



REX640 Cyber Security Deployment Guideline

RELION[®] PROTECTION AND CONTROL





Document ID: 1MRS759122 Issued: 2023-01-09 Revision: D

 $^{\odot}$ Copyright 2023 ABB. All rights reserved

Copyright

This document and parts thereof must not be reproduced or copied without written permission from ABB, and the contents thereof must not be imparted to a third party, nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license.

Trademarks

ABB and Relion are registered trademarks of the ABB Group. All other brand or product names mentioned in this document may be trademarks or registered trademarks of their respective holders.

Open Source Software

This product contains open source software. For license information refer to product documentation at *#http://www.abb.com/EN-*.

Warranty

Please inquire about the terms of warranty from your nearest ABB representative.

#http://www.abb.com/mediumvoltage/EN-

Disclaimer

The data, examples and diagrams in this manual are included solely for the concept or product description and are not to be deemed as a statement of guaranteed properties. All persons responsible for applying the equipment addressed in this manual must satisfy themselves that each intended application is suitable and acceptable, including that any applicable safety or other operational requirements are complied with. In particular, any risks in applications where a system failure and/or product failure would create a risk for harm to property or persons (including but not limited to personal injuries or death) shall be the sole responsibility of the person or entity applying the equipment, and those so responsible are hereby requested to ensure that all measures are taken to exclude or mitigate such risks.

This product has been designed to be connected and communicate data and information via a network interface which should be connected to a secure network. It is the sole responsibility of the person or entity responsible for network administration to ensure a secure connection to the network and to take the necessary measures (such as, but not limited to, installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, etc.) to protect the product and the network, its system and interface included, against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB is not liable for any such damages and/or losses.

This document has been carefully checked by ABB but deviations cannot be completely ruled out. In case any errors are detected, the reader is kindly requested to notify the manufacturer. Other than under explicit contractual commitments, in no event shall ABB be responsible or liable for any loss or damage resulting from the use of this manual or the application of the equipment.

In case of discrepancies between the English and any other language version, the wording of the English version shall prevail.

Conformity

This product complies with the directive of the Council of the European Communities on the approximation of the laws of the Member States relating to electromagnetic compatibility (EMC Directive 2014/30/EU) and concerning electrical equipment for use within specified voltage limits (Low-voltage directive 2014/35/EU). This conformity is the result of tests conducted by the third party testing laboratory Intertek in accordance with the product standard EN 60255-26 for the EMC directive, and with the product standards EN 60255-1 and EN 60255-27 for the low voltage directive. The product is designed in accordance with the international standards of the IEC 60255 series.

Contents

1	Inti	Introduction9				
	1.1	This m	anual			
	1.2	Intended audience				
	1.3	Produc	ct documentation			
		1.3.1	Product documentation set			
		1.3.2	Document revision history			
		1.3.3	Related documentation	10		
	1.4	Symbo	ols and conventions	11		
		1.4.1	Symbols	11		
		1.4.2	Document conventions	11		
2	Sec	curity i	in distribution automation	12		
	2.1	Genera	al security in distribution automation	12		
3	Sec	ure sv	/stem setup	13		
	3.1	Basics	system hardening rules			
	3.2	Relay c	communication interfaces			
	3.3	TCP/IP	P-based protocols and used IP ports.			
	0.0	3.3.1	Ethernet ports			
		3.3.2	Protocol control			
		3.3.3	Protocol write access rights			
		3.3.4	Ethernet filter and rate limiter			
	3.4	Secure	e communication	25		
		3.4.1	Certificate handling			
	3.5	Time s	synchronization			
	3.6	Encryp	otion algorithms	33		
4	Use	er mar	nagement			
	4.1	Local u	user account management			
		4.1.1	Password policies	36		
	4.2	Centra	al account management			
		4.2.1	Central account management server			
		4.2.2	CAM client – protection relay			
		4.2.3	Authentication in central account management mode			
		4.2.4	User account creation and authentication	40		
		4.2.5	Central account management and certificates	41		
	4.3	Local user account management and central account management				
	4.4	Login banner4				

