Adresse** für Server A ein.
- ✧ Geben Sie den **Server UDP-Port** ein.
- ✧ Geben Sie an, welcher **Modulsteckplatz** verwendet wird.
- ✧ Geben Sie den **PSK-Schlüssel** ein, der mindestens 16 Zeichen lang ist.
- ✧ Aktivieren Sie bei Bedarf das Kontrollkästchen **Sek. Server aktiv** und geben Sie die Daten für einen 2. RADIUS-Server, Server B, ein.
- ✧ Geben Sie für Server B eine andere **IP-Adresse** als für Server A ein.
- ✧ Bei den Einstellungen gehen Sie wie bei Server A vor.

HINWEIS

Bei Verwendung eines neuen RADIUS-Servers muss beim alten und neuen RADIUS-Server der SECADM für das Konto identisch sein. Weitere Informationen zum SECADM des Kontos, siehe Kapitel *3.2.8 Grundlegende Eigenschaften der Zuweisung von Rechten und unterstützten Rollen*.

3.2.5 Anmeldeversuche

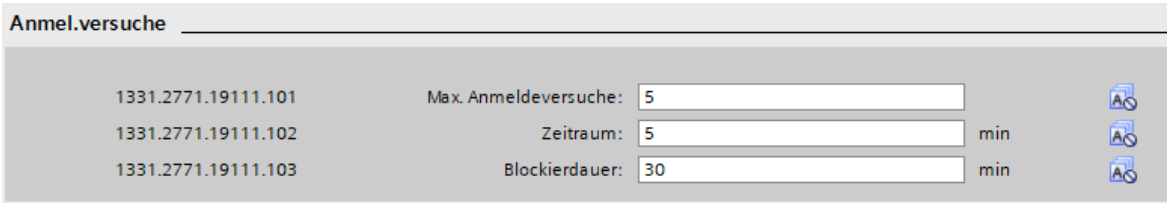
Folgende Parameter können Sie für die Handhabung falscher Anmeldeversuche konfigurieren:

- **`Max. Anmeldeversuche`**
  Mit diesem Parameter legen Sie die maximale Anzahl aufeinanderfolgender Anmeldeversuche für einen Benutzer fest.
- **`Zeitraum`**
  Mit diesem Parameter legen Sie den Zeitraum fest, nach dem die Anzahl der Anmeldeversuche nach dem letzten nicht erfolgreichen Versuch wieder zurück auf 0 gesetzt wird.

- **Blockierdauer**

  Mit diesem Parameter legen Sie die Zeitdauer fest, für die das Gerät nach Erreichen der maximalen Anzahl an Anmeldeversuchen blockiert wird.

  Bei einer Anmeldung mit falschen Zugangsdaten werden die Anmeldeversuche gezählt. Wenn die maximale Anzahl an Anmeldeversuchen erreicht wird, ist eine Anmeldung für die eingestellte **Blockierdauer** nicht möglich. Wenn diese **Blockierdauer** abgelaufen ist, können weitere Anmeldeversuche vorgenommen werden.



[sc_logon_attempts, 2, de_DE]

Bild 3-8 Anmeldeversuche

HINWEIS

Unter folgenden Bedingungen sind keine Anmeldeversuche möglich:

- Die Anmeldung wird blockiert.
- Die Gerätezeit ist nicht mit einem zentralen Zeit-Server synchronisiert und liegt vor der Gesamtzeit von Anmeldeblockierung und **Blockierdauer**.

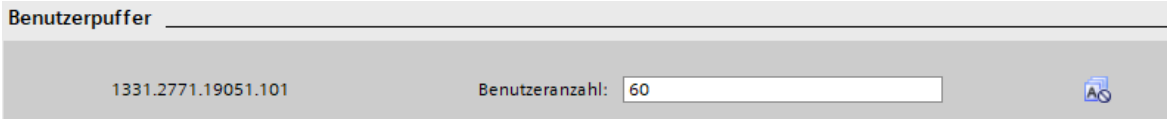
3.2.6 Benutzerpuffergröße

Bei Aktivierung der Benutzerpuffer-Funktion der RBAC speichert das Gerät die Anmeldedaten von Benutzern, die durch den RADIUS-Server erfolgreich authentifiziert wurden. Bei Unterbrechung der Verbindung des RADIUS-Servers können sich diese Benutzer mit den hinterlegten Anmeldedaten anmelden und das Gerät mit ihren hinterlegten Rollen bedienen. Bei erfolgreicher Anmeldung eines Benutzers aktualisiert das Gerät den entsprechenden Eintrag im Benutzerpuffer mit den neuesten Anmeldeinformationen (Benutzername und Passwort mit Hash) und der/den Rolle(n).

Mit dem Parameter **Benutzerpuffergröße** definieren Sie die maximale Anzahl hinterlegter Benutzerkonten. Der Benutzerpuffer kann durch Einstellen der Größe auf ***0*** deaktiviert werden.

HINWEIS

Wenn die SIPROTEC 5-Kommunikationsmodule zur RBAC-Authentifizierung verwendet werden, dann setzen Sie die Puffergröße auf mindestens ***1***.



[sc_rbac_user_cache, 2, de_DE]

Bild 3-9 Benutzerpuffereinstellungen

3.2.7 Sicherheitseinstellungen laden

Laden Sie die Sicherheitseinstellungen nach der erfolgten Konfiguration der RBAC in das SIPROTEC 5-Gerät.

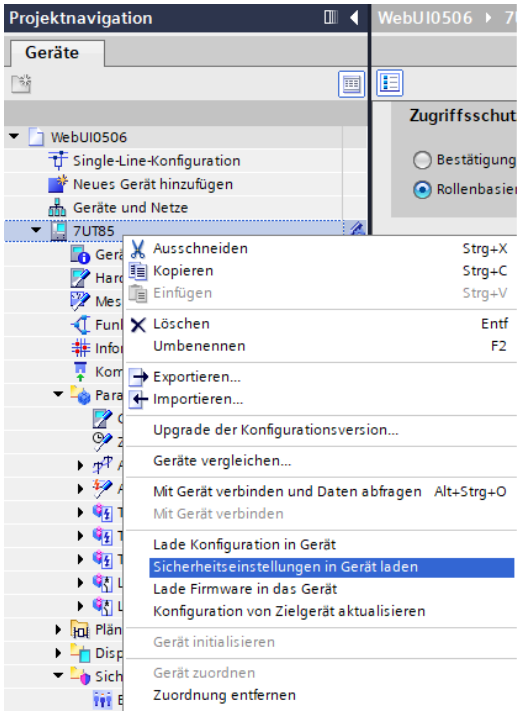
HINWEIS

Nur Benutzerkonten mit der Rolle SECADM oder Administrator sind berechtigt, Sicherheitseinstellungen in ein Gerät zu laden.

Laden der Sicherheitseinstellungen

Gehen Sie wie folgt vor:

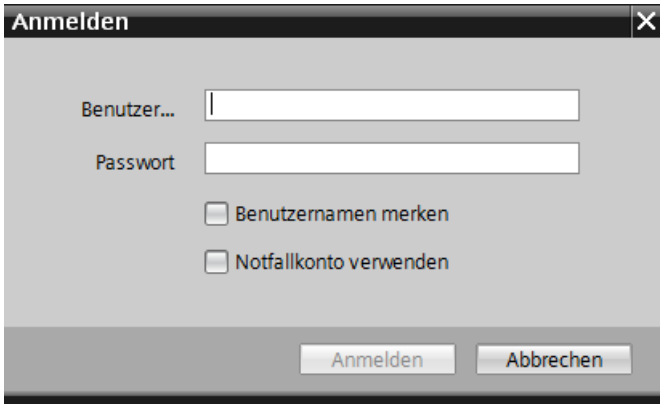
- ✧ Wählen Sie in der Projektnavigation das Gerät aus.
- ✧ Klicken Sie mit der rechten Maustaste auf das Gerät.
- ✧ Wählen Sie im geöffneten Kontextmenü **Sicherheitseinstellungen in Gerät laden**.



[sc_secutrans, 1, de_DE]

Bild 3-10 Menüauswahl Sicherheitseinstellungen in Gerät laden

Wenn RBAC aktiviert ist, erscheint der folgende Anmeldedialog:



[sc_logondev, 2, de_DE]

Bild 3-11 Am Gerät anmelden

- ✧ Geben Sie den **Benutzernamen** ein.

✧ Geben Sie das **Passwort** ein.

✧ Klicken Sie auf die Schaltfläche **Anmelden**.

Die Übertragung der Sicherheitseinstellungen in das Gerät beginnt. Wenn das Gerät die Sicherheitseinstellungen empfangen hat, prüft dieses die RADIUS-Servereinstellungen durch einen Authentifizierungsversuch mit dem eingegebenen Benutzernamen und dem Passwort. Das Gerät akzeptiert die Sicherheitseinstellungen nur, wenn die Authentifizierung erfolgreich war. Schließlich wird das Übertragungsergebnis angezeigt.

✧ Bestätigen Sie das Ergebnis mit **OK**.

Die Sicherheitseinstellungen wurden nun im Gerät aktiviert.

HINWEIS

Die Übertragung der Sicherheitseinstellungen funktioniert nur, wenn mindestens einer der konfigurierten RADIUS-Server erreichbar ist.

Wenn kein RADIUS-Server verfügbar ist, weist das Gerät die Sicherheitseinstellungen zurück. Die hinterlegten Anmeldedaten von Sicherheitsadministratoren oder Administratoren sind hierfür nicht geeignet.

3.2.8 Grundlegende Eigenschaften der Zuweisung von Rechten und unterstützten Rollen

Eine Rolle ist eine Kombination von Rechten, die für das SIPROTEC 5-Gerät definiert wurden. Sie können Benutzern in verschiedenen Kontexten eine Rolle zuweisen. Die Rollen eines Benutzers in einem bestimmten Kontext bestimmen, welche Aktionen der Benutzer am SIPROTEC 5-Gerät durchführen kann und welche nicht.

Die folgenden Tabellen geben eine Übersicht über die grundlegenden Eigenschaften der Rechte und unterstützten Rollen gemäß:

- IEEE 1686
- BDEW Whitepaper
- Norm IEC 62351-8
- Betriebsbedingte Anforderungen von SIPROTEC 5

HINWEIS

Sie können die Sicherheitseinstellungen unabhängig von Ihren Zugriffsrechten nicht über die Bedieneinheit des Gerätes ändern.

Tabelle 3-1 Generelle Zuweisung von Rechten und unterstützten Rollen in DIGSI 5

Rechte	Funktion der Rechte	Zuweisung von unterstützten Rollen						
		VIEWER	OPERATOR[2] + ENGINEER	ENGINEER	INSTALLER	SECADM	SECAUD[3] + ENGINEER	Administrator
Keine	Anzeige allgemeiner Informationen auf dem IED	X	X	X	X	X	X	X
View data	Betriebsdaten auf dem IED anzeigen	–	X	X	X	–	X	X

2 In DIGSI 5 kann mit der Rolle OPERATOR allein nicht gearbeitet werden.

3 In DIGSI 5 kann mit der Rolle SECAUD allein nicht gearbeitet werden.

Rechte	Funktion der Rechte	Zuweisung von unterstützten Rollen						
		VIEWER	OPERATOR[2] + ENGINEER	ENGINEER	INSTALLER	SECADM	SECAUD[3] + ENGINEER	Administrator
Force values	• Werte ändern • Istwerte überschreiben • Prozess auslösen	–	X	–	–	–	–	X
Change CFG	Konfiguration ändern/herunterladen/ hochladen	–	X	X	X	–	X	X
Change FW	Firmware ändern	–	–	–	X	–	–	X
Audit trail	Audit trail	–	–	–	–	–	X	X
Security management	Sicherheitsfunktionen verwalten und ausführen	–	–	–	–	X	–	X

Tabelle 3-2 Generelle Zuweisung von Rechten und unterstützten Rollen für die browser-basierte Benutzeroberfläche

Rechte	Funktion der Rechte	Zuweisung von unterstützten Rollen						
		VIEWER	OPERATOR[4] + ENGINEER	ENGINEER	INSTALLER	SECADM	SECAUD[5] + ENGINEER	Administrator
Keine	Anzeige allgemeiner Informationen auf dem IED	X	X	X	X	X	X	X
View data	Betriebsdaten auf dem IED anzeigen	–	X	X	X	–	X	X
Force values	• Werte ändern • Istwerte überschreiben • Prozess auslösen	–	X	–	–	–	–	X
Change CFG	Konfiguration ändern/herunterladen/ hochladen	–	X	X	X	–	X	X

2 In DIGSI 5 kann mit der Rolle OPERATOR allein nicht gearbeitet werden.
3 In DIGSI 5 kann mit der Rolle SECAUD allein nicht gearbeitet werden.
4 In der browser-basierten Benutzeroberfläche kann mit der Rolle OPERATOR allein nicht gearbeitet werden.
5 In der browser-basierten Benutzeroberfläche kann mit der Rolle SECAUD allein nicht gearbeitet werden.

Tabelle 3-3 Generelle Zuweisung von Rechten und unterstützten Rollen auf der Bedieneinheit des Gerätes

Rechte	Funktion der Rechte	Zuweisung von unterstützten Rollen						
		VIEWER	OPERATOR	ENGINEER	INSTALLER	SECADM	SECAUD	Administrator
Keine	Anzeige allgemeiner Informationen auf dem IED	X	X	X	X	X	X	X
View data	Betriebsdaten auf dem IED anzeigen	X[6]	X	X	X	X[6]	X[6]	X
View CFG settings	Konfigurationseinstellungen am IED anzeigen	X	X	X	X	X	–	X
Force values	• Werte ändern • Istwerte überschreiben • Prozess auslösen	–	X	–	–	–	–	X
Change CFG	Konfiguration ändern	–	–	X	X	–	–	X
Change FW	Firmware ändern	–	–	–	–	–	–	–
Audit trail	Audit trail	–	–	–	–	–	X	X
Security management	Sicherheitsfunktionen verwalten und ausführen	–	–	–	–	–	–	–

Zusätzlich zu den normbasierten, unterstützten Rollen sind die folgenden zusätzlichen unterstützten Rollen verfügbar. Diese weiteren unterstützten Rollen gelten für bekannte Operationen des Gerätes mit deaktiviertem RBAC, z.B. Schutz gegen unabsichtliche Operationen mit Bestätigungscodes.

- OPERATOR_SWITCHING
- SWITCHING_AUTHORITY
- INTERLOCKING_MODE

Benutzernamen, denen die zusätzlichen unterstützten Rollen zugewiesen wurden, können nur auf der Bedieneinheit des Gerätes arbeiten. Um solche Benutzernamen verwenden zu können, müssen Sie diese zuerst auf dem RADIUS-Server konfigurieren. Weitere Informationen zur Konfiguration des RADIUS-Servers finden Sie im Download-Bereich unter *http://www.siemens.com/gridsecurity* > **Cyber Security Products and Solutions** > **Cyber Security General Downloads** > **Application Notes**.

Tabelle 3-4 Generelle Zuweisung von Rechten und zusätzlichen unterstützten Rollen auf der Bedieneinheit des Gerätes

Rechte	Funktion der Rechte	Zuweisung von zusätzlichen unterstützten Rollen		
		OPERATOR_SWITCHING	SWITCHING_AUTHORITY	INTERLOCKING_MODE
Keine	Anzeige allgemeiner Informationen auf dem IED	X	X	X
View data	Betriebsdaten auf dem IED anzeigen	X	X	X

6 Protokolle sind ausgeschlossen.

Rechte	Funktion der Rechte	Zuweisung von zusätzlichen unterstützten Rollen		
		OPERATOR_SWITCHING	SWITCHING_AUTHORITY	INTERLOCKING_MODE
View CFG settings	Konfigurationseinstellungen am IED anzeigen	X	X	X
Force values	• Werte ändern • Istwerte überschreiben • Prozess auslösen	X	X	X
Change authority	Änderung der Schalthoheit	–	X	–
Change interlock mode	Änderung des Verriegelungsmodus	–	–	X

3.2.9 Benutzernamen an der Bedieneinheit des Gerätes

An der Bedieneinheit des Gerätes werden 2 Arten von Benutzernamen angezeigt:

- Standard-Benutzernamen
  SIPROTEC 5-Geräte werden mit den folgenden vordefinierten Benutzernamen für die Anmeldung ausschließlich an der Bedieneinheit des Gerätes ausgeliefert. Diese Benutzernamen werden mit den von den SIPROTEC 5-Geräten unterstützten Rollen verknüpft:
  - VIEWER
  - OPERATOR
  - ENGINEER
  - INSTALLER
  - SECADM
  - SECAUD
  - OPERATOR_SWITCHING
  - SWITCHING_AUTHORITY
  - INTERLOCKING_MODE
  - ADMIN
- Benutzerdefinierte Benutzernamen
  An der Bedieneinheit des Gerätes können Sie sich mit individuellen numerischen Benutzernamen und numerischen Passwörtern anmelden, die wie andere Benutzerkonten auf dem zentralen RADIUS-Server verwaltet werden. Solche Benutzernamen werden durch Auswahl der Option **USER_ID** auf der Anmeldeseite der Bedieneinheit des Gerätes eingegeben.
  Beachten Sie Folgendes bei der Konfiguration dieser Benutzernamen auf dem RADIUS-Server:
  - Benutzernamen und Passwörter sind rein numerisch.
  - Der Benutzername ist 1 bis 8 Ziffern lang.
  - Das Passwort ist 1 bis 15 Ziffern lang.

HINWEIS

Die benutzerdefinierten Benutzernamen können nur an der Bedieneinheit des Gerätes verwendet werden und nicht in DIGSI 5 oder auf der browserbasierten Benutzeroberfläche. Stellen Sie für diese Einschränkung das Feld **Zuständigkeitsbereich** (AoR) wie folgt ein:

- Setzen Sie das Feld AoR für die Standard-Benutzernamen auf einen beliebigen Wert. Die maximale Länge des Felds AoR beträgt 49 Zeichen.
- Für die benutzerdefinierten Benutzernamen setzen Sie das Feld AoR auf ***Local***.

```
"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, --_--]

Bild 3-12 Konfiguration der Benutzer auf dem RADIUS-Server

3.2.10 Anmeldung am Gerät über die Bedieneinheit des Gerätes

Benutzerauthentifizierung und -autorisierung beginnen mit dem SIPROTEC 5-Gerät. In diesem Fall ist das Gerät der RADIUS-Client und sendet eine Zugriffsanfrage an den RADIUS-Server.

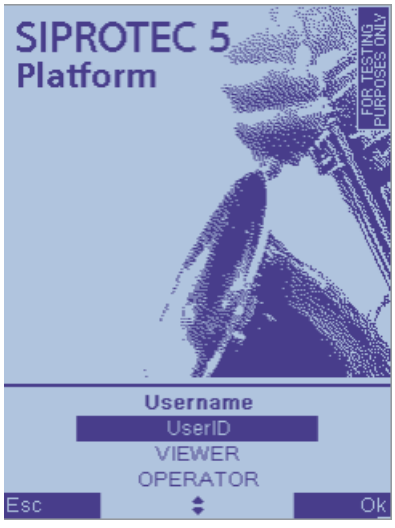
Diese Anfrage enthält die Anmeldedaten des Benutzers.

Anmeldung am Gerät

Gehen Sie wie folgt vor:

✧ Drücken Sie auf den Softkey **Anmeld.** am Gerät.

Im unteren Bereich des Geräte-Displays erscheint eine Auswahl der Benutzernamen.



[sc_Login, 1, de_DE]

Bild 3-13 Liste der Benutzernamen

✧ Nutzen Sie die Navigationstasten nach oben oder unten und wählen Sie den gewünschten Benutzernamen aus oder geben Sie einen Benutzernamen ein.

✧ Bestätigen Sie Ihre Auswahl durch Drücken des Softkeys **OK**.

Sie werden zur Eingabe des Passwortes aufgefordert.



[sc_Enter passcode, 1, de_DE]

Bild 3-14 Seite zur Eingabe des Passwortes

- ✧ Geben Sie das numerische Passwort ein.
- ✧ Schließen Sie Ihre Eingabe mit dem Softkey **Enter** ab.

HINWEIS

Wenn die Nachricht *Blocked by another client* (Blockiert durch anderen Client) angezeigt wird, warten Sie eine Minute lang und melden sich dann noch einmal an.

Weitere Informationen zum Anmelden am Gerät über DIGSI siehe DIGSI Online-Hilfe.

3.3 Rollenbasierte Ansichten in DIGSI 5

Mit dieser Funktion von DIGSI 5 wird die Benutzeroberfläche an die jeweilige Rolle angepasst, mit der sich der Benutzer bei der Windows-Sitzung angemeldet hat. Beim Start von DIGSI 5 werden Ihr Benutzername gemäß der Windows-Anmeldungssitzung und Ihre unterstützte(n) Rolle(n) oben rechts auf der DIGSI 5-Benutzeroberfläche angezeigt. Diese Funktion ist am besten für die Benutzerkonten geeignet, die zentral in einem Microsoft-Active Directory-Domänen-Controller verwaltet werden. Ein zentral verwaltetes Benutzerkonto kann einer oder mehreren zentral definierten Benutzergruppe(n) hinzugefügt werden, die dann als die Rollen, die von DIGSI 5 erkannt werden, verwendet werden.

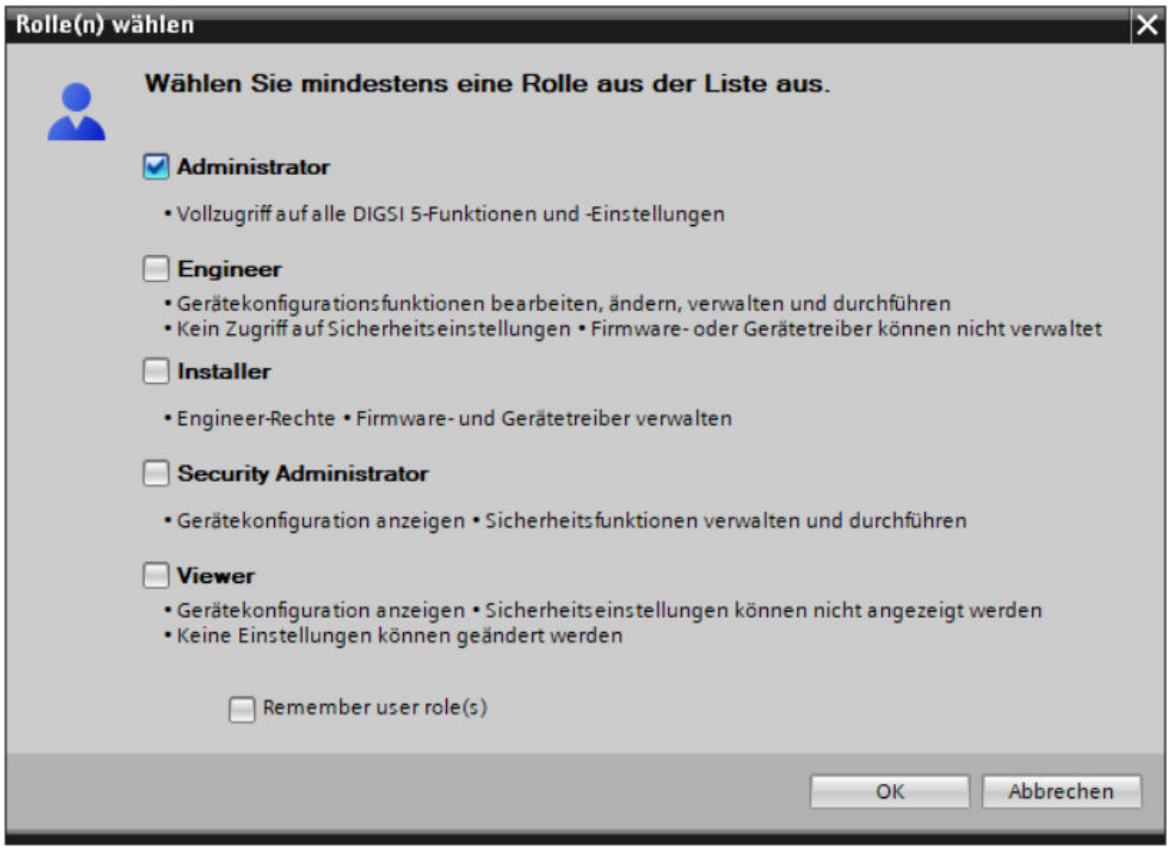
Im Allgemeinen werden die Rollen über den Security Administrator im Active Directory (AD) konfiguriert. Die folgenden Gruppennamen müssen bei der Konfiguration der unterschiedlichen Rollen im Active Directory verwendet werden:

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

Wenn die unterstützte Windows-Rolle (Benutzergruppe in Active Directory) auf Ihrem PC mit der folgenden Liste von n DIGSI 5 vordefinierten Rollen übereinstimmt, wird der entsprechende Rollenname mit dem Benutzernamen angezeigt:

- Administrator:
  Benutzer mit dieser Rolle können die gesamte DIGSI 5-Benutzeroberfläche einsehen (die einzige verfügbare Benutzeroberflächenoption für Versionen vor DIGSI 5 V7.90).
- Engineer:
  Benutzer mit dieser Rolle haben Zugriff auf alle Funktionen, außer auf die Funktionen zum Verwalten von Sicherheit, Firmware- und Gerätetreibern.
- Installer:
  Benutzer mit dieser Rolle haben Zugriff auf alle Funktionen, außer auf die Funktionen zum Verwalten von Sicherheitsoptionen.
- Security Administrator:
  Benutzer mit dieser Rolle können die Sicherheitsoptionen verwalten, die übrigen Geräteeinstellungen aber nur einsehen.
- Viewer:
  Benutzer mit dieser Rolle können die Gerätekonfiguration einsehen, diese aber nicht bearbeiten oder auf die Sicherheitseinstellungen zugreifen.

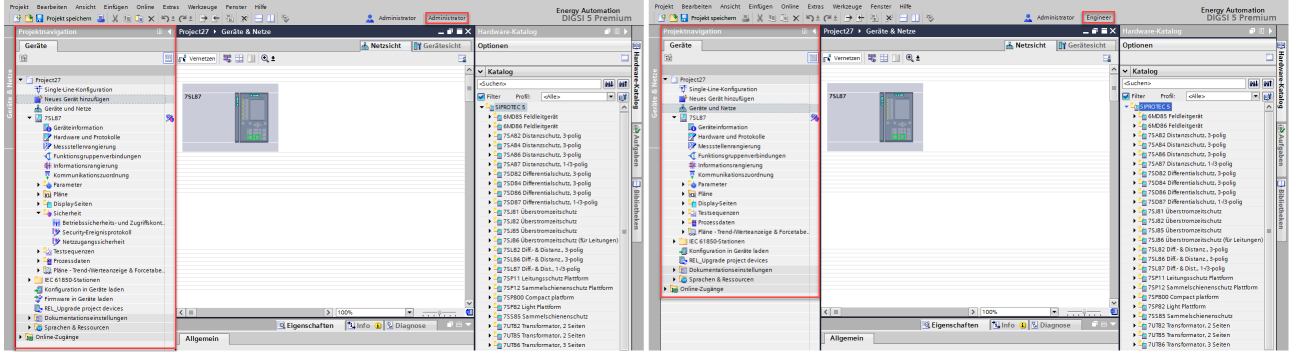
Wenn die unterstützte Windows-Rolle mit keiner der vordefinierten, von DIGSI 5 unterstützten Rollen übereinstimmt, wird standardmäßig der Rollenname **Administrator** angezeigt. Wenn Sie Ihren Zugriff auf DIGSI 5-Funktionen dennoch einschränken wollen, um versehentliche Änderungen am Projekt zu verhindern, können Sie dazu manuell eine spezifische Rolle für die aktuelle DIGSI 5-Sitzung auswählen. Sie können auf den Benutzernamen oder die unterstützte Rolle klicken, um den Dialog **Rolle(n) auswählen** zu öffnen und die erforderliche Rolle auszuwählen. Die mit jeder Rolle verbundenen Berechtigungen sind im Dialog **Rolle(n) auswählen** aufgeführt.



[sc_digsi_user_roles, 1, de_DE]

Die ausgewählten Rollen werden dann auf der DIGSI 5-Benutzeroberfläche auf dieselbe Weise übernommen, wie sie vom Gerät auf dem Display übernommen werden (nur lesen, lesen und schreiben, ausblenden).

Das folgende Bild zeigt die Unterschiede in der angezeigten Benutzeroberfläche bei Anmeldung mit unterschiedlichen unterstützten Rollen (**Administrator** und **Engineer**). Der als **Engineer** angemeldete Benutzer hat keinen Zugriff auf Sicherheitseinstellungen und kann auch die Firmware- oder Gerätetreiber nicht verwalten.



[sc_digsi_admin_engineer_view, 1, de_DE]

Unterstützte Rollen und Rechte

Aktion	ADMIN	ENGINEER	INSTALLER	VIEWER	SECADM
Gerätetreiber importieren	J	N	J	N	N
Gerätetreiber deinstallieren	J	N	J	N	N
Drucken und Druckvorschau	J	J	J	J	N
Konsistenz prüfen	J	J	J	J	N

Aktion	ADMIN	ENGINEER	INSTALLER	VIEWER	SECADM
Exportieren	J	J	N	J	J
Importieren	J	J	N	N	N
Bearbeiten – umbenennen, ausschneiden, einfügen, löschen	J	J	N	N	J
Bearbeiten – kopieren	J	J	J	J	J
Projekt erstellen/löschen	J	J	N	N	J
Projekt archivieren	J	J	J	J	J
Projekt speichern	J	J	N	N	J
Projekt speichern unter	J	J	J	J	J
Single-Line-Editor	S	S	L	L	N
Neues Gerät hinzufügen	J	J	N	N	N
Geräte- und Netzwerk-Editor	S	S	L	L	N
Konfiguration in Geräte laden	J	J	N	N	N
Firmware in Geräte laden	J	N	J	N	N
IEC-Station	J	J	N	N	N
Hardware- und Protokoll-Editor	S	S	L	L	L
Neue Display-Seite hinzufügen	J	J	N	N	N
Neue Testsequenz hinzufügen	J	J	N	N	N
Geräteinformations-Editor	S	S	L	L	L
Editor für Messstellenrangierung	S	S	L	L	N
Editor für Funktionsgruppenverbindungen	S	S	L	L	N
Editor für Informationsrangierung	S	S	L	L	N
Editor für Kommunikationszuordnung	S	S	L	L	N
Editor für Parameter	S	S	L	L	N
Editor für Schreiberinteraktion	S	S	L	L	N
Editor für Störfallanzeige-Konfiguration	S	S	L	L	N
Editor für Schalterinteraktion	S	S	L	L	N
Display-Seiten-Editor	S	S	L	L	N
Zeiteinstellungen-Editor	S	S	L	L	L
Schreibersignalbestellung	S	S	L	L	N
Geräteeinstellungen-Editor	S	S	L	L	L
Netzzugangssicherheit	S	N	N	N	S
Editor für Security-Ereignisprotokollierung	S	N	N	N	S
Betriebssicherheits- und Zugriffskontrolle	S	N	N	N	S
Geräte zuordnen und Zuordnung aufheben	J	J	N	N	N
Firmware online laden und Konfiguration laden	J	J	N	N	N
Auf Werkseinstellungen zurücksetzen, Anmeldedaten sicher zurücksetzen und SCF in Gerät laden	S	N	N	N	J
SCRF, SFRF herunterladen und gespeicherte Anmeldedaten entfernen	J	J	N	N	J
Prozessdaten abrufen	J	J	N	N	N
Schutzfunktionen	J	N	N	N	N
Prozessdatenzugriff	S	L	L	L	N
Online-SLE	S	S	L	L	N

Aktion	ADMIN	ENGINEER	INSTALLER	VIEWER	SECADM
Online-Geräteinformations-Editor					
Online-Geräteinformations-Editor: Geräteinformation	S	S	L	L	L
Online-Geräteinformations-Editor: Ressourcenverbrauch	L	L	L	L	L
Registerkarte Meldepuffer					
Online-Geräteinformations-Editor: Gerätediagnosepuffer	S	S	L	L	L
Online-Geräteinformations-Editor: Sicherheitsmeldungen	L	N	N	N	L
Online-Geräteinformations-Editor: Diagnoseinformationen	L	L	L	L	L

Legende	
J	Ja
N	Nein
S	Schreibzugriff
L	Lesezugriff

Unterstützte Rollen zwischen Offline- und Online-Konfiguration umschalten

- Unabhängig davon, welche Rollen für den/von dem Benutzer bei der Offline-Arbeit mit DIGSI 5 angewendet werden, wird die DIGSI 5-Benutzeroberfläche beim erfolgreichen Anmelden an einem RBAC-Gerät ggf. angepasst, um der/den Rolle(n) zu entsprechen, die vom Gerät für den angemeldeten Benutzer ermittelt wurde(n). Nach dem Verbindungsaufbau mit einem RBAC-Gerät wird der Zustand der Projektnavigation und der Menüs/Symbolleisten-Schaltflächen gemäß der/den unterstützten Online-Rolle(n) aktualisiert und alle geöffneten Editoren werden geschlossen. Außerdem wird die unterstützte Online-Rolle oben rechts auf der DIGSI-Benutzeroberfläche angezeigt.
- Wenn der Benutzer die gespeicherten Online-Anmeldedaten in DIGSI 5 löscht oder die Online-Sitzung abläuft, werden die Online-Rollen des Benutzers beibehalten.

3.4 Notfallzugang

Wenn der RADIUS-Server bei der Anmeldung am Gerät nicht erreichbar ist und Sie sich nicht als Benutzer anmelden können, können Sie sich über den Notfallzugang am Gerät anmelden.

Siemens empfiehlt die Konfiguration des Notfallzugangs für DIGSI 5 und die Vor-Ort-Bedienung bei der Inbetriebnahme des Gerätes oder bei der Konfiguration der Cyber-Security-Parameter.

Bedenken Sie folgende Punkte, bevor Sie das Notfallkonto aktivieren:

- Sie verwenden den Notfallzugang nur, wenn der/die RADIUS-Server nicht erreichbar ist/sind.
- Zur Konfiguration des Notfallzugangs ist die Rolle des Security-Administrators erforderlich.
- Nach der Aktivierung der RBAC-Funktion besteht kein Notfallkonto.

Notfallkonto aktivieren

✧ Starten Sie DIGSI 5.

✧ Öffnen Sie das Projekt in DIGSI 5.

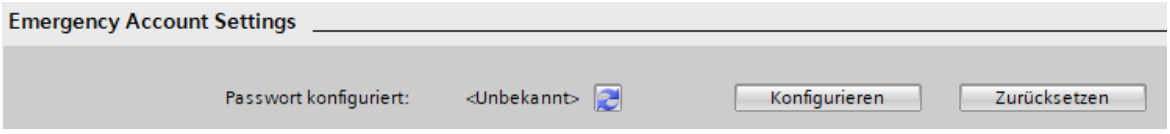
✧ Öffnen Sie in der Projektnavigation den Menüeintrag **Sicherheit**.

✧ Doppelklicken Sie auf den Menüeintrag **Betriebssicherheits- und Zugriffskontrolle**.

✧ Klicken Sie unter **Emergency Account Settings** auf **Konfigurieren**.

Mit der Taste zum Aktualisieren können Sie den Status des Notfallskontos im Gerät überprüfen:

– **Ja**: das Notfallpasswort ist konfiguriert.
– **Nein**: das Notfallpasswort ist nicht konfiguriert.
– **Unbekannt**: **RBAC** ist im Gerät nicht aktiv.



[sc_emergency_account_settings, 2, de_DE]

Bild 3-15 Notfallkonto-Einstellungen in DIGSI

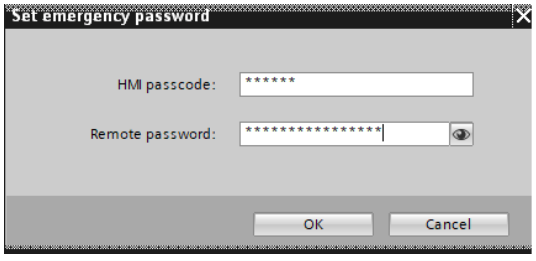
✧ Geben Sie für die Vor-Ort-Bedienung des Geräts ein Notfallpasswort mit mindestens 6 Ziffern ein.

Das Notfallpasswort für die Vor-Ort-Bedieneinheit kann nur direkt an der Bedieneinheit des Geräts eingegeben werden.

✧ Für die Bedienung über DIGSI 5 geben Sie ein Notfallpasswort mit mindestens 8 Zeichen ein, das aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen muss.

Das Notfallpasswort für den Zugriff über DIGSI kann nur über DIGSI 5 eingegeben werden.

✧ Bestätigen Sie die Eingaben mit **OK**.



[sc_set_emergency_password, 2, de_DE]

Bild 3-16 Dialog für die Eingabe der Notfallpasswörter

Jetzt ist der Notfallzugang mit denselben Rechten wie die Rolle des Administrators ausgestattet.

4 Malware Protection

4.1	Übersicht	46
4.2	Malware-Schutz für Engineering-Software	47
4.3	Integritätsprüfung der heruntergeladenen Datei	48

4.1 Übersicht

SIPROTEC 5-Geräte basieren auf dem Betriebssystem VxWorks, für das kein spezielles Antivirenprogramm erhältlich ist. Außerdem verfügen SIPROTEC 5-Geräte über eine interne Firewall zum Schutz vor Angriffen über das Netzwerk. Zur Verbesserung des Schutzes ist die Firewall standardmäßig aktiviert.

Sie können nur digital signierte Firmware-Dateien in das Gerät laden und die Geräte vor manipulierten oder fehlerhaften Firmware-Dateien schützen. Das Gerät akzeptiert nur signierte Firmware-Dateien und signierte Hardware-Konfigurationen. Die Signierung erfolgt sicher in den Siemens-Produktionsstätten mit der Siemens-internen Public-Key-Infrastruktur für Produkte.