	4.5	Systen	n use notification	
5	Sec	urity	logging	43
5	5 1	Socuri	tylog	د ر در
	5.1	Contra	L Activity Logging	
	5.2	Securi	tv log events.	
	0.0	beeuri		
6	Usi	ng the	e HMI	49
	6.1	Using	local HMI	
		6.1.1	Connecting local HMI	
		6.1.2	Logging in	51
		6.1.3	Logging out	53
		6.1.4	Pairing HMI with protection relay	54
	6.2	Using	Web HMI	57
		6.2.1	Connecting to Web HMI	57
		6.2.2	Logging in	58
		6.2.3	Logging out	61
7	Pro	tectic	on of relay and system configuration	62
			fi of feldy and system configuration	
	7.1	Backu	o files	
	7.1	Backuj 7.1.1	o files Creating a backup from the relay configuration	
	7.1	Backu 7.1.1 7.1.2	o files Creating a backup from the relay configuration Creating a backup from the PCM600 project	
	7.1 7.2	Backuj 7.1.1 7.1.2 Restor	p files Creating a backup from the relay configuration Creating a backup from the PCM600 project ing factory settings	
	7.1 7.2 7.3	Backuj 7.1.1 7.1.2 Restor Restor	o files Creating a backup from the relay configuration Creating a backup from the PCM600 project ing factory settings ing relay backup from local HMI	
	7.1 7.2 7.3 7.4	Backu 7.1.1 7.1.2 Restor Restor Restor	p files Creating a backup from the relay configuration Creating a backup from the PCM600 project ing factory settings ing relay backup from local HMI ing relay backup from switchgear HMI	
	7.1 7.2 7.3 7.4 7.5	Backu 7.1.1 7.1.2 Restor Restor Restor Restor	p files Creating a backup from the relay configuration Creating a backup from the PCM600 project ing factory settings ing relay backup from local HMI ing relay backup from switchgear HMI ing the administrator password	62
	7.1 7.2 7.3 7.4 7.5 7.6	Backuj 7.1.1 7.1.2 Restor Restor Restor Restor Decom	p files Creating a backup from the relay configuration Creating a backup from the PCM600 project ing factory settings ing relay backup from local HMI ing relay backup from switchgear HMI ing the administrator password	
	7.1 7.2 7.3 7.4 7.5 7.6	Backu 7.1.1 7.1.2 Restor Restor Restor Decom 7.6.1	o files Creating a backup from the relay configuration Creating a backup from the PCM600 project ing factory settings ing relay backup from local HMI ing relay backup from switchgear HMI ing the administrator password missioning Deleting sensitive information from the protection relay	62
8	7.1 7.2 7.3 7.4 7.5 7.6 Sta	Backuj 7.1.1 7.1.2 Restor Restor Restor Decom 7.6.1	creating a backup from the relay configuration Creating a backup from the PCM600 project ing factory settings ing relay backup from local HMI ing relay backup from switchgear HMI ing the administrator password missioning Deleting sensitive information from the protection relay	
8	7.1 7.2 7.3 7.4 7.5 7.6 Sta 8.1	Backup 7.1.1 7.1.2 Restor Restor Restor Decom 7.6.1	o files Creating a backup from the relay configuration Creating a backup from the PCM600 project ing factory settings ing relay backup from local HMI ing relay backup from switchgear HMI ing the administrator password missioning Deleting sensitive information from the protection relay I compliance statement	
8	7.1 7.2 7.3 7.4 7.5 7.6 Sta 8.1	Backup 7.1.1 7.1.2 Restor Restor Restor Decom 7.6.1	o files Creating a backup from the relay configuration Creating a backup from the PCM600 project ing factory settings ing relay backup from local HMI ing relay backup from switchgear HMI ing the administrator password missioning Deleting sensitive information from the protection relay I compliance statement	

1 Introduction

1.1 This manual

The cyber security deployment guideline describes the process for handling cyber security when communicating with the protection relay. The cyber security deployment guideline provides information on how to secure the system on which the protection relay is installed. The guideline can be used as a technical reference during the engineering phase, installation and commissioning phase, and during normal service.

1.2 Intended audience

This guideline is intended for the system engineering, commissioning, operation and maintenance personnel handling cybersecurity during the product lifecycle.

The personnel is expected to have general knowledge about topics related to cybersecurity.

- Protection and control devices, gateways and workstations
- Networking, including Ethernet and TCP/IP with its concept of ports and services
- Security policies
- Firewalls
- Antivirus protection
- Application whitelisting
- Secure remote communication
- Public key infrastructure (PKI)

1.3 Product documentation

1.3.1 Product documentation set



Figure 1: The intended use of documents during the product life cycle

1.3.2 Document revision history

Document revision/ date	Product connectivity level	History
A/2018-12-14	PCL1	First release
B/2020-02-13	PCL2	Content updated to correspond to the prod- uct connectivity level
C/2020-12-09	PCL3	Content updated to correspond to the prod- uct connectivity level
D/2023-01-09	PCL4	Content updated to correspond to the prod- uct connectivity level

1.3.3 Related documentation



Download the latest documents from the ABB Web site *www.abb.com/ mediumvoltage*.