Außerdem werden Viren normalerweise per E-Mail übertragen, beim Surfen im Internet oder durch infizierte Wechseldatenträger. SIPROTEC 5-Geräte sind für diese Infektionswege nicht anfällig.

Die Authentifizierung zwischen DIGSI 5 und dem Gerät mit digitalen Zertifikaten hindert Anwendungen außer DIGSI 5 daran, die Gerätekonfiguration zu ändern oder auf sie zuzugreifen. Weitere Informationen über die Ausgabe eigener Zertifikate für die Autorisierung von DIGSI 5-Installationen und die Interaktion mit SIPROTEC 5-Geräten siehe Kapitel *5.2 DIGSI 5 Client-Authentifizierung*.

4.2 Malware-Schutz für Engineering-Software

Die PC-basierte Engineering-Software für SIPROTEC-Geräte – DIGSI 5 – wird zum Schutz ihrer Integrität mit einem signierten Installationsprogramm installiert. Siemens prüft regelmäßig die Kompatibilität neuer Antivirus-Muster mit der neuesten Version von DIGSI und erstattet Bericht. Diese Berichte können jeden Monat im Internet abgerufen werden und beinhalten auch die Ergebnisse der Prüfung der Kompatibilität von Microsoft Windows-Patches. Außerdem wird jede Version von DIGSI 5 vor der Auslieferung gegen eine Vielzahl von Antiviren-Scannern getestet.

Die DIGSI-Software wird auch auf Kompatibilität mit Whitelisting-Applikationslösungen geprüft, wobei nur zugelassene Software ausgeführt werden darf. Schadprogramme, die nach Aktivierung des Whitelisting-Schutzes auftreten, können nicht ausgeführt werden. Der Vorteil der Whitelisting-Applikation für geschützte und isolierte Unterstationsnetzwerke ist, dass die Antiviren-Muster für neu entdeckte Schadprogramme nicht sofort aktualisiert werden müssen.

Mit diesen Schritten werden SIPROTEC 5-Geräte und DIGSI 5 in der Zielumgebung sicherer und zuverlässiger.

4.3 Integritätsprüfung der heruntergeladenen Datei

Sie können auch die Integrität der SIPROTEC Firmware- und Software-Dateien prüfen, die auf dem von Siemens unterstützten Portal heruntergeladen werden können. Für jede herunterladbare Firmware- und Software-Datei wird der entsprechende SHA-256-Fingerprint im Internet veröffentlicht[7].

Tools wie Certutil in Microsoft Windows können für folgende Zwecke verwendet werden:

- Erzeugen des SHA-256-Fingerprints für die Datei, die Sie herunterladen.
- Prüfen, ob der SHA-256-Fingerprint mit dem veröffentlichten Fingerprint zur Verifizierung der Integrität der Datei übereinstimmt.

7 *http://www.siemens.com/gridsecurity* -> **Product Security** -> **Downloads** -> **Software**

5 Communication Security

5.1	Zugriffsbeschränkungen für Ethernet anwenden	50
5.2	DIGSI 5 Client-Authentifizierung	51
5.3	Sicherheit von Interaktionen zwischen Web-Browser und Gerät	58

5.1 Zugriffsbeschränkungen für Ethernet anwenden

Über die Sicherheitseinstellungen können Sie die Zugriffsrechte einer DIGSI 5-Verbindung für die einzelnen Ethernet-Schnittstellen (Port J und Ethernet-Kommunikationsmodul) einschränken.



HINWEIS

Wenn das Gerät über ein Ethernet-Kommunikationsmodul verfügt, können Sie auch Port E, Port F, Port N oder Port P verwenden.

Sie können die Sicherheitsparameter in DIGSI 5 in der Projektnavigation unter **Sicherheit** -> **Netzzugangssicherheit** einstellen.
Sie können folgende Zugriffsrechte einstellen:

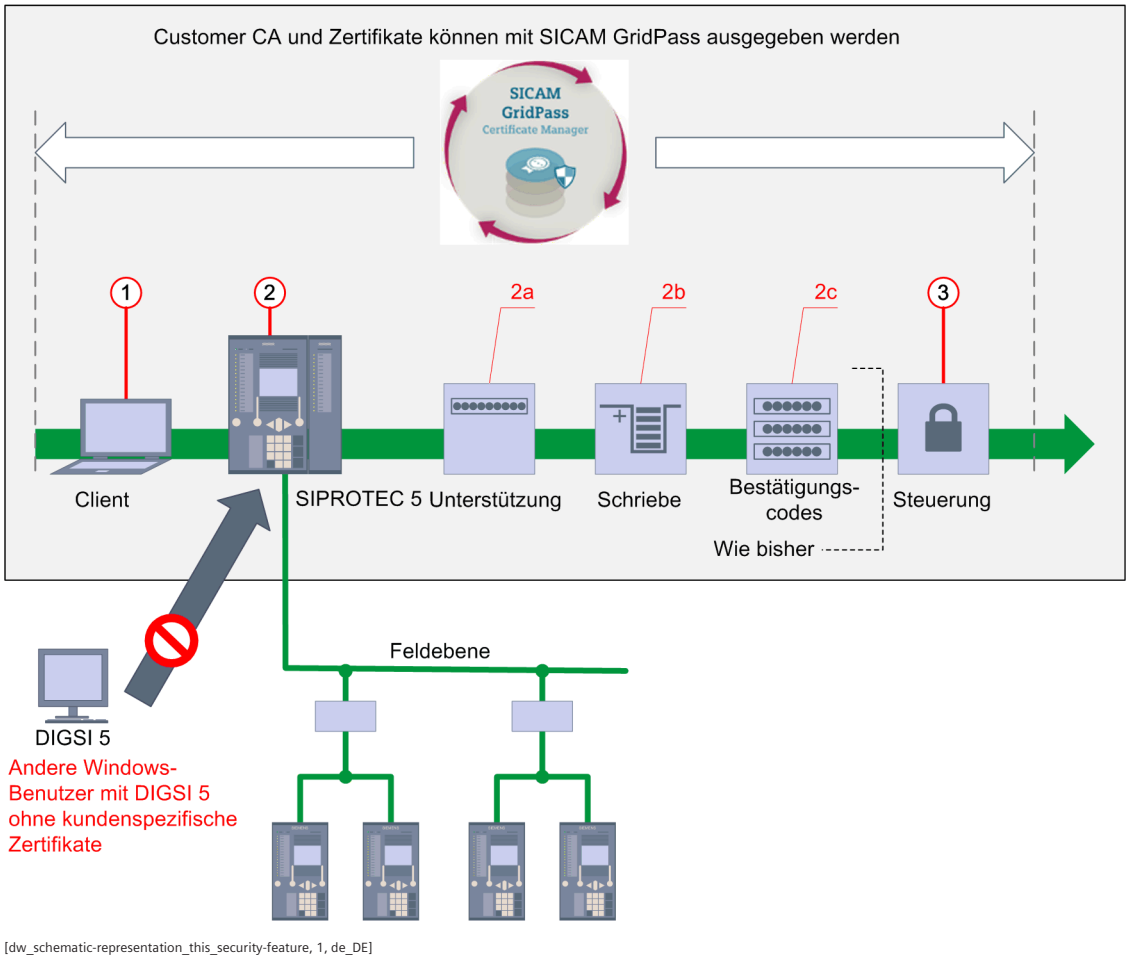
- Kein Zugriff
  Keine DIGSI-Kommunikation über diese Schnittstelle möglich.
- Lesezugriff
  Über diese Schnittstelle haben Sie Lesezugriff auf das Gerät.
- Lese- und Schreibzugriff
  Über diese Schnittstelle ist Lese- und Schreibzugriff möglich.

5.2 DIGSI 5 Client-Authentifizierung

5.2.1 Allgemeine Informationen

Mit der neuen Funktion **DIGSI Client-Authentifizierung** können Sie in DIGSI 5 eigene digitale Zertifikate für die sichere Kommunikation zwischen DIGSI 5 und dem SIPROTEC 5-Gerät verwenden.

Sobald diese Funktion eingerichtet wurde, ist eine Verbindung zu einem Gerät mit der Standardversion von DIGSI 5 über das eingebettete voreingestellte Client-Zertifikat von Siemens nicht mehr möglich. Dies verhindert den Zugriff von unberechtigten Windows-Benutzer mit DIGSI 5-Installation auf einsatzfähige SIPROTEC 5-Geräte.



[dw_schematic-representation_this_security-feature, 1, de_DE]

Bild 5-1 Schematische Darstellung der Sicherheitsfunktion

1	Installation von Client-Zertifikaten, die vom Kunden erstellt wurden, im Windows-Benutzerkonto (Client-Autorisierung).
2	Installation der Kunden-CA, die für die Signierung des DIGSI 5 Client-Zertifikats im Gerät verwendet wird Neu: Nur DIGSI 5-Installationen, die von der Kunden-CA signiert wurden, sind zulässig.
2a	Geräteseitiger Support für Role-Based Access Control einschließlich zentraler Benutzerverwaltung und Notfallzugang (Funktion wie gehabt)
2b	Aufzeichnung sicherheitsrelevanter Ereignisse und Alarme über Syslog und Aufzeichnung in permanenten Sicherheitsmeldepuffern im Gerät (Funktion wie gehabt)

2c	Bestätigungscodes für sicherheitskritische Handlungen (Funktion wie gehabt)
3	Kommunikation mit gegenseitiger Authentifizierung und Verschlüsselung zwischen DIGSI 5 und dem SIPROTEC 5-Gerät

Beim Aufbau der Verbindung mit einem SIPROTEC 5-Gerät übergibt DIGSI 5 sein digitales Client-Zertifikat (im Folgenden **Client-Zertifikat** genannt) an das Gerät zur Authentifizierung. Wenn Sie für Ihre DIGSI 5-Installation statt der Siemens-Standardzertifikate ein eigenes Client-Zertifikat verwenden möchten, dann benötigen Sie eine Public Key Infrastructure (PKI) mit einer betriebsbereiten Certificate Authority (CA) für die Erstellung oder digitale Signierung solcher Client-Zertifikate. Weitere Informationen zur Installation einer PKI für Ihre betrieblichen Anforderungen finden Sie im Handbuch SICAM GridPass (*http://www.siemens.com/sicam-gridpass*).

Vor der Verwendung der Funktion zur Client-Authentifizierung in DIGSI müssen Sie zuerst die Windows-Benutzerkonten, die für die Verwendung von DIGSI 5 autorisiert sind, konfigurieren und entsprechend auch die SIPROTEC 5-Geräte.

Um die neue Funktion **DIGSI Client-Authentifizierung** zu konfigurieren, gehen Sie wie folgt vor:

- Richten Sie einen DIGSI 5 CA-Store (CA = Certificate Authority) ein.
- Konfigurieren Sie die Sicherheitsfunktion DIGSI 5 Client-Authentifizierung.
- Verifizieren Sie die konfigurierte CA über einen Web-Browser.

Weitere Informationen zu diesen Schritten finden Sie in den folgenden Kapiteln.

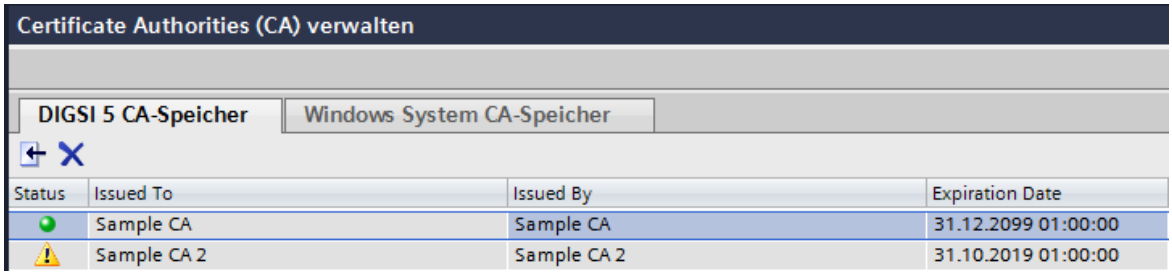
5.2.2 Konfiguration

5.2.2.1 DIGSI 5 CA-Store einrichten

Um eigene Client-Zertifikate zu verwenden, müssen Sie DIGSI 5 zuerst das entsprechende Zertifikat der ausgebenden CA mitteilen. Das ist die CA, mit der Sie die Client-Zertifikate erstellen, die Sie (neben den entsprechenden Private Keys) auf allen für die Nutzung von DIGSI 5 autorisierten Windows-Benutzerkonten installieren.

Dazu müssen Sie Ihre ausgebende CA zum **DIGSI 5 CA-Speicher** hinzufügen. Der **DIGSI 5 CA-Speicher** verwaltet eine Liste aller CAs, die für Dienste konfiguriert werden können, die eine sichere Authentifizierung basierend auf Ihrer PKI erfordern.

Sie können auf den **DIGSI 5 CA-Speicher** über das Menü **Werkzeuge** > **Certificate Authorities (CA) verwalten** zugreifen:



[sc_Manage_CA, 1, de_DE]

Es gibt 2 Möglichkeiten, eine bestehende Zertifizierungsstelle (CA) zum **DIGSI 5 CA-Speicher** hinzuzufügen:

- Import der CA aus dem Windows System CA-Speicher
- Import aus einer Datei

Import der CA aus dem Windows System CA-Speicher

✧ Wenn Sie Ihre ausgebende CA bereits im Windows CA-Speicher installiert haben, können Sie diese von dort importieren. Öffnen Sie die Registerkarte **Windows System CA-Speicher** und wählen Sie die CA aus, die Sie zum **DIGSI 5 CA-Speicher** hinzufügen möchten.

✧ Klicken Sie **In DIGSI 5 CA-Speicher importieren**.

Import aus einer Datei

Sie können Ihre ausgebende CA auch aus einer Datei importieren:

✧ Öffnen Sie die Registerkarte **DIGSI 5 CA-Speicher** und klicken Sie **In DIGSI 5 CA-Speicher importieren**.

Ein Datei-Browser wird angezeigt.

✧ Wählen Sie die CA-Datei aus, die Sie importieren möchten, und bestätigen Sie den Vorgang, um die CA-Datei zum **DIGSI 5 CA-Speicher** hinzuzufügen.

In beiden Fällen wird bei erfolgreichem Abschluss des Vorgangs die importierte CA in der Liste im **DIGSI 5 CA-Speicher** mit einem Symbol angezeigt, das die Gültigkeitsdauer des gewählten CA-Zertifikats angibt:

Symbol	Erklärung
	Die CA ist noch mindestens 180 Tage lang gültig.
	Die CA läuft innerhalb der nächsten 180 Tage ab.
	Die CA ist abgelaufen und daher nicht mehr gültig.

HINWEIS

Derzeit können bis zu 8 CAs im **DIGSI 5 CA-Speicher** verwaltet werden. Bei einer Überschreitung der Anzahl wird die Liste abgeschnitten. Entfernen Sie vor dem Hinzufügen weiterer CAs manuell diejenigen CAs, die nicht mehr verwendet werden.

CA aus dem DIGSI 5 CA-Speicher entfernen

✧ Wenn Sie eine CA aus dem **DIGSI 5 CA-Speicher** entfernen möchten, wählen Sie die CA in der Liste aus und klicken **Aus DIGSI 5 CA-Speicher entfernen**.

HINWEIS

Wenn die CA im geöffneten Projekt bereits mit einem oder mehreren Geräten verknüpft ist, wird eine Warnung angezeigt, wenn Sie sie entfernen möchten.

5.2.2.2 Konfiguration der Sicherheitsfunktion DIGSI 5 Client-Authentifizierung

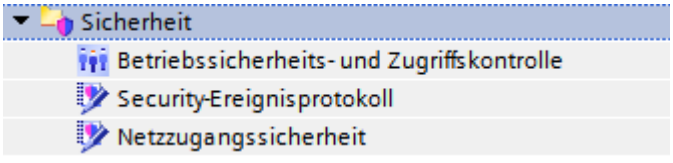
HINWEIS

Wenn Sie ein Projekt mit einer CA geöffnet haben, die derzeit nicht in diesem CA-Store enthalten ist, wird automatisch eine konfigurierte CA zum DIGSI CA-Store hinzugefügt. Dies gilt auch für Online-Verbindungen zu bestehenden Geräten.

Sie müssen Ihre Geräte so konfigurieren, dass diese mit Ihren Client-Zertifikaten ausschließlich DIGSI 5-Verbindungsanfragen akzeptieren.

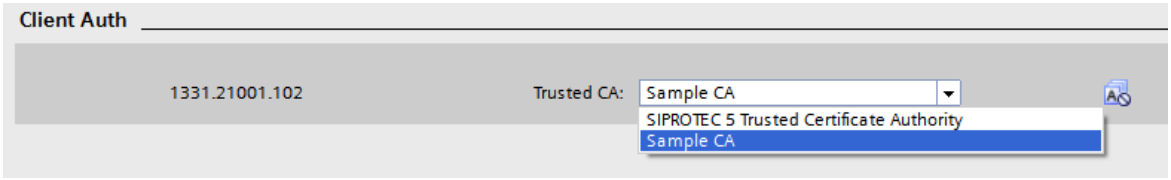
So konfigurieren Sie die **DIGSI Client-Authentifizierung für ein Gerät**:

✧ Wählen Sie in der Projektnavigation das entsprechende Gerät aus, navigieren Sie zu **Sicherheit** und wählen Sie **Netzzugangssicherheit**:



[sc_Network_access_security, 1, de_DE]

Die folgenden Informationen werden dargestellt:



[sc_client_authentication, 1, de_DE]

✧ Wählen Sie aus der Auswahlliste **Trusted CA** die für Ihre DIGSI 5 Client-Zertifikate verwendete Zertifizierungsstelle.

In dieser Auswahlliste werden die Zertifizierungsstellen angezeigt, die im **DIGSI 5 CA Store** derzeit importiert sind (siehe Kapitel *5.2.2.1 DIGSI 5 CA-Store einrichten*). Der Voreinstellwert dieser Auswahlliste ist **SIPROTEC 5 Trusted Certificate Authority**. Wenn Sie diesen Wert ausgewählt haben, wird das Standardverhalten für die Verbindung von DIGSI 5 zum SIPROTEC 5-Gerät mit den DIGSI 5-Client-Zertifikaten von Siemens aktiviert.

Laden Sie diese Einstellungen in das Gerät, damit sie wirksam werden.

HINWEIS

Navigieren Sie zur Verifizierung der konfigurierten Zertifizierungsstelle über die Benutzeroberfläche zu **Parameter** > **Sicherheit** > **Client Auth** > **Trusted CA**.

✧ Um die Kommunikation mit dem Gerät aufzubauen, muss ein von der gewählten Zertifizierungsstelle ausgegebenes Client-Zertifikat auf dem DIGSI-PC installiert sein.

Wenn mehrere Client-Zertifikate zur Auswahl stehen, werden Sie zur Auswahl aufgefordert. Wenn auf dem DIGSI 5-PC kein Client-Zertifikat installiert ist, wird eine entsprechende Fehlermeldung angezeigt.

5.2.2.3 Verifizierung der konfigurierten CA über einen Web-Browser

Sie können die Konfiguration der **DIGSI Client-Authentifizierung** über einen Web-Browser prüfen.

Gehen Sie zur Überprüfung der Einstellungen wie folgt vor:

✧ Öffnen Sie den Web-Browser und melden Sie sich an einem Gerät an, das nur Verbindungsanfragen von DIGSI 5-Installationen mit Ihren eigenen von der Zertifizierungsstelle ausgegebenen Zertifikaten akzeptiert (und keine Siemens-Standardzertifikate).

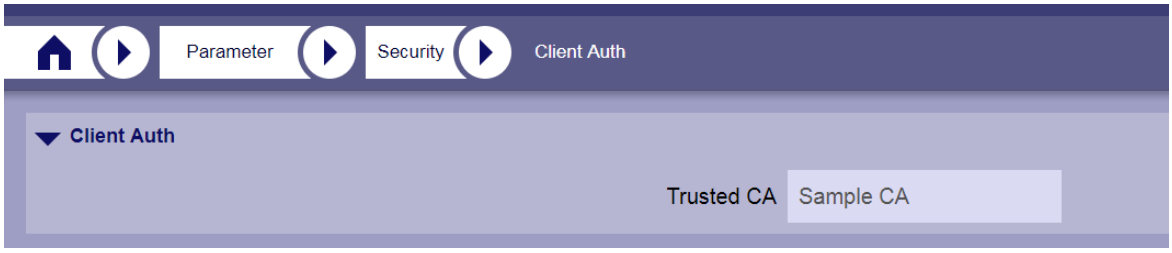
✧ Navigieren Sie zu **Zertifikate** > **Zertifizierungsstellen**.



[sc_CerAuth., 1, de_DE]

✧ Navigieren Sie zu **Parameter** > **Security** > **Client-Auth**.

Die konfigurierte kundenspezifische Zertifizierungsstelle kann auch auf der Seite für die Einstellungen zur **Client-Authentifizierung** überprüft werden:



[sc_settings_ClientAuth, 1, de_DE]

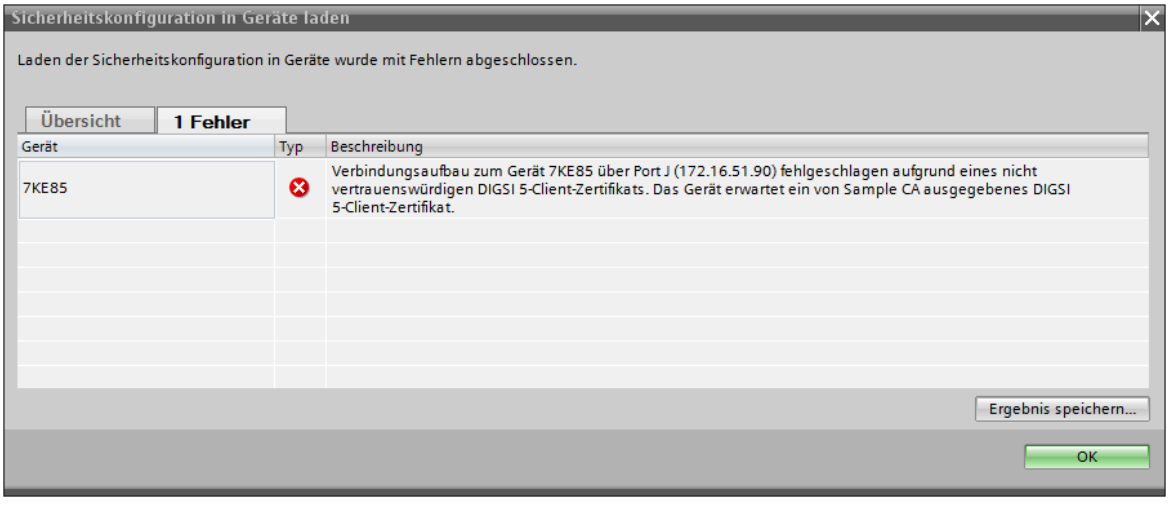
Wenn Sie die **SIPROTEC 5 Trusted Certificate Authority** ausgewählt haben, ist der Wert für **Trusted CA** auf **Standard** gesetzt.

5.2.2.4 Unbefugter Zugriff mit DIGSI 5 auf SIPROTEC 5-Geräte

Bei der Konfiguration einer vertrauenswürdigen Zertifizierungsstelle muss ein gültiges, von der Zertifizierungsstelle signiertes Client-Zertifikat im Windows System CA-Store vorliegen, damit eine sichere Verbindung zum SIPROTEC 5-Gerät aufgebaut werden kann.

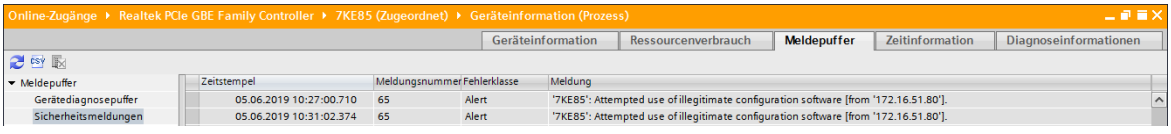
Kein gültiges Zertifikat

Wenn kein gültiges Client-Zertifikat vorliegt, kann DIGSI 5 keine Verbindung zum SIPROTEC 5-Gerät aufbauen. Stattdessen erhalten Sie eine Fehlermeldung mit Angabe des erwarteten Client-Zertifikats:



[sc_unauthorized_DIGSI_access, 1, de_DE]

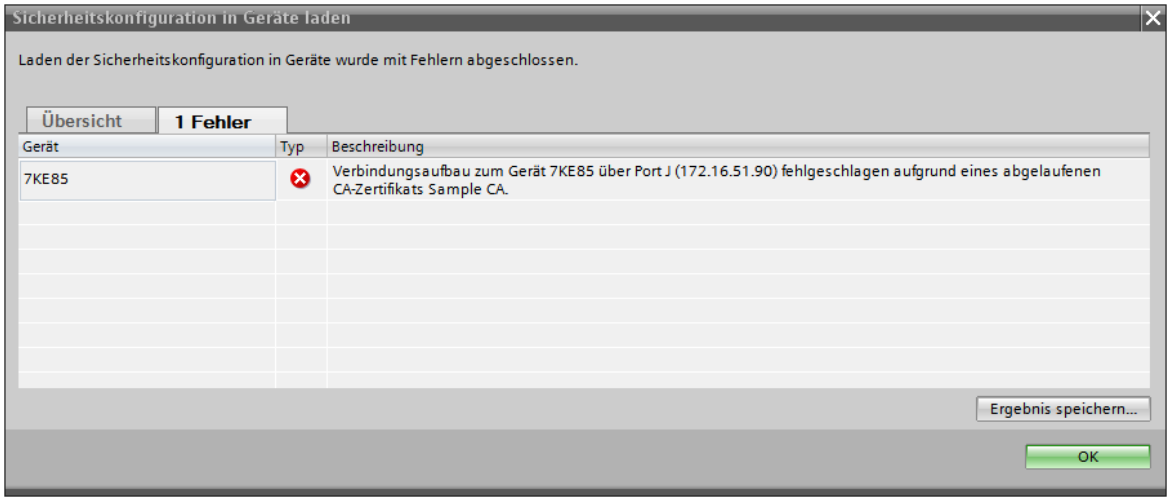
Dieser nicht autorisierte Zugriffsversuch führt auch zu einem Eintrag im Sicherheitsmeldepuffer:



[sc_unauthorized_DIGSI_access_security_log, 1, de_DE]

Abgelaufenes Zertifikat

Wenn die konfigurierte vertrauenswürdige Zertifizierungsstelle vor der Erneuerung abgelaufen ist, wird bei einem Verbindungsversuch zum SIPROTEC 5-Gerät die folgende Fehlermeldung angezeigt:



[sc_unauthorized_DIGSI_access_message, 1, de_DE]

Hinweise zur Wiederherstellung nach einer unbeabsichtigten Sperrung finden Sie in Kapitel *5.2.2.5 Wiederherstellung nach einer Sperrung über sicheres Zurücksetzen der Anmeldedaten*.

5.2.2.5 Wiederherstellung nach einer Sperrung über sicheres Zurücksetzen der Anmeldedaten

Mit der Konfiguration einer vertrauenswürdigen Zertifizierungsstelle muss ein gültiges, von der Zertifizierungsstelle signiertes Client-Zertifikat im Windows System CA-Store vorliegen, damit eine sichere Verbindung zum SIPROTEC 5-Gerät aufgebaut werden kann.

Wenn die vertrauenswürdige Zertifizierungsstelle vor deren Erneuerung abläuft oder wenn das entsprechende Client-Zertifikat nicht mehr im Windows System CA-Store vorliegt, kann DIGSI nicht mehr mit dem SIPROTEC 5-Gerät kommunizieren. Eine Wiederherstellung ist in diesem Fall nur durch das Zurücksetzen der Zugangsanmeldedaten über eine USB-Verbindung möglich.

Für die Wiederherstellung müssen Sie vorher die **Datei zum Zurücksetzen der Sicherheitsanmeldedaten und Konfiguration** (SCRF-Datei) vom Gerät heruntergeladen haben.

Herunterladen der SCRF-Datei

Gehen Sie dazu vor wie folgt vor:

✧ Wählen Sie in der Projektnavigation das Gerät aus und wählen Sie **Online** > **Sicherheit** > **Datei zum Zurücksetzen der Anmeldedaten herunterladen...**.

✧ Befolgen Sie die Empfehlungen zum Umgang mit SCRF-Dateien in Kapitel *9.1.1 Herunterladen der Datei zum Rücksetzen der Sicherheitsanmeldedaten und Konfiguration (SCRF)*.

Wiederherstellung nach einer Sperrung

Zur Wiederherstellung nach einer Sperrung kann diese SCRF-Datei über USB ohne ein gültiges Client-Zertifikat in das Gerät hochgeladen werden.

Gehen Sie dazu vor wie folgt vor:

✧ Wählen Sie in der Projektnavigation das Gerät aus und wählen Sie **Online** > **Sicherheit** > **Anmeldedaten zurücksetzen...**.

Dadurch werden die Validierungseinstellungen für das Client-Zertifikat im Gerät auf die Werkseinstellungen zurückgesetzt und DIGSI 5-Installationen mit eingebauten Siemens Client-Zertifikaten können mit dem Gerät kommunizieren.



HINWEIS

Folglich werden alle sicherheitsrelevanten Einstellungen auf die Standardwerte gesetzt!

5.3 Sicherheit von Interaktionen zwischen Web-Browser und Gerät

Abgesehen vom Einsatz des Engineering-Werkzeugs DIGSI 5 für die Konfiguration und Wartung verfügen SIPROTEC 5-Geräte über ein Web-Front-End, das mit einem Standard-Web-Browser genutzt werden kann. Dies ist in Kapitel **Bedienen mit browser-basierter Benutzeroberfläche** im SIPROTEC 5-Betriebshandbuch beschrieben.

HINWEIS

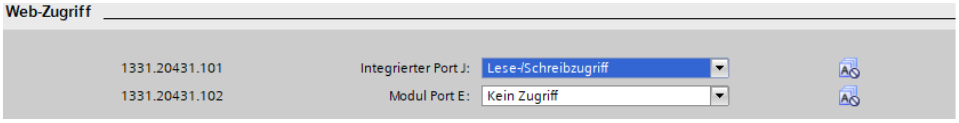
Sie können das SIPROTEC 5-Gerät parallel über DIGSI 5 und über die **browser-basierte Benutzeroberfläche** bedienen.

Vor der Bedienung des Gerätes über einen Web-Browser müssen Sie zuerst die Sicherheitseinstellungen überprüfen. Weitere Informationen hierzu, siehe Kapitel *5.1 Zugriffsbeschränkungen für Ethernet anwenden*.

So bedienen Sie das Gerät über die **browser-basierte Benutzeroberfläche**:

- Schließen Sie das SIPROTEC 5-Gerät (z.B. Port J) mit einem Netzwerkkabel an Ihren PC an.

Legen Sie zur Verbesserung der Verbindungssicherheit folgende Zugriffseinstellungen in DIGSI unter **Netzzugangssicherheit** fest:



[sc_webaccess, 2, de_DE]

Bild 5-2 Sicherheitseinstellungen in DIGSI

HINWEIS

Notieren Sie die IP-Adresse und die Port-Nummer der Schnittstelle, die für die Kommunikation von PC und **browser-basierter Benutzeroberfläche** verwendet wird. Stellen Sie sicher, dass die 12-stellige IP-Adresse für den Web-Browser korrekt im Format ***.***.***.*** über DIGSI eingestellt wurde.

- Starten Sie den Web-Browser auf Ihrem PC.
- Geben Sie die IP-Adresse des Gerätes in die Adresszeile des Web-Browsers ein, gefolgt von der Port-Nummer 4443, z.B. https://172.16.60.60:4443, und bestätigen Sie den Eintrag mit der Enter-Taste.

HINWEIS

Manche Web-Browser haben eventuell Probleme mit der Verbindung zur angegebenen IP-Adresse des Gerätes. Löschen Sie in diesem Fall das entsprechende Zertifikat im Web-Browser.

Je nach Sicherheitskonfiguration des SIPROTEC 5-Gerätes sind folgende Anmeldedialoge verfügbar:

- Variante 1:

  Wenn Sie ein Verbindungspasswort in DIGSI 5 unter **Betriebssicherheits- und Zugriffskontrolle** eingegeben haben, beginnt der Anmeldedialog mit dem Benutzernamen **Siprotec 5**. Dieser Benutzername kann nicht geändert werden. Sie müssen das in DIGSI konfigurierte Verbindungspasswort verwenden.

- Variante 2:

  Wenn Sie die Role-Based Access Control (RBAC) in DIGSI 5 unter **Betriebssicherheits- und Zugriffskontrolle** konfiguriert haben, beginnt der Anmeldedialog mit der Abfrage des von Ihnen im RADIUS-Server konfigurierten Benutzernamens und Passworts.

- Variante 3:

  Wenn Sie keine Role-Based Access Control (RBAC) und kein Verbindungspasswort konfiguriert haben, beginnt der Anmeldedialog mit dem Benutzernamen **Siprotec 5**. Dieser Benutzername kann nicht geändert werden. Das Texteingabefeld für das Passwort muss leer gelassen werden.

Wenn der Web-Browser erfolgreich mit dem Gerät verbunden wurde, wird der folgende Anmeldedialog (für Variante 2) angezeigt, z.B.:



[scwebmonitor, 1, de_DE]

Bild 5-3 Anmeldedialog für die browser-basierte Benutzeroberfläche

- Geben Sie den Benutzernamen in das Texteingabefeld **User name** (Benutzername) ein.
- Klicken Sie in das Texteingabefeld **Password** (Passwort) und geben Sie das Passwort ein.
- Wählen Sie die Sprache.
  Die Sprachauswahl hängt von der für die Benutzeroberfläche des Geräts eingestellten Sprache ab.

HINWEIS

Bei aktiver RBAC ist der Zugriff nur nach erfolgreicher Authentifizierung des Benutzernamens und Passworts möglich. Nähere Informationen hierzu, siehe Kapitel *3.2 Role-Based Access Control (RBAC) in SIPROTEC 5*.

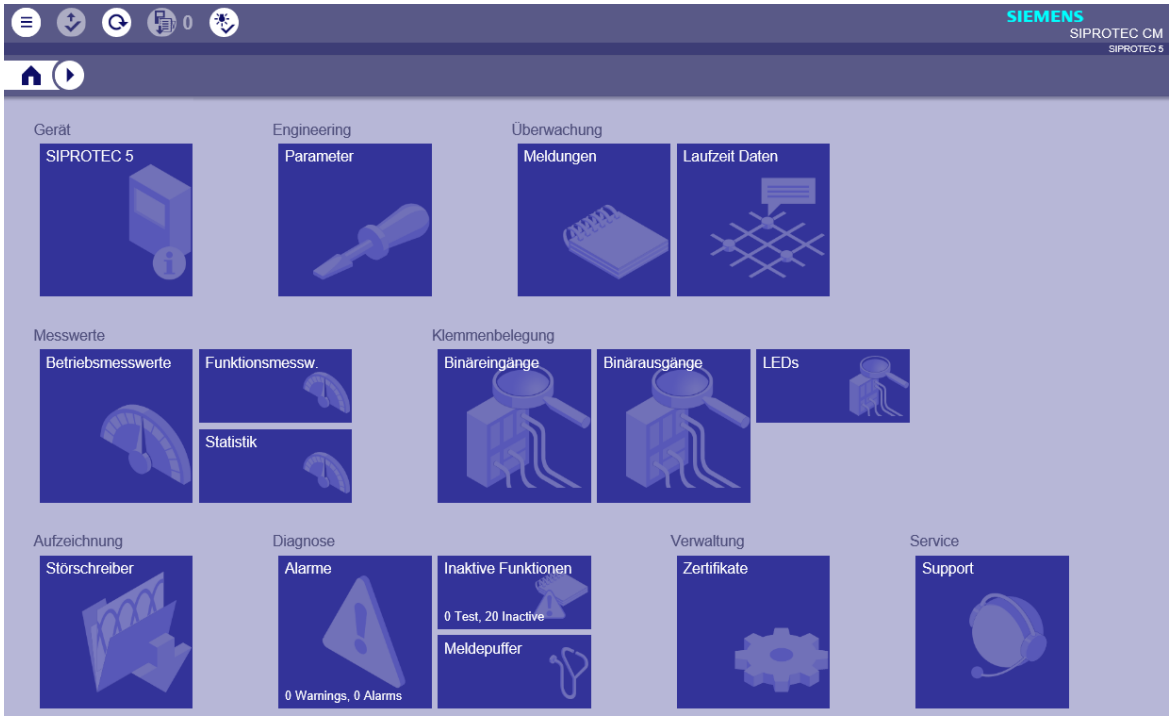
- Klicken Sie auf die Schaltfläche mit dem Häkchen.



[scwebmonitor_enter, 1, --_--]

Bild 5-4 Schaltfläche zur Bestätigung

Nach erfolgreicher Anmeldung stehen folgende Schaltflächen zur Verfügung:



[sc_webUI, 1, de_DE]

Bild 5-5 Schaltflächen für die browser-basierte Benutzeroberfläche

Sie können die entsprechenden Bereiche anzeigen oder diese durch Klicken auf die verschiedenen Schaltflächen bearbeiten.

Zeitüberschreitung

HINWEIS

Wenn innerhalb eines festgelegten Zeitraums keine Benutzeraktion auf der **browser-basierten Benutzeroberfläche** verzeichnet wird, wird die Verbindung vom Web-Browser zum Gerät getrennt.

Die folgende Meldung wird angezeigt:



[scwebmonitor14, 1, de_DE]

Bild 5-6 Zeitüberschreitung

Nach Ablauf einer bestimmten Zeit müssen Sie sich erneut über den Web-Browser am Gerät anmelden.

6 Certificate Management

6.1	Einleitung	62
6.2	Zertifikate im Einsatz	64
6.3	Zertifizierungsstellen	65
6.4	Angeforderte Zertifikate	66

6.1 Einleitung

Mit der **Zertifikatsverwaltung** können Sie digitale Zertifikate verwalten. Diese umfasst z.B. folgende Prozesse:

- Prüfung aktueller Zertifikate
- Herunterladen von CSR-Dateien (Certificate Signing Request)
- Hochladen von Zertifikaten
- Löschen von Zertifikaten

Bei aktiver RBAC wird mit der Rolle **SECADM** oder **Administrator** bei der **browser-basierten Benutzeroberfläche** die Schaltfläche **Zertifikate** angezeigt.



[sc_certificates_button, 1, de_DE]

Wenn Sie die Schaltfläche **Zertifikate** klicken, werden die folgenden Bereiche angezeigt:

- Zertifikate im Einsatz
- Zertifizierungsstellen
- Angeforderte Zertifikate

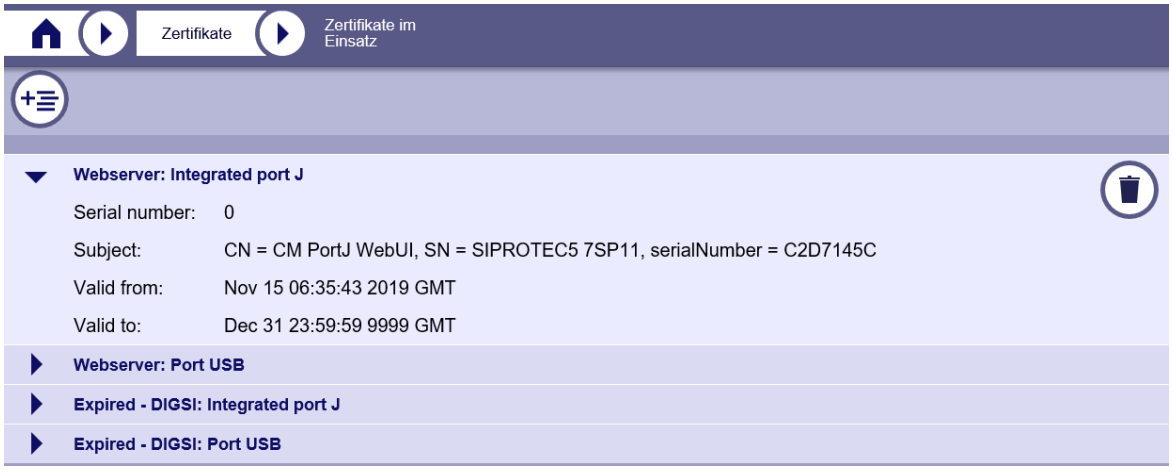


[sc_CM, 1, de_DE]

Nähere Informationen zu diesen Bereichen finden Sie in den folgenden Kapiteln.

6.2 Zertifikate im Einsatz

Die Zertifikate, die derzeit im Gerät verwendet werden, werden im Bereich **Zertifikate im Einsatz** angezeigt. In diesem Bereich können Sie Zertifikate auch hochladen oder löschen.



[sc_certificates, 1, de_DE]

HINWEIS

Nur Zertifikate im Format .pem werden zum Hochladen in die Geräte akzeptiert.

6.3 Zertifizierungsstellen

Wenn Sie in DIGSI 5 Ihre Zertifizierungsstellen in den **DIGSI 5 CA-Store** importiert haben und die Zertifizierungsstellen in das Gerät geladen haben, werden die Zertifizierungsstellen bei der **browser-basierten Benutzeroberfläche** im Bereich **Zertifizierungsstellen** angezeigt.



[sc_Cert.Auth., 1, de_DE]

6.4 Angeforderte Zertifikate

Wenn Sie eine zertifikatsbezogene Funktion in DIGSI 5 aktivieren und ins Gerät laden, erzeugt das Gerät automatisch eine entsprechende CSR-Datei. Diese CSR-Dateien werden im Bereich **Angeforderte Zertifikate** aufgeführt.

Mit der Schaltfläche für den Export können Sie eine CSR-Datei zur Signierung auf Ihren lokalen PC herunterladen.



[sc_crt_export, 1, de_DE]

7 Backup and Restore

7.1	Allgemein	68
7.2	Archivieren und Dearchivieren eines Projekts	69

7.1 Allgemein

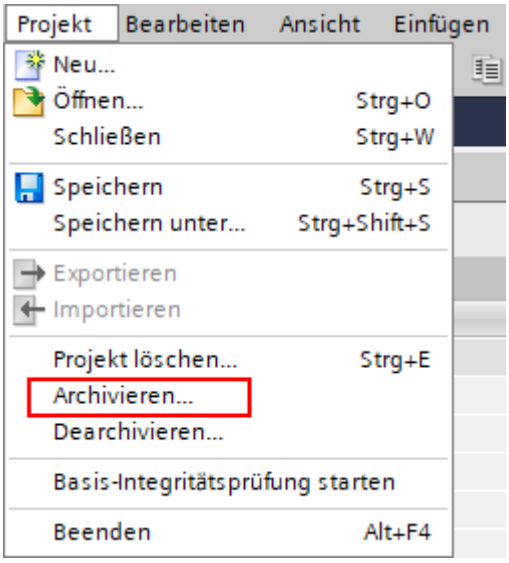
DIGSI 5 verwaltet die Komponenten einer Anlage und alle damit verbundenen Projektdaten. Projekte sind in Windows als Ordner strukturiert. Wenn die Voreinstellung nicht geändert wurde, finden Sie die Projektordner unter **Eigene Dateien\Automatisierung**. Für jedes Projekt wird ein Ordner mit dem Namen des Projektes erstellt.

7.2 Archivieren und Dearchivieren eines Projekts

Um ein Projekt als Sicherungsdatei zu speichern und zu einem späteren Zeitpunkt zu dearchivieren, können Sie das in DIGSI 5 erstellte Projekt unter demselben oder einem anderen Namen am gewünschten Speicherort archivieren. Nachdem Sie das aktuell geöffnete Projekt in DIGSI 5 archiviert haben, können Sie es weiter bearbeiten, ohne es zu schließen. Bei Bedarf können Sie die archivierte Version des Projekts jederzeit dearchivieren und weiter bearbeiten.

Archivieren eines Projekts

✧ Klicken Sie im Menü **Projekt** auf **Archivieren...**.

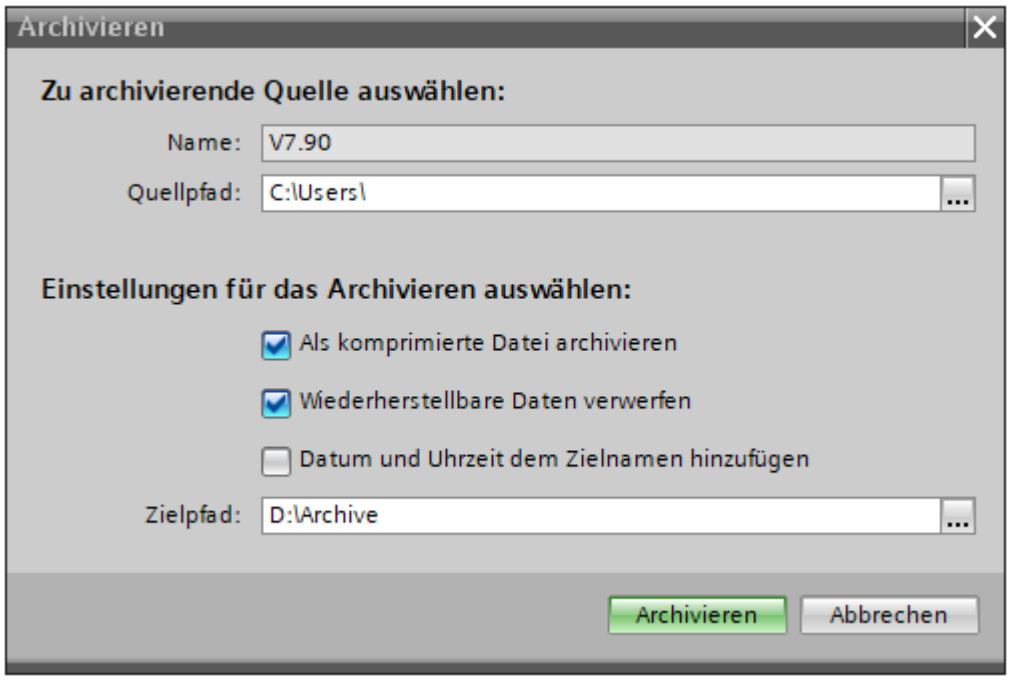


[sc_ProjectMenu, 1, de_DE]

Bild 7-1 Menüeintrag Archivieren

Der Dialog **Archivieren** wird mit dem Standarddateinamen geöffnet.

✧ Wenn erforderlich, geben Sie den neuen Archivpfad ein.



[sc_ArchiveProject, 1, de_DE]

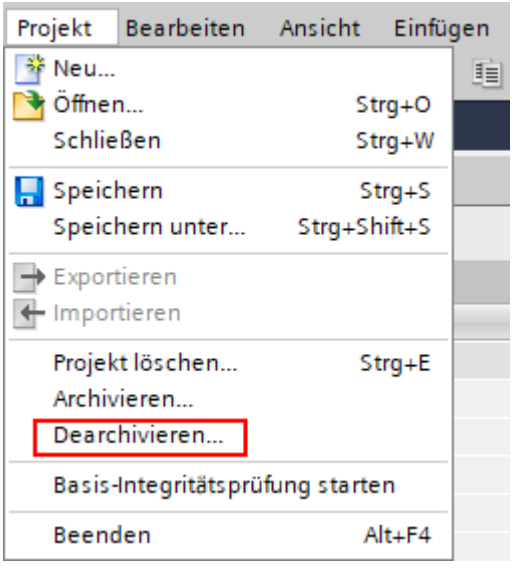
Bild 7-2 Dialog Archivieren

✧ Klicken Sie **Archivieren**.
Ein Fortschrittsdialog wird angezeigt, in dem der Archivierungsstatus angezeigt wird.

Die archivierte Projektdatei wird am gewünschten Speicherort mit der Dateierweiterung **.dz5** gespeichert.

Dearchivieren eines archivierten Projekts

✧ Klicken Sie im Menü **Projekt** auf **Dearchivieren...**.



[sc_ProjectMenu2, 1, de_DE]

Bild 7-3 Menüeintrag Dearchivieren

✧ Wählen Sie im entsprechenden Ordner das archivierte Projekt mit der Dateierweiterung **.dz5**.

✧ Wählen Sie das Zielverzeichnis aus, in dem Sie das dearchivierte Projekt speichern möchten.

Das dearchivierte Projekt wird in DIGSI 5 geöffnet.

8 Security Logging

8.1	Übersicht	74
8.2	Unterstützte System- und Firmware-Versionen	75
8.3	Logged Security Events	76
8.4	Configuration	90
8.5	Auditberichte anzeigen	98

8.1 Übersicht

SIPROTEC 5-Geräte und DIGSI 5 bieten einen Sicherheitsaudit-Trail, der sicherheitsrelevante Ereignisse chronologisch aufzeichnet und nach Ursprung und Schweregrad kategorisiert.

Die SIPROTEC 5-Geräte senden die sicherheitsrelevanten Ereignisse automatisch an einen externen syslog-Server, DIGSI 5 sendet solche Ereignisse an das Windows Ereignisprotokoll.

Die Übertragung der Sicherheitsereignisse an den/die konfigurierten syslog-Server erfolgt bei Auftreten des Sicherheitsereignisses spontan und ohne Bestätigung über UDP (User Datagram Protocol). Die aufgezeichneten Sicherheitsereignisse können im Nachhinein aus dem geräteinternen Sicherheitsereignispuffer ausgelesen werden. Die Sicherheitsereignisse werden auf Englisch angezeigt.



HINWEIS

Auf dem/den syslog-Server/n empfiehlt Siemens, die empfangenen Sicherheitsereignisse vor unbefugtem Lese- und Schreibzugriff durch die Rolle Auditor zu schützen.

8.2 Unterstützte System- und Firmware-Versionen

Die folgende Tabelle zeigt die System- und Firmware-Versionen, die syslog unterstützen:

System	Firmware	Version	Unterstützte Schnittstelle
SIPROTEC 5	CP100 CP300	V07.50 oder höher	• Port J • Port E • Port F • Port P • Port N

8.3 Logged Security Events

8.3.1 Aufbau von Sicherheitsereignissen

Ein syslog-Ereignis besteht aus folgenden Elementen:

Element	Beschreibung
Schweregrad	Schweregrade des Ereignisses: • Ereignis • Alarm
Daten	Datum, an dem das Ereignis vom syslog-Server empfangen oder protokolliert wurde
Zeit	Uhrzeit, zu der das Ereignis vom syslog-Server empfangen oder protokolliert wurde • T Zeit • hh:mm:ss.ttt Uhrzeit des Auftretens des Ereignisses • +hh:mm Zeitabweichung von GMT
IP-Adresse	IP-Adresse des Produktes oder der untergeordneten Komponente, die den Protokolleintrag generiert
Modulname	Name des Produktmoduls, das den Protokolleintrag generiert
BOM	Byte Order Mark für UTF8-Kodierung
Produktname	Name des Produkts, das den Protokolleintrag generiert
Meldungstext	Der Meldungsteil eines syslog-Ereignisses Abhängig vom Ereignis kann der Meldungstext verschiedene zusätzliche Angaben (%A1%, %A2%, %A3% und %A4%) enthalten.

8.3.2 Syslog-Ereignisse SIPROTEC 5



HINWEIS

Die Anzeige von Sicherheitsmeldepuffern wird von der **browser-basierten Benutzeroberfläche** nicht unterstützt.

Schweregrad Ereignis

Die folgende Tabelle zeigt die syslog-Ereignisse mit Schweregrad ***Ereignis***.

Tabelle 8-1 Syslog-Ereignisse mit Schweregrad Ereignis

Syslog-Ereignis	Zusätzliche Angaben 1 (%A1%)	Zusätzliche Angaben 2 (%A2%)	Zusätzliche Angaben 3 (%A3%)	Zusätzliche Angaben 4 (%A4%)
The storage capacity of the security audit buffer has decreased below the set threshold of %A1% entries. (Die Speicherkapazität des Sicherheitsauditpuffers ist unter den eingestellten Schwellwert von %A1% gesunken.)	Der Schwellwert der vom Benutzer eingestellten Speicherkapazität oder Standardwert (80 %)	–	–	–
The user %A1% has initiated a remote session from %A2% with role(s) %A3%. (Der Benutzer %A1% hat eine Fernsitzung von %A2% mit der/den Rolle/n %A3% initiiert.)	Konto-ID	IP-Adresse des Fernbedienplatzes	Die dem Benutzer zugewiesenen Rollen, mit Komma als Listentrennzeichen.	–
A user has initiated a remote session from %A1%. (Ein Benutzer hat eine Fernsitzung von %A1% initiiert.)	Die dem Benutzer zugewiesenen Rollen, mit Komma als Listentrennzeichen.	–	–	–
A user has initiated a local session with role(s) %A1%. (Der Benutzer hat eine lokale Sitzung mit der/den Rolle/n %A1% initiiert.)	Die dem Benutzer zugewiesenen Rollen, mit Komma als Listentrennzeichen.	–	–	–
A user has initiated a local session. (Der Benutzer hat eine lokale Sitzung initiiert.)	–	–	–	–
The user %A1% has logged out. (Der Benutzer %A1% hat sich abgemeldet.)	Konto-ID	–	–	–
The user has ended an interactive session. (Der Benutzer hat eine interaktive Sitzung beendet.)	–	–	–	–
The interactive session with the user %A1% has been terminated due to the timeout (%A2%). (Die interaktive Sitzung mit dem Benutzer %A1% wurde aufgrund einer Zeitüberschreitung (%A2%) beendet.)	Konto-ID	Durch den Benutzer eingestellter Schwellwert für die Zeitüberschreitung oder Standardwert (10 Minuten) für die Zeit ohne Benutzeraktion; nach dieser Zeitspanne wird die bestehende interaktive Benutzersitzung beendet	–	–

Syslog-Ereignis	Zusätzliche Angaben 1 (%A1%)	Zusätzliche Angaben 2 (%A2%)	Zusätzliche Angaben 3 (%A3%)	Zusätzliche Angaben 4 (%A4%)
A user-interactive session has been terminated due to the time-out (%A1%). (Die interaktive Sitzung wurde aufgrund einer Zeitüberschreitung (%A1%) beendet.)	Durch den Benutzer eingestellter Schwellwert für die Zeitüberschreitung oder Standardwert (10 Minuten) für die Zeit ohne Benutzeraktion; nach dieser Zeitspanne wird die bestehende interaktive Benutzersitzung beendet	–	–	–
The password protection of type %A1% has been disabled. (Der Passwortschutz vom Typ %A1% wurde deaktiviert.)	Text, der den Zweck des Passwortes eindeutig festlegt. Beim Verbindungspasswort für SIPROTEC 5 sollte hier z.B. ***connection password*** stehen.	–	–	–
User manually overrode real data. (Der Benutzer hat Realdaten manuell überschrieben.)	–	–	–	–
User manually overrode real data from %A1%. (Der Benutzer hat Realdaten von %A1% manuell überschrieben.)	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	–	–	–
User %A1% manually overrode real data (Benutzer %A1% hat Realdaten manuell überschrieben) [//Protokollierung durch Produkte, die RBAC unterstützen]	Konto-ID	–	–	–

Syslog-Ereignis	Zusätzliche Angaben 1 (%A1%)	Zusätzliche Angaben 2 (%A2%)	Zusätzliche Angaben 3 (%A3%)	Zusätzliche Angaben 4 (%A4%)
User %A1% manually overrode real data from %A2% (Benutzer %A1% hat echte Daten von %A2% manuell überschrieben) [//Protokollierung durch Produkte, die RBAC unterstützen]	Konto-ID	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	–	–
User caused a control operation %A1%. (Benutzer hat Steuerungshandlung %A1% ausgelöst.) Zusätzliche Angaben: %A2%	Der Typ der ausgeführten Steuerungshandlung, z.B. Deaktivierung des Leistungsschalters	Zusätzliche Angaben zur Steuerungshandlung, z.B. <FG.FN.FB.Signalname des Leistungsschalters gemäß DIGSI 5-Betriebsmeldepuffer>	–	–
User caused a control operation from %A1%: %A2%. (Benutzer hat Steuerungshandlung von %A1% ausgelöst: %A2%.) Zusätzliche Angaben: %A3%	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	Der Typ der ausgeführten Steuerungshandlung, z.B. Deaktivierung des Leistungsschalters	Zusätzliche Angaben zur Steuerungshandlung, z.B. <FG.FN.FB.Signalname des Leistungsschalters gemäß DIGSI 5-Betriebsmeldepuffer>	–
User %A1% caused a control operation: %A2%. (Benutzer %A1% hat Steuerungshandlung ausgelöst: %A2%.) Zusätzliche Angaben: %A3%	Konto-ID	–	Zusätzliche Angaben zur Steuerungshandlung, z.B. <FG.FN.FB.Signalname des Leistungsschalters gemäß DIGSI 5-Betriebsmeldepuffer>	–
User %A1% caused a control operation from %A2%: %A3%. (Benutzer %A1% hat Steuerungshandlung von %A2% ausgelöst: %A3%.) Zusätzliche Angaben: %A4%	Konto-ID	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	Der Typ der ausgeführten Steuerungshandlung, z.B. Deaktivierung des Leistungsschalters	Zusätzliche Angaben zur Steuerungshandlung, z.B. <FG.FN.FB.Signalname des Leistungsschalters gemäß DIGSI 5-Betriebsmeldepuffer>

Syslog-Ereignis	Zusätzliche Angaben 1 (%A1%)	Zusätzliche Angaben 2 (%A2%)	Zusätzliche Angaben 3 (%A3%)	Zusätzliche Angaben 4 (%A4%)
Configuration settings were downloaded from %A1%. (Konfigurationseinstellungen wurden von %A1% heruntergeladen.)	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	–	–	–
User %A1% downloaded configuration settings from %A2%. (Benutzer %A1% hat Konfigurationseinstellungen von %A2% heruntergeladen.)	Konto-ID	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	–	–
Configuration settings were uploaded from %A1%. (Konfigurationseinstellungen wurden von %A1% hochgeladen.)	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	–	–	–
User %A1% uploaded configuration settings from %A2%. (Benutzer %A1% hat Konfigurationseinstellungen von %A2% hochgeladen.)	Konto-ID	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	–	–
Configuration settings were changed (Konfigurationseinstellungen wurden geändert)	–	–	–	–

Syslog-Ereignis	Zusätzliche Angaben 1 (%A1%)	Zusätzliche Angaben 2 (%A2%)	Zusätzliche Angaben 3 (%A3%)	Zusätzliche Angaben 4 (%A4%)
Configuration settings were changed using %A1% (Konfigurationseinstellungen wurden mit %A1% geändert)	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	–	–	–
User %A1% changed configuration settings. (Benutzer %A1% hat Konfigurationseinstellungen geändert.)	Konto-ID	Der benutzerbezogene Name des Produkts, bei dem die Konfiguration hochgeladen wurde, zum Beispiel Schutzgerät über Web oder Frontabdeckung	–	–
User %A1% changed configuration settings from %A2%. (Benutzer %A1% hat Konfigurationseinstellungen von %A2% geändert.)	Konto-ID	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	–	–
Firmware version %A1% was uploaded from %A2%. (Firmware-Version %A1% wurde von %A2% hochgeladen.)	Version der hochgeladenen Firmware	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	–	–

Syslog-Ereignis	Zusätzliche Angaben 1 (%A1%)	Zusätzliche Angaben 2 (%A2%)	Zusätzliche Angaben 3 (%A3%)	Zusätzliche Angaben 4 (%A4%)
User %A1% uploaded firmware file from %A2%. (Benutzer %A1% hat Firmware-Datei von %A2% hochgeladen.)	Konto-ID	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	–	–
Audit log was viewed. (Auditbericht wurde eingesehen.)	–	–	–	–
Audit log was downloaded from %A2%. (Auditbericht wurde von %A2% heruntergeladen.)	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	–	–	–
User %A1% viewed audit log. (Benutzer %A1% hat Auditbericht eingesehen.)	Konto-ID	–	–	–
User %A1% viewed audit log from %A2%. (Benutzer %A1% hat Auditbericht von %A2% eingesehen.)	Konto-ID	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	–	–
A change to time/date was carried out. (Zeit oder Datum wurde geändert.)	–	–	–	–

Syslog-Ereignis	Zusätzliche Angaben 1 (%A1%)	Zusätzliche Angaben 2 (%A2%)	Zusätzliche Angaben 3 (%A3%)	Zusätzliche Angaben 4 (%A4%)
A change to time/date was carried out from %A1%. (Uhrzeit/Datum wurde geändert von %A1%.)	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	–	–	–
User %A1% changed time/ date. (Benutzer %A1% hat Uhrzeit/Datum geändert.)	Konto-ID	–	–	–
User %A1% changed time/ date from %A2%. (Benutzer %A1% hat Uhrzeit/Datum von %A2% geändert.)	Konto-ID	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	–	–
A hardware change has been detected: %A1%. (Eine Änderung der Hardware wurde festgestellt: %A1%.)	Die erkannte Änderung, z.B., wenn eine I/O-Baugruppe in einen I/O-Steckplatz gesteckt wird.	–	–	–
Settings related to user management were changed: %A1% (set to value %A2%). (Parameter für die Benutzerverwaltung wurden geändert: %A1% (auf Wert %A2% gesetzt).)	Der Name des geänderten Parameters	Der neue Parameterwert	–	–
Settings related to user authentication were changed: %A1% (set to value %A2%). (Parameter für die Benutzerauthentifizierung wurden geändert: %A1% (auf Wert %A2% gesetzt).)	Der Name des geänderten Parameters	Der neue Parameterwert	–	–
Settings related to secure communication were changed:%A1% (set to value %A2%). (Parameter für die sichere Kommunikation wurden geändert: %A1% (auf Wert %A2% gesetzt).)	Der Name des geänderten Parameters	Der neue Parameterwert	–	–

Syslog-Ereignis	Zusätzliche Angaben 1 (%A1%)	Zusätzliche Angaben 2 (%A2%)	Zusätzliche Angaben 3 (%A3%)	Zusätzliche Angaben 4 (%A4%)
Settings related to offline security monitoring were changed: %A1% (set to value %A2%). (Parameter für die Offline-Sicherheitsüberwachung wurden geändert: %A1% (auf Wert %A2% gesetzt).)	Der Name des geänderten Parameters	Der neue Parameterwert	–	–
Settings related to online security monitoring were changed: %A1% (set to value %A2%). (Parameter für die Online-Sicherheitsüberwachung wurden geändert: %A1% (auf Wert %A2% gesetzt).)	Der Name des geänderten Parameters	Der neue Parameterwert	–	–
User %A1% changed settings related to user management: %A2% (set to value %A3%). (Benutzer %A1% hat Parameter für die Benutzerverwaltung geändert: %A2% (auf Wert %A3% gesetzt).)	Konto-ID	Der Name des geänderten Parameters	Der neue Parameterwert	–
User %A1% changed settings related to user authentication: %A2% (set to value %A3%). (Benutzer %A1% hat Parameter für die Benutzerauthentifizierung geändert: %A2% (auf Wert %A3% gesetzt).)	Konto-ID	Der Name des geänderten Parameters	Der neue Parameterwert	–
User %A1% changed settings related to secure communication:%A2% (set to value %A3%). (Benutzer %A1% hat Parameter für die sichere Kommunikation geändert: %A2% (auf Wert %A3% gesetzt).)	Konto-ID	Der Name des geänderten Parameters	Der neue Parameterwert	–
User %A1% changed settings related to offline security monitoring: %A2% (set to value %A3%). (Benutzer %A1% hat Parameter für die Offline-Sicherheitsüberwachung geändert: %A2% (auf Wert %A3% gesetzt).)	Konto-ID	Der Name des geänderten Parameters	Der neue Parameterwert	–
User %A1% changed settings related to online security monitoring: %A2% (set to value %A3%). (Benutzer %A1% hat Parameter für die Online-Sicherheitsüberwachung geändert: %A2% (auf Wert %A3% gesetzt).)	Konto-ID	Der Name des geänderten Parameters	Der neue Parameterwert	–

Syslog-Ereignis	Zusätzliche Angaben 1 (%A1%)	Zusätzliche Angaben 2 (%A2%)	Zusätzliche Angaben 3 (%A3%)	Zusätzliche Angaben 4 (%A4%)
The configuration tool was started. (Das Konfigurationswerkzeug wurde gestartet.)	–	–	–	–
User %A1% logged in with role(s) %A2%. (Benutzer %A1% hat sich mit der/den Rolle/n %A2% angemeldet.)	Konto-ID	Die dem Benutzer zugewiesenen Rollen, mit Komma als Listentrennzeichen	–	–
The configuration tool was closed. (Das Konfigurationswerkzeug wurde geschlossen.)	–	–	–	–
User %A1% logged out. (Benutzer %A1% hat sich abgemeldet.)	Konto-ID	–	–	–
Primary %A1% server %A2% check failed (Primärer %A1% Server %A2% Prüfung fehlgeschlagen)	Protokoll (RADIUS)	IP-Adresse	–	–

Schweregrad Alarm

Die folgende Tabelle zeigt die syslog-Ereignisse mit Schweregrad ***Alarm***.

Tabelle 8-2 Syslog-Ereignisse mit Schweregrad Alarm

Syslog-Ereignis	Zusätzliche Angaben 1 (%A1%)	Zusätzliche Angaben 2 (%A2%)	Zusätzliche Angaben 3 (%A3%)	Zusätzliche Angaben 4 (%A4%)
While logging on to user account %A1% (%A2%-managed account) from %A3%, 3 incorrect password entries in succession were attempted. (Bei der Anmeldung an Benutzerkonto %A1% (%A2%-verwaltetes Konto) von %A3% wurde das Passwort 3-mal hintereinander falsch eingegeben.)	Konto-ID	Kontotypen: • Beim produktverwalteten (lokalen) Benutzerkonto ist der Kontotyp der Produktname. • Beim AD-Benutzer ist der Kontotyp LDAP. • Beim RADIUS-Benutzer ist der Kontotyp ***RADIUS***.	%A3% kann Folgendes sein: • Der benutzerbezogene Name des Produkts, bei dem Anmeldeversuche erkannt wurden • Wenn ein Fernbedienplatz verwendet wird, ist %A3% die IP-Adresse des Fernbedienplatzes. • Bedieneinheit des Gerätes	–
Repeated attempt to log on to user account %A1% (%A2%-managed account) from %A3%. (Wiederholter Anmeldeversuch an Benutzerkonto %A1% (%A2%-verwaltetes Konto) von %A3%.)	Konto-ID	Kontotypen: • Beim produktverwalteten (lokalen) Benutzerkonto ist der Kontotyp der Produktname. • Beim AD-Benutzer ist der Kontotyp LDAP. • Beim RADIUS-Benutzer ist der Kontotyp ***RADIUS***.	Dies kann Folgendes sein: • Der benutzerbezogene Name des Produkts, bei dem Anmeldeversuche erkannt wurden • Wenn ein Fernbedienplatz verwendet wird, ist %A3% die IP-Adresse des Fernbedienplatzes. • Bedieneinheit des Gerätes	–

Syslog-Ereignis	Zusätzliche Angaben 1 (%A1%)	Zusätzliche Angaben 2 (%A2%)	Zusätzliche Angaben 3 (%A3%)	Zusätzliche Angaben 4 (%A4%)
User account %A1% (%A2%-managed account) blocked for the next %A3% minutes after too many attempts to log on unsuccessfully from %A4% (Benutzerkonto %A1% (%A2%-verwaltetes Konto) für die nächsten %A3% Minuten gesperrt aufgrund zu vieler erfolgloser Anmeldeversuche von %A4%)	Konto-ID	Kontotypen: • Beim produktverwalteten (lokalen) Benutzerkonto ist der Kontotyp der Produktname. • Beim AD-Benutzer ist der Kontotyp LDAP. • Beim RADIUS-Benutzer ist der Kontotyp ***RADIUS***.	Die eingestellte Blockierdauer des Kontos in Minuten	Dies kann Folgendes sein: • Der benutzerbezogene Name des Produkts, bei dem Anmeldeversuche erkannt wurden • Wenn ein Fernbedienplatz verwendet wird, ist %A3% die IP-Adresse des Fernbedienplatzes. • Bedieneinheit des Gerätes
Restart initiated (with action: %A1%) (Neustart initiiert (mit Aktion: %A1%))	Zusätzliche Angaben zur genauen Aktion, die den Neustart ausgelöst hat, z.B. Betriebstaste, SD-Karte eingeführt, etc.	–	–	–
Restart initiated from %A1% (with action: %A2%) (Neustart initiiert von %A1% (mit Aktion: %A2%))	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	Zusätzliche Angaben zur genauen Aktion, die den Neustart ausgelöst hat, z.B. Parameterübertragung	–	–
User %A1% initiated restart (with action: %A2%). (Benutzer %A1% hat Neustart initiiert (Mit Aktion: %A2%).)	Konto-ID	Zusätzliche Angaben zur genauen Aktion, die den Neustart ausgelöst hat, z.B. Betriebstaste, SD-Karte eingeführt, etc.	–	–

Syslog-Ereignis	Zusätzliche Angaben 1 (%A1%)	Zusätzliche Angaben 2 (%A2%)	Zusätzliche Angaben 3 (%A3%)	Zusätzliche Angaben 4 (%A4%)
User %A1% initiated restart from %A2% (with action: %A3%). (Benutzer %A1% hat Neustart von %A2% initiiert (Mit Aktion: %A3%).)	Konto-ID	Vom Benutzer gewählter Fernbedienplatz (z.B. Engineering-Werkzeug), von dem aus die Änderungen durchgeführt werden sollen. Wenn Software für den PC verwendet wird, dann ist dies die IP-Adresse des Rechners.	Zusätzliche Angaben zur genauen Aktion, die den Neustart ausgelöst hat, z.B. Parameterübertragung	–
Attempted use of illegitimate configuration software (from %A1%) (Versuchter Einsatz unrechtmäßiger Konfigurationssoftware (von %A1%))	Die IP-Adresse des PC, auf dem die nicht autorisierte Software erkannt wurde	–	–	–
Attempted download of invalid configuration settings (from %A1%) (Versuchter Download ungültiger Konfigurationseinstellungen (von %A1%))	Die Quelle der unberechtigten Konfigurationen, z.B. die IP-Adresse des PC, SD-Karte, etc.	–	–	–
Attempted download of invalid firmware file(s) (from %A1%) (Versuchter Download ungültiger Firmware-Datei(en) (von %A1%))	Die Quelle der unberechtigten Konfigurationen, z.B. die IP-Adresse des PC, SD-Karte, etc.	–	–	–
Attempted download of unauthorized configuration settings (from %A1%) (Versuchter Download nicht autorisierter Konfigurationseinstellungen (von %A1%))	Die Quelle der unberechtigten Konfigurationen, z.B. die IP-Adresse des PC, SD-Karte, etc.	–	–	–
Attempted download of unauthorized firmware file(s) (from %A1%) (Versuchter Download nicht autorisierter Firmware-Datei(en) (von %A1%))	Die Quelle der unberechtigten Firmware-Datei(en), z.B. die IP-Adresse des PC, SD-Karte, etc.	–	–	–

Syslog-Ereignis	Zusätzliche Angaben 1 (%A1%)	Zusätzliche Angaben 2 (%A2%)	Zusätzliche Angaben 3 (%A3%)	Zusätzliche Angaben 4 (%A4%)
Time synchronization message is outside of the internal clock. (Zeitsynchronisationsmeldung weicht vom internen Zeitgeber ab.)	–	–	–	–
An improper user-performed field hardware change has been detected: %A1%. (Eine unsachgemäße Änderung der Hardware durch den Benutzer wurde festgestellt: %A1%.)	Die erkannte unsachgemäße Änderung, z.B., wenn eine falsche I/O-Baugruppe in einen I/O-Steckplatz gesteckt wird.	–	–	–

8.4 Configuration

8.4.1 Übersicht

Um Cyber-Security-Ereignisse beim Betrieb von SIPROTEC 5-Geräten aufzuzeichnen, werden Schriebe automatisch erstellt und die Daten werden gesammelt. Alle im geräteinternen Sicherheitsmeldepuffer aufgezeichneten sicherheitsrelevanten Ereignisse und Alarme können gleichzeitig auch an einen zentralen syslog-Server übertragen werden. Dadurch können sicherheitsrelevante Ereignisse von mehreren Transformatorstationen aufgezeichnet werden, die Normen und Richtlinien wie etwa IEEE 1686, IEC 62443 und BDEW Whitepaper erfüllen müssen. Die Protokollierung wird zentral auf 1 oder 2 selbstgewählten syslog-Servern gestartet. Die Kombination verschiedener Protokolldaten der verwendeten Geräte ermöglicht einen allgemeinen Überblick über das Gerätenetzwerk. Sie können diese Daten analysieren und überwachen. Dadurch können sicherheitskritische Ereignisse protokolliert und entsprechende Änderungen verfolgt werden. Sie können mithilfe der Protokolldaten auch Angriffe auf die betriebenen Geräte verfolgen.

Sie können die gesammelten Protokolldaten im Sicherheitsmeldepuffer lokal auf dem Geräte-Display anzeigen, unabhängig von der aktuellen Betriebsart des Gerätes. Die Alarme und sicherheitskritischen Meldungen werden chronologisch im Sicherheitsmeldepuffer gespeichert. Sie können diese Einträge nicht verändern oder löschen.

Sie können z.B. folgende Fragen beantworten:

- Wie viele Anmeldeversuche wurden vorgenommen?
- Wann wurde die Gerätekonfiguration zuletzt aktualisiert?

Die vollständige Liste der aufgezeichneten Sicherheitsereignisse finden Sie unter *Aufzeichnungen, Seite 92*.

Zentralen syslog-Server konfigurieren

Nachdem Sie DIGSI 5 gestartet haben und die Verbindung zu einem Gerät hergestellt haben, wählen Sie in der Projektnavigation **Sicherheit** > **Security-Ereignisprotokoll**. Der Menüeintrag **Sicherh. Prot.** enthält die Einstellalternativen für einen zentralen syslog-Server. Sie können bis zu 2 syslog-Server aktivieren.

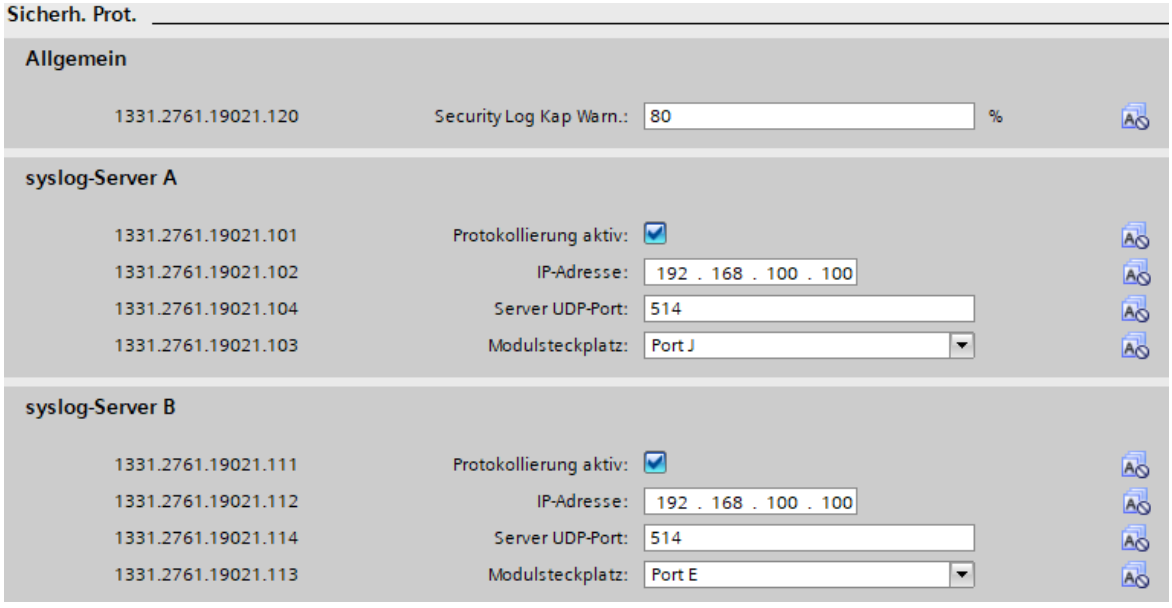
Im Bereich **Allgemein** legen Sie die Warnschwelle für die Kapazität des geräteinternen Sicherheitsmeldepuffers fest.

Die Protokollierung aktivieren Sie unter **syslog-Server A** und/oder **B**. Geben Sie folgende Informationen ein:

- IP-Adresse
- Server UDP-Port
- Modulsteckplatz

Weitere Informationen zum Sicherheitsmeldepuffer finden Sie im Kapitel *8.3 Logged Security Events*

Bild 8-1 zeigt beispielhaft die Einstellung der IP-Adressen und Ports zweier syslog-Server in DIGSI 5.



[sc_event_logging, 3, de_DE]

Bild 8-1 Einstellbeispiel für die IP-Adressen und Ports der syslog-Server

Mit dem einstellbaren Schwellwert **Security Log Kap.Warn.** können Sie festlegen, ab welcher Nutzung des Sicherheitsmeldepuffers eine Warnmeldung ausgegeben wird. Eine Warnschwelle von 80 % bedeutet, dass der eingestellte Kapazitätsgrenzwert nach ca. 1600 Einträgen im Sicherheitsmeldepuffer erreicht ist. Weitere Warnmeldungen werden ausgegeben, wenn die Kapazitätsgrenzwerte 85 %, 90 %, 95 % und 98 % erreicht werden.

Wenn das als Ringspeicher organisierte Protokoll die Kapazitätsgrenze von 100 % überschreitet, werden die ältesten Einträge automatisch überschrieben und die Kapazitätsauslastung wird auf 0 % zurückgesetzt.

Wenn Sie den Sicherheitsmeldepuffer mit DIGSI 5 auslesen, wird die Kapazitätsauslastung auf 0 % zurückgesetzt. Die Meldungen bleiben im Gerät erhalten. Sie müssen alle Einstellungen mit DIGSI 5 vornehmen.

HINWEIS

Wenn Sie die Firmware auf eine frühere Version als V07.50 einstellen, wird die geräteinterne Protokollgröße vom derzeitigen Wert von 2048 Einträgen auf 500 Einträge verkleinert. Die ältere Firmware unterstützt nur 500 Einträge in einem anderen Format. In diesem Fall werden die neuesten 500 Einträge aus dem aktuellen/syslog-fähigen Gerätestatus und Format übernommen und im älteren Format, das für die Firmware geeignet ist, angelegt. Die restlichen Einträge gehen verloren.

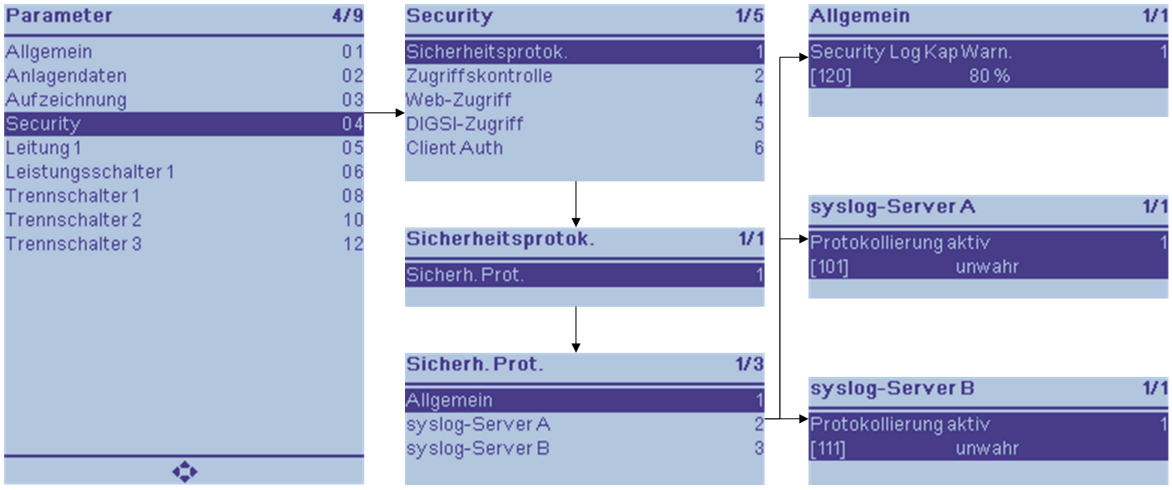
Nach dem Downgrade wird der Inhalt des internen Protokolls mit seinen 2048 Einträgen gelöscht. Als neuester Eintrag im umgestellten Protokoll nach dem Downgrade wird eine Meldung zum erfolgten Firmware-Downgrade angezeigt.

Anzeige über die Vor-Ort-Bedieneinheit

Auf dem Geräte-Display können Sie die Einstellungen für die verwendeten syslog-Server prüfen. *Bild 8-2* zeigt beispielhaft die Einstellungen für Port und IP-Adressen eines syslog-Servers am Gerät.

Wählen Sie auf dem Geräte-Display Folgendes aus:

- Hauptmenü > **Parameter** > **Security** > **Sicherheitsprotok.**



[le_menu_central_logging, 1, de_DE]

Bild 8-2 Gerätemenü für syslog-Server

Aufzeichnungen

Folgende Elemente werden im Sicherheitsmeldepuffer protokolliert und an einen verbundenen syslog-Server weitergeleitet:

- Aktionen
  - Erfolgreiche Abmeldung eines Benutzers, auch nach einer bestimmten Zeitspanne
  - Erfolgreiche Anmeldung eines Benutzers
  - Änderung oder Löschen des Verbindungspassworts
  - Aktualisierung oder Wiederherstellung der Firmware-Version des Gerätes
  - Aktualisierung der Konfiguration im Gerät
  - Änderung der Betriebsart des Gerätes
  - Änderung von Datum und Uhrzeit
  - Änderung oder Überschreiben von Einträgen zu den Zustandswerten durch den angemeldeten Benutzer
  - Schalthandlungen durch den registrierten Benutzer
- Potentielle Fehler
  - Anzahl der Einträge mit richtigen oder falschen Passwörtern
  - Nicht erfolgreiche Anmeldeversuche durch dreimalige falsche Eingabe des Passworts
  - Reboot oder Neustart des Gerätes
- Andere Einträge
  - Kapazitätswarnung des Sicherheitsmeldepuffers

Die folgende Tabelle zeigt, wann welcher Meldungstyp (einschließlich Format) und welche Aktion erwartet wird.

Ereignis-/Alarmübersicht	Schweregrad der Syslog-Meldungen	Ereignisinformationen
Erfolgreiche Anmeldung von fern oder lokal	WARNUNG	Der Inhalt der Ereignisse für die erfolgreiche Anmeldung hängt davon ab, ob RBAC aktiv ist oder nicht und vom Standort, von dem aus die Anmeldung erfolgt: Von fern (z.B. DIGSI 5) oder lokal (Vor-Ort-Bedienung).
Manuelle Abmeldung	WARNUNG	Die Ereignisse für die manuelle Abmeldung werden im Audit-Trail protokolliert und mit syslog UDP übertragen. Der Inhalt der Meldungen hängt davon ab, ob RBAC aktiv ist oder nicht.
Zeitlich bestimmte Abmeldung	WARNUNG	Der Inhalt der Meldungen hängt davon ab, ob RBAC aktiv ist oder nicht.
Steuerungshandlungen erzwingen	WARNUNG	Ereignisse für lokal oder von fern initiierte Steuerungshandlungen. Zum Beispiel: • Änderung der Position der Pole • Auslöse-/Schließvorgänge im Zusammenhang mit der Primärtechnik • Befehlsvorgänge im Zusammenhang mit der Primärtechnik • Änderungen der Betriebsart im Zusammenhang mit der Primärtechnik • Start/Abbruch der Schaltfolge • Änderung der Spulenposition • Steuerung der sequentiellen Spannungen/Zielspannungen • Steuerung der Schalthoheit • Steuerung der Wicklungsauswahl
Herunterladen der Konfiguration	WARNUNG	Ereignisse im Zusammenhang mit dem Herunterladen der Schutzkonfiguration auf einen PC
Hochladen der Konfiguration	WARNUNG	Ereignisse im Zusammenhang mit dem Hochladen der Schutzkonfiguration von einem PC auf ein Gerät
Konfigurationsänderung	WARNUNG	Ereignisse, die eine Änderung der derzeitigen Konfiguration anzeigen, z.B. durch die Änderung eines Parameters
Firmware-Änderung	WARNUNG	Ereignisse im Zusammenhang mit dem Hochladen der Geräte-Firmware in das Gerät
Zugriff auf Auditprotokoll	WARNUNG	Ereignisse im Zusammenhang mit der Anzeige und dem Herunterladen des Audit-Trails des Gerätes
Änderung von Uhrzeit und Datum	WARNUNG	Ereignisse, die Änderungen der aktuellen Uhrzeit-/Datumseinstellungen anzeigen.
Sicherheitsmanagement	ALARM	Ereignisse, die Änderungen der aktuellen Sicherheitskonfiguration für folgende Elemente anzeigen: • Benutzerverwaltung • Benutzerauthentifizierung • Sichere Kommunikation • Einstellungen für Sicherheitsüberwachung (Protokollierung)

Ereignis-/Alarmübersicht	Schweregrad der Syslog-Meldungen	Ereignisinformationen
Anmeldung fehlgeschlagen	ALARM	Ereignisse für einen fehlgeschlagenen Anmeldeversuch. Wenn RBAC aktiv ist, werden die fehlgeschlagenen Anmeldeversuche nach 3 Versuchen für einen Benutzernamen innerhalb des konfigurierten Zeitfensters protokolliert. Danach wird jeder neue fehlgeschlagene Versuch für denselben Benutzernamen ebenso protokolliert, bis die maximale Anzahl an Anmeldeversuchen erreicht ist. Wenn die Anzahl der Anmeldeversuche ausgeschöpft ist, wird die Anmeldung für diesen Benutzernamen für die eingestellte Zeitspanne gesperrt. Das bedeutet, dass weitere Anmeldeversuche für diesen Benutzernamen abgelehnt und protokolliert werden, unabhängig davon, ob die Kombination von Benutzername und Passwort richtig ist oder nicht. Wenn die Sperrzeit abgelaufen ist, wird der Zähler für den blockierten Benutzernamen zurückgesetzt. Der Zähler für diesen Benutzernamen wird auch dann zurückgesetzt, wenn für diesen Benutzernamen ein erfolgreicher Anmeldeversuch erfolgt ist oder wenn die Zeitspanne ohne Überschreitung der maximalen Anzahl an Anmeldeversuchen erreicht wurde.
Neustart des Produkts	ALARM	Ereignisse beim Neustart des Gerätes. Protokolliert werden Hochfahren und Neustart des Gerätes durch Entfernen der Stromversorgung oder durch Verwendung eines geräteinternen Mechanismus zum Neustart, z.B. durch eine Reset-Taste, Einschaltfolge oder Zugriff auf Software.
Ungültige Konfiguration und Firmware	ALARM	Ereignisse aufgrund der Erkennung einer ungültigen Konfiguration oder Firmware, z.B. eine Signaturprüfung eines SIPROTEC 5-Gerätes



HINWEIS

Die Verwendung eines Bestätigungscodes wird nicht protokolliert. Nur für die Cyber-Security relevante Ereignisse werden protokolliert.

Bereitstellung über Kommunikationsprotokolle

Wenn erforderlich, können Sie für die Cyber-Security kritische Alarme oder Warnmeldungen über folgende Kommunikationsprotokolle an ein Überwachungssystem (z.B. die Leitstelle) senden:

- IEC 60870-5-104
- DNP3
- IEC 61850
- IEC 60870-5-103

Alle Warnmeldungen und Alarme liegen als temporäre Meldungen vor.
Diese Daten werden in den folgenden Betriebsarten des Gerätes übertragen:

- Simulationsmodus
- Prozessmodus
- Inbetriebsetzungsmodus
- Fallback-Modus (Rückfallmodus)

8.4.2 Windows Ereignisprotokoll

Übersicht

Gemäß Cyber-Security-Standard IEEE 1686 muss DIGSI 5 die sicherheitsrelevanten Ereignisse im Windows Ereignisprotokoll dokumentieren. Diese Protokolle können in der **Ereignisanzeige** eingesehen werden. In der **Ereignisanzeige** wird ein Knoten mit dem Namen **DIGSI 5** angezeigt. Unter dem Knoten **Gruppen** > **Lokale Benutzer und Gruppen** im Fenster **Computerverwaltung** Ihres Rechners wird eine Gruppe mit dem Namen **DIGSI 5 SECAUD** angezeigt.

Die Ereignisse für folgende Vorgänge in DIGSI 5 werden protokolliert:

- DIGSI 5 öffnen
- DIGSI 5 beenden
- Konfiguration in das Gerät laden
- Firmware in das Gerät laden
- DAF (Device Attribute File) in Gerät aktualisieren
- Gerätedaten aktualisieren
- Konfigurationen vom Zielgerät aus aktualisieren
- Online-Gerät ins Projekt kopieren

Einträge des Windows Ereignisprotokolls lesen

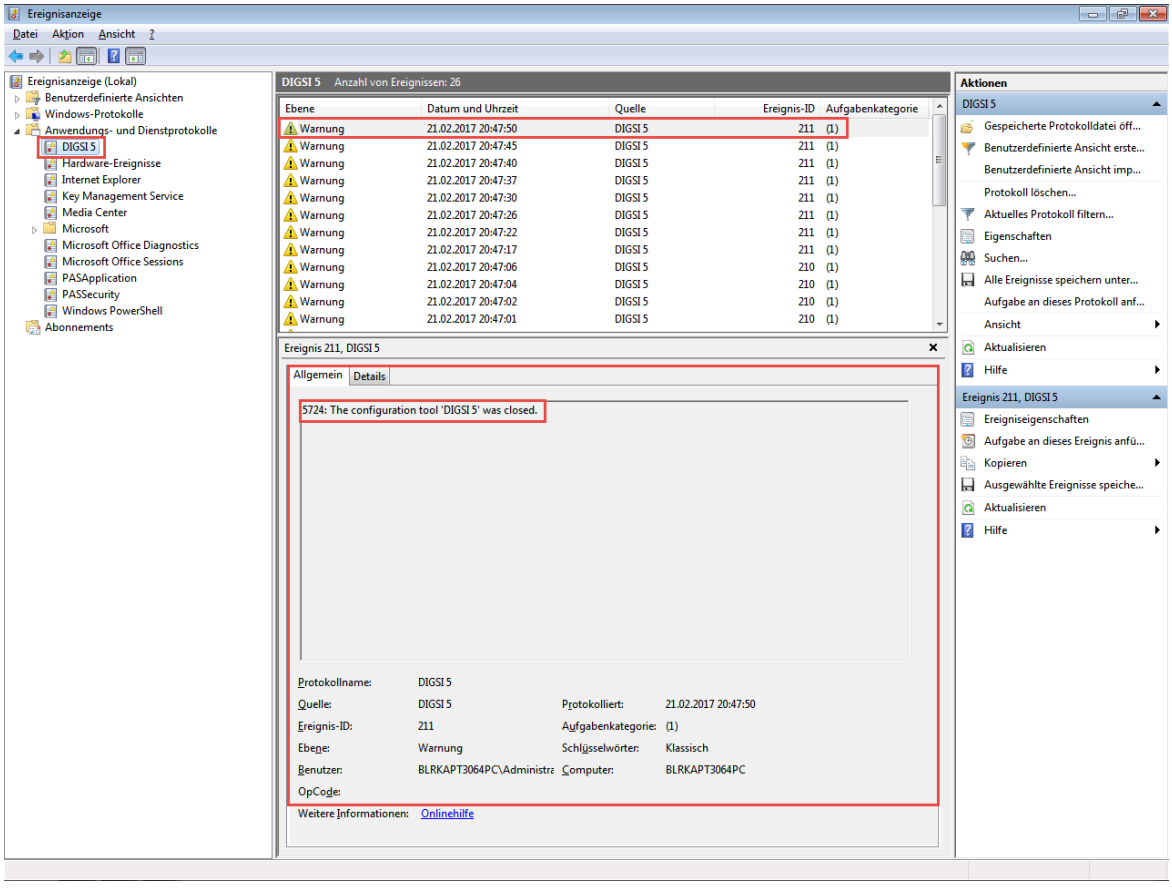
So lesen Sie Einträge des Windows Ereignisprotokolls:

✧ Klicken Sie **Start** -> **Systemsteuerung** -> **Administrative Tools** -> **Ereignisanzeige**.

– oder –

✧ Wählen Sie **Start** > **Ausführen...** und geben Sie **eventvwr** in den Dialog ein.

✧ Klicken Sie **OK**.
Der Dialog **Ereignisanzeige** wird angezeigt.



[sc_EventViewer, 1, de_DE]

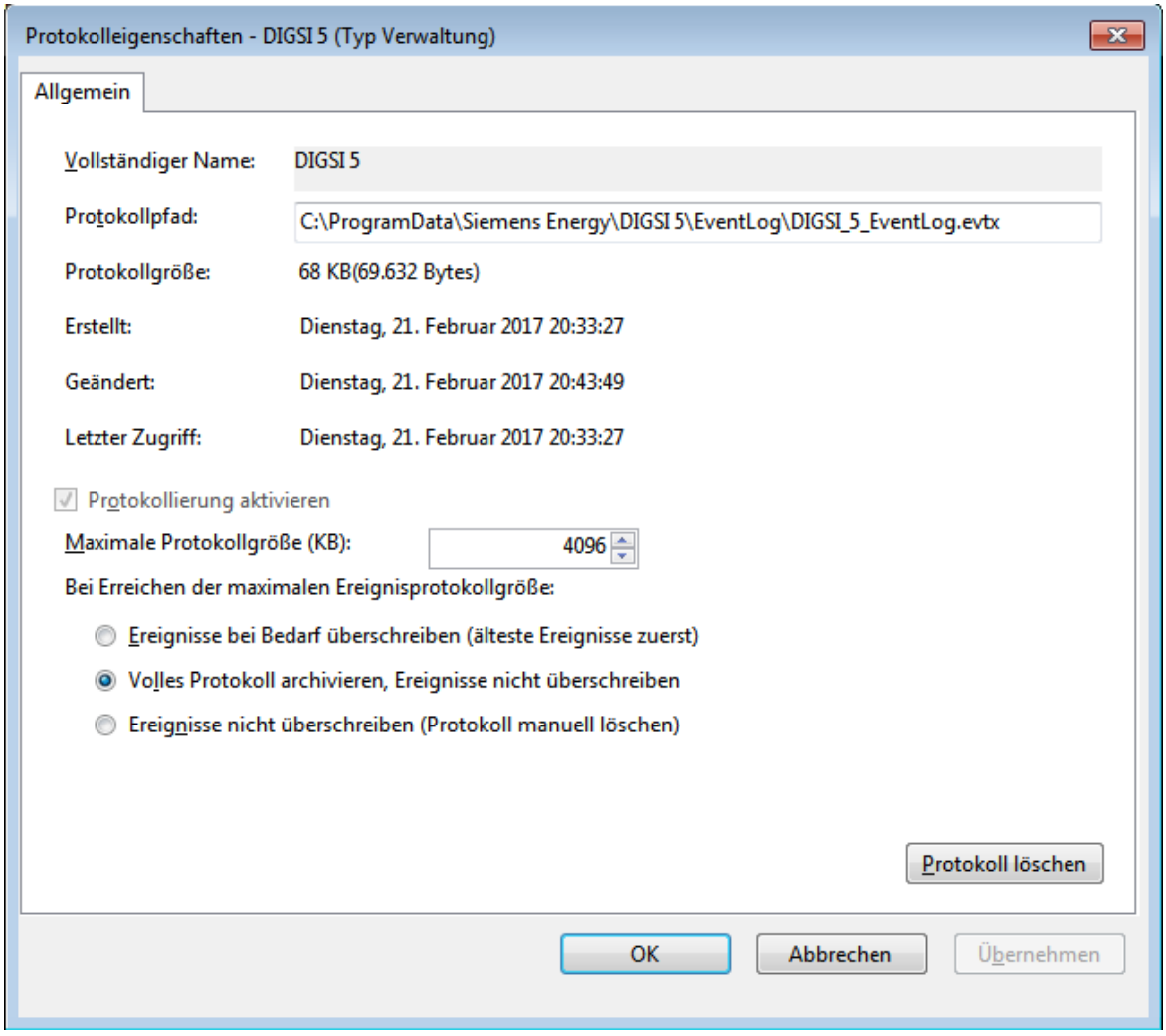
Bild 8-3 Ereignisanzeige

In der Registerkarte **Allgemein** werden die Ereigniseigenschaften mit zusätzlichen Informationen zum protokollierten Ereignis angezeigt. Die im Bild angezeigte Ereignis-ID ist die Prozess-ID der DIGSI-Instanz, für die das Ereignis protokolliert wurde.

Protokolleigenschaften anzeigen – DIGSI 5

✧ Klicken Sie im Fenster **Ereignisanzeige** unter dem Ordner **Anwendungs- und Dienstprotokolle** mit der rechten Maustaste auf den Knoten **DIGSI 5** und wählen Sie im Kontextmenü die Option **Eigenschaften** aus.

Der Dialog **Protokolleigenschaften - DIGSI 5** wird angezeigt.



[sc_EventViewer_Properties, 1, de_DE]

Bild 8-4 Ereignisanzeige – DIGSI 5-Protokolleigenschaften

Standardmäßig werden die Ereignisprotokolle an folgendem Ort gespeichert:
`C:\ProgramData\Siemens Energy\DIGSI 5\EventLog\DIGSI_5_EventLog.evtx`
Die maximale Protokollgröße beträgt 4096 KB.
Wenn die maximale Protokollgröße erreicht wurde, wird die Option **Volles Protokoll archivieren, Ereignisse nicht überschreiben** standardmäßig aktiviert.
Sie können die gewünschte Option gemäß Ihren Anforderungen auswählen.

8.5 Auditberichte anzeigen

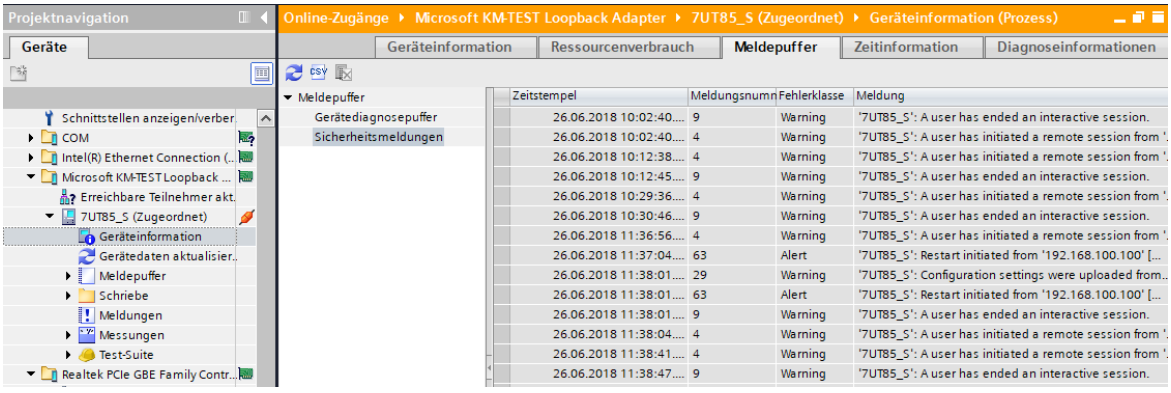
Im Sicherheitsmeldepuffer werden Zugriffe auf Bereiche des Gerätes mit eingeschränktem Zugriffsrecht protokolliert. Erfolglose und unberechtigte Zugriffsversuche werden ebenso aufgezeichnet. Im Sicherheitsmeldepuffer können bis zu 2048 Meldungen gespeichert werden.

Auslesen vom PC mit DIGSI 5

- Um auf den Sicherheitsmeldepuffer Ihres SIPROTEC 5-Gerätes zuzugreifen, benutzen Sie das Fenster der Projektnavigation. Der Online-Zugriff auf das Gerät muss möglich sein.
  Projekt -> **Online-Zugänge** -> **Gerät** -> **Geräteinformation** -> **Meldepuffer** -> **Sicherheitsmeldungen**

Der zuletzt aus dem Gerät geladene Zustand des Sicherheitsmeldepuffers wird angezeigt.

- Aktualisieren Sie vorher die Inhalte durch Anklicken der Aktualisierungspfeile in der Kopfzeile.

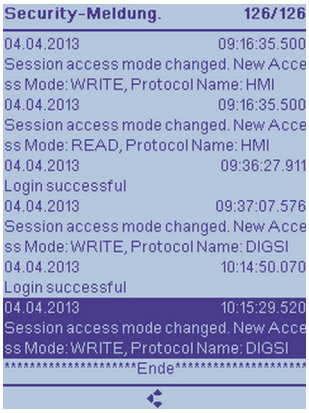


[scsecmld-180816-01, 2, de_DE]

Bild 8-5 Auslesen der Sicherheitsmeldungen mit DIGSI 5

Auslesen am Gerät über die Vor-Ort-Bedieneinheit

- Um vom Hauptmenü auf den Sicherheitsmeldepuffer zuzugreifen, benutzen Sie die Navigationstasten der Vor-Ort-Bedieneinheit.
  Hauptmenü -> **Test & Diagnose** -> **Meldepuffer** -> **Sicherheitsmeldungen**
- An der Vor-Ort-Bedieneinheit können Sie mit den Navigationstasten (oben/unten) innerhalb der angezeigten Meldungsliste navigieren.



[scseclog-090413-01.tif, 1, de_DE]

Bild 8-6 Auslesen des Sicherheitsmeldepuffers an der Vor-Ort-Bedieneinheit des Gerätes



HINWEIS

- Die protokollierten Meldungen sind vorkonfiguriert und können nicht verändert werden!
- Sie können diesen als Ringspeicher organisierten Meldepuffer nicht löschen.
- Wenn Sie sicherheitsrelevante Informationen ohne Informationsverlust aus dem Gerät archivieren wollen, so müssen Sie diesen Meldepuffer regelmäßig auslesen.

9 Securely Resetting the Device Configuration

9.1	Security Credentials and Configuration Reset	102
9.2	Secure Factory Reset	104

9.1 Security Credentials and Configuration Reset

9.1.1 Herunterladen der Datei zum Rücksetzen der Sicherheitsanmeldedaten und Konfiguration (SCRF)

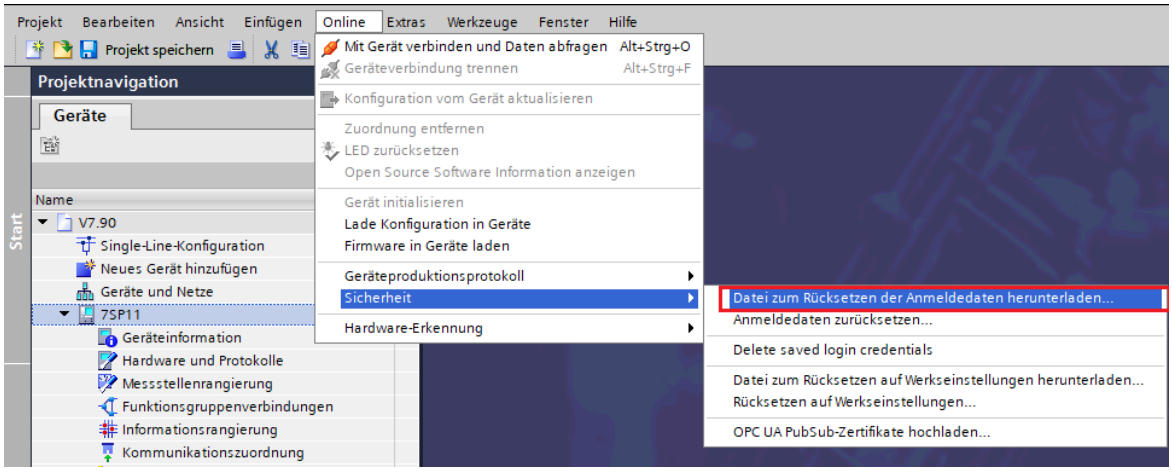
HINWEIS

Sichern und speichern Sie die SCRF-Datei bei der Inbetriebnahme des Gerätes an einem sicheren Ort, da jeder diese Datei verwenden kann.

Nur Benutzerkonten mit der Rolle SECADM oder Administrator sind berechtigt, die SCRF-Datei von einem Gerät herunterzuladen.

Herunterladen der SCRF-Datei

- ✧ Schließen Sie das SIPROTEC 5-Gerät mit einem Netzwerkkabel an einen PC an.
- ✧ Starten Sie DIGSI 5.
- ✧ Wählen Sie das Gerät aus und aktivieren Sie die RBAC-Funktion.
- ✧ Öffnen Sie den Menüeintrag **Online**.
- ✧ Wählen Sie **Sicherheit** -> **Datei zum Zurücksetzen der Anmeldedaten herunterladen...**.



[sc_download_scrf, 2, de_DE]

Bild 9-1 Herunterladen der SCRF-Datei

- ✧ Wählen Sie einen Speicherort auf dem PC, z.B. D:\Siprotec5Sicherheitsdaten.
- ✧ Bestätigen Sie die Aktion mit **OK**.

9.1.2 Sicherheitseinstellungen zurücksetzen

Wenn die Verbindung zum RADIUS-Server unterbrochen oder der Notfallzugang nicht eingerichtet wurde, können Sie die Sicherheitseinstellungen des Gerätes zurücksetzen, um wieder interaktiv auf Geräte zugreifen zu können, bei denen RBAC aktiviert ist.

Vor dem Zurücksetzen der Sicherheitseinstellungen müssen Sie Folgendes beachten:

- Jedes Gerät hat eine eindeutige SCRF-Datei.
  Mit einer SCRF-Datei können nur die Sicherheitseinstellungen des Geräts zurückgesetzt werden, von dem die SCRF heruntergeladen wurde.

- Seien Sie immer äußerst sorgsam beim Umgang mit der SCRF-Datei und verhindern Sie unberechtigten Zugriff auf diese Dateien.
  Denn unabhängig von den zugewiesenen Rollen kann jeder die Sicherheitseinstellungen eines Gerätes durch Hochladen der SCRF-Datei in das Gerät zurücksetzen. Daher muss die SCRF-Datei nach dem Zurücksetzen effektiv vom PC entfernt werden.
- Mit einer SCRF-Datei können die Sicherheitseinstellungen immer zurückgesetzt werden.

Zurücksetzen der Sicherheitseinstellungen

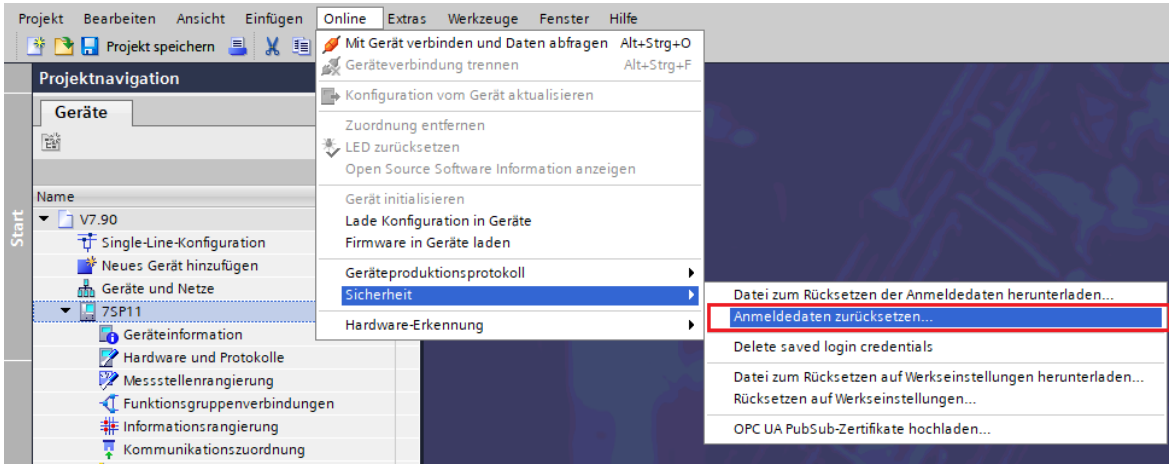
✧ Speichern Sie die SCRF-Datei auf dem PC.

✧ Schließen Sie das SIPROTEC 5-Gerät mit einem Netzwerkkabel an einen PC an.

✧ Starten Sie DIGSI 5.

✧ Wählen Sie das Gerät aus und öffnen Sie den Menüeintrag **Online**.

✧ Wählen Sie **Sicherheit** -> **Anmeldedaten zurücksetzen...**.



[sc_upload_scrf_en, 1, de_DE]

Bild 9-2 Hochladen der SCRF-Datei

✧ Übertragen Sie die SCRF-Datei auf das Gerät.

Bei erfolgreicher Rücksetzung zeigt DIGSI eine Meldung an und alle Sicherheitseinstellungen im SIPROTEC 5-Gerät sind deaktiviert.

HINWEIS

Nach dem Hochladen einer SCRF-Datei werden die Sicherheitseinstellungen auf der Bedieneinheit des Gerätes und auf der browser-basierten Benutzeroberfläche nicht aktualisiert. Zum Aktualisieren ist ein Neustart erforderlich. Um Auswirkungen auf die Schutzfunktionen zu vermeiden, startet das Gerät nicht automatisch neu. Sie können den Neustart des Gerätes entsprechend der aktuellen Situation festlegen.

9.2 Secure Factory Reset

9.2.1 Herunterladen der Datei zum sicheren Zurücksetzen auf Werkseinstellungen (SFRF)

Um ein SIPROTEC 5-Gerät wieder in den Auslieferzustand zu versetzen, müssen Sie zuerst die signierte SFRF-Datei vom Gerät herunterladen.

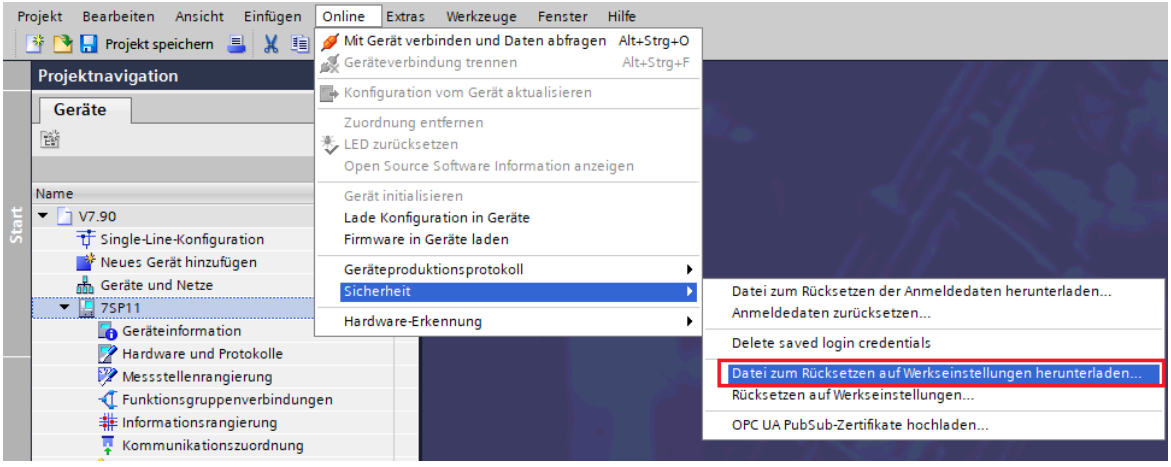
HINWEIS

Sichern und speichern Sie die SFRF-Datei bei der Inbetriebnahme des Gerätes an einem sicheren Ort, da jeder diese Datei verwenden kann.

Zur Konfiguration der Werkseinstellungen ist die Rolle des Sicherheitsadministrators erforderlich.

Herunterladen der SFRF-Datei

- ✧ Schließen Sie das SIPROTEC 5-Gerät mit einem Netzwerkkabel an einen PC an.
- ✧ Starten Sie DIGSI 5.
- ✧ Wählen Sie das Gerät aus und aktivieren Sie die RBAC-Funktion.
- ✧ Wählen Sie das Gerät aus und öffnen Sie den Menüeintrag **Online**.
- ✧ Wählen Sie **Sicherheit** -> **Datei zum Zurücksetzen auf Werkseinstellungen herunterladen...**.



[sc_download_sfrf, 2, de_DE]

Bild 9-3 Herunterladen der SFRF-Datei

- ✧ Wählen Sie einen Speicherort auf dem PC, z.B. D:\Siprotec5Sicherheitsdaten.
- ✧ Bestätigen Sie die Aktion mit **OK**.
- ✧ Sichern und speichern Sie die SFRF-Datei an einem sicheren Ort.

9.2.2 Zurücksetzen auf die Werkseinstellungen

Zur Wiederherstellung der Werkseinstellungen laden Sie die SFRF-Datei in das Gerät.
Vor dem Zurücksetzen der Sicherheitseinstellungen müssen Sie Folgendes beachten:

- Jedes Gerät hat eine eindeutige SFRF-Datei.
  Mit einer SFRF-Datei können nur die Sicherheitseinstellungen des Geräts zurückgesetzt werden, von dem die SFRF heruntergeladen wurde.

- Seien Sie immer äußerst sorgsam beim Umgang mit der SFRF-Datei und verhindern Sie unberechtigten Zugriff auf diese Dateien.
  Denn unabhängig von der/den zugewiesenen Rolle/n kann jeder das Gerät durch Hochladen einer SFRF-Datei in das Gerät auf Werkseinstellungen zurücksetzen. Daher muss die SFRF-Datei nach dem Zurücksetzen effektiv vom PC entfernt werden.
- Mit einer SFRF-Datei kann ein SIPROTEC 5-Gerät immer auf Werkseinstellungen zurückgesetzt werden.

Zurücksetzen auf Werkseinstellungen

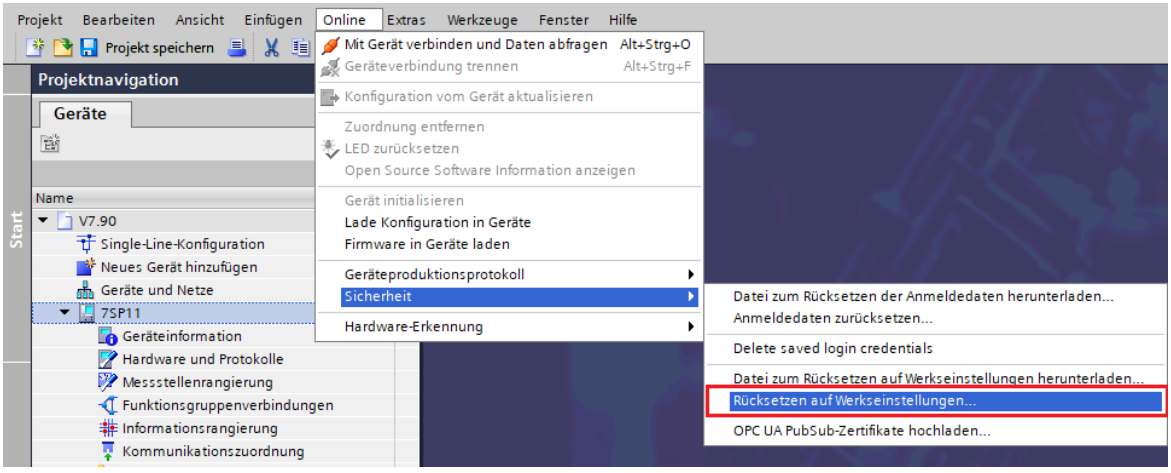
✧ Speichern Sie die SFRF-Datei auf dem PC.

✧ Schließen Sie das SIPROTEC 5-Gerät mit einem Netzwerkkabel an einen PC an.

✧ Starten Sie DIGSI 5.

✧ Wählen Sie das Gerät aus und öffnen Sie den Menüeintrag **Online**.

✧ Wählen Sie **Sicherheit** -> **Zurücksetzen auf Werkseinstellungen...**.



[sc_SFRF, 1, de_DE]

✧ Übertragen Sie die SFRF-Datei auf das Gerät.

Nach dem Neustart des Gerätes sind die Werkseinstellungen wiederhergestellt.

HINWEIS

Alle Daten auf dem Gerät sowie die Sicherheits- und Schutzeinstellungen werden beim Laden der SFRF-Datei gelöscht.

10 Security Patch Management

10.1	Allgemein	108
10.2	SIPROTEC 5 Patch-Management	109
10.3	DIGSI 5 Patch-Management	110

10.1 Allgemein

Der Patch-Management-Prozess erfolgt gemäß Kapitel 2.1.1.3 des BDEW-Whitepaper.

Das Gesamtsystem sollte die Installation von Patches aller Systemkomponenten während des normalen Systembetriebs zulassen. Die Installation eines Patches sollte ohne Unterbrechung des normalen Systembetriebs möglich sein und mit wenig Auswirkungen auf die Verfügbarkeit des Systems. Zum Beispiel sollte es nicht notwendig sein, die Primärsysteme für Erzeugung, Übertragung oder Verteilung herunterzufahren, um Updates auf Sekundärsystemen durchzuführen. Vorzugsweise werden die Patches zuerst auf passiven Redundanzkomponenten installiert. Nach der Umschaltung (Wechsel der aktiven Komponente im redundanten System) und einer nachfolgenden Prüfung wird der Patch auf den restlichen Komponenten installiert.

Ein Patch-Management-Prozess für das gesamte System sollte unterstützt werden. Dieser Prozess sollte Prüfung, Installation und Dokumentation von Sicherheits-Patches und System-Updates verwalten. Generell sollte es möglich sein, dass das Betriebspersonal, das das System verwaltet, auch die Patches und Updates installiert. Installation und Deinstallation von Patches und Updates sollten durch den Systembetreiber autorisiert werden und nicht automatisch durchgeführt werden.

10.2 SIPROTEC 5 Patch-Management

Um sicherzustellen, dass die SIPROTEC 5-Geräte die neueste Firmware verwenden, können Sie alle Firmware-Dateien für diese Geräte einzeln herunterladen und aktualisieren.

Während der Aktualisierung der Firmware ist das betreffende Gerät nicht betriebsbereit. Wenn eine Unterbrechung des Normalbetriebs nicht akzeptabel ist und Sie einen kontinuierlichen Betrieb sicherstellen möchten, setzen Sie redundante Systeme ein.

Für die Produktentwicklung von SIPROTEC 5 hat Siemens einen Patch-Management-Prozess, der alle Firmware-Stände sowie die entsprechenden Verbesserungen zur Nachverfolgung dokumentiert.

10.3 DIGSI 5 Patch-Management

Sie können die DIGSI 5-Installationen mit Wartungsupdates und Hotfixes aktualisieren.

Für die Entwicklung von DIGSI 5 hat Siemens einen Patch-Management-Prozess. Alle enthaltenen Versionen, Verbesserungen und Bereinigungen von Software-Fehlern werden zur Nachverfolgung dokumentiert. Sicherheitsupdates für Komponenten von Fremdherstellern, die von DIGSI 5 verwendet werden (z.B. Windows-Betriebssystem), werden in diesem Rahmen ebenfalls getestet und für DIGSI 5 freigegeben. Siemens bietet die Updates kostenfrei an.

Ab V3.00 kann DIGSI 5 melden, ob ein deaktivierter Gerätetreiber installiert wurde. Normalerweise führt der für die Systempflege verantwortliche Systembediener oder Servicetechniker die entsprechende Installation durch. Weitere Informationen zu Updates von SIPROTEC 5 für Sicherheitslücken finden Sie unter *www.siemens.com/cert/advisories*.

Literaturverzeichnis

/1/ Online-Hilfe DIGSI 5
C53000-D5000-C001

/2/ Systemhärtung für Stationsautomatisierung und Schutz
E50417-H8900-C619

/3/ SIPROTEC 5, Betrieb
C53000-D5000-C003

Glossar

DIGSI

Konfigurationssoftware für SIPROTEC

GOOSE

Generic **O**bject-**O**riented **S**ubstation **E**vent

Schutzgerät

Ein Schutzgerät erkennt fehlerhafte Zustände in Verteilnetzen unter Berücksichtigung von verschiedenen Kriterien, wie Fehlerentfernung, Fehlerrichtung oder Störfalldauer, eine Abschaltung des fehlerhaften Netzabschnittes bewirken.

SIPROTEC

Die eingetragene Marke SIPROTEC bezeichnet die Produktfamilie der Schutzgeräte und Störschreiber.

SIPROTEC 5-Gerät

Dieser Objekttyp repräsentiert ein reales SIPROTEC-Gerät mit allen darin enthaltenen Einstellwerten und Prozessdaten.

Stichwortverzeichnis

A

Access control 23
Anmeldeversuche 30
Authentifizieren 25

B

Benutzerpuffergröße 31

D

Diagnose 21

M

Maßnahmen zur Härtung 22

N

Normen 15
Notfallzugang
    Aktivierung 43

O

Offene Ports 20

P

Patch-Management-Prozess 108

R

RADIUS-Server
    Konfiguration in DIGSI 5 30
RBAC 27
    Aktivierung 28
    Benutzernamen 36
    Einleitung 27
    RADIUS-Server 28
Rollenbasierte Ansichten 39

S

Sicherheit 58
Sicherheitseinstellungen in Gerät laden 31
Sicherheitsmeldepuffer 98
syslog-Server 90
Systemhärtung
    Annahmen und Randbedingungen 19
    Ziele 18

T

Technologien 14

V

Verbindungspasswort 25
    Deaktivieren 25
    Einleitung 24
    Konfiguration 24
    Rücksetzen 25
    Zeichenbeschränkung 24

W

Wichtige Sicherheitsanforderungen 16

Z

Zeitüberschreitung 60
Zertifikatsverwaltung

CSR exportieren 66
Signierte Zertifikate 64
Vorbedingungen 62
Zuweisung von Rechten und unterstützten Rollen 33