1.4 Symbols and conventions

1.4.1 Symbols



The caution icon indicates important information or warning related to the concept discussed in the text. It might indicate the presence of a hazard which could result in corruption of software or damage to equipment or property.



The information icon alerts the reader of important facts and conditions.



The tip icon indicates advice on, for example, how to design your project or how to use a certain function.

Although warning hazards are related to personal injury, it is necessary to understand that under certain operational conditions, operation of damaged equipment may result in degraded process performance leading to personal injury or death. Therefore, comply fully with all warning and caution notices.

1.4.2 Document conventions

A particular convention may not be used in this manual.

- Abbreviations and acronyms are spelled out in the glossary. The glossary also contains definitions of important terms.
- Menu paths are presented in bold.

Select Main menu > Settings.

Parameter names are shown in italics.

The function can be enabled and disabled with the Operation setting

Parameter values are indicated with quotation marks.

The corresponding parameter values are "On" and "Off".

• Input/output messages and monitored data names are shown in Courier font.

When the function starts, the START output is set to TRUE.

- Values of quantities are expressed with a number and an SI unit. The corresponding imperial units may be given in parentheses.
- This document assumes that the parameter setting visibility is "Advanced".

2

Security in distribution automation

2.1 General security in distribution automation

Technological advancements and breakthroughs have caused a significant evolution in the electric power grid. As a result, the emerging "smart grid" and "Internet of Things" are quickly becoming a reality. At the heart of these intelligent advancements are specialized IT systems – various control and automation solutions such as distribution automation systems. To provide end users with comprehensive real-time information, enabling higher reliability and greater control, automation systems have become ever more interconnected. To combat the increased risks associated with these interconnections, ABB offers a wide range of cyber security products and solutions for automation systems and critical infrastructure.

The new generation of automation systems uses open standards such as DNP3 and IEC 61850 and commercial technologies, in particular Ethernet and TCP/IP based communication protocols. They also enable connectivity to external networks, such as office intranet systems and the Internet. These changes in technology, including the adoption of open IT standards, have brought huge benefits from an operational perspective, but they have also introduced cyber security concerns previously known only to office or enterprise IT systems.

To counter cyber security risks, open IT standards are equipped with cyber security mechanisms. These mechanisms, developed in a large number of enterprise environments, are proven technologies. They enable the design, development and continuous improvement of cyber security solutions for control systems, including distribution automation applications.

ABB understands the importance of cyber security and its role in advancing the security of distribution networks. A customer investing in new ABB technologies can rely on system solutions where reliability and security have the highest priority.

At ABB, we are addressing cyber security requirements on a system level as well as on a product level to support cyber security standards or recommendations from organizations such as NERC CIP, IEC 62351, IEC 62443, IEEE 1686, ENISA and BDEW Whitepaper.

Reporting of vulnerability or cyber security issues related to any ABB product can be done via cybersecurity@ch.abb.com.

3 Secure system setup

3.1 Basic system hardening rules

Today's distribution automation systems are basically specialized IT systems. Therefore, several rules of hardening an automation system apply to these systems, too. Protection and control relays are from the automation system perspective on the lowest level and closest to the actual primary process. It is important to apply defense-in-depth information assurance concept where each layer in the system is capable of protecting the automation system and therefore protection and control relays are also part of this concept. The following should be taken into consideration when planning the system protection.

- Recognizing and familiarizing all parts of the system and the system's communication links
- Removing all unnecessary communication links in the system
- Rating the security level of remaining connections and improving with applicable methods
- Hardening the system by removing or deactivating all unused processes, communication ports and services
- Checking that the whole system has backups available from all applicable parts
- Collecting and storing backups of the system components and keeping those up-to-date
- Removing all unnecessary user accounts
- Defining password policies
- Changing default passwords and using strong passwords
- Checking that the link from substation to upper level system uses strong encryption and authentication
- Segregating public network (untrusted) from automation networks (trusted)
- Segmenting traffic and networks
- Using firewalls and demilitarized zones
- Assessing the system periodically
- Using malware protection in workstations and keeping those up-to-date

It is important to utilize the defence-in-depth concept when designing automation system security. It is not recommended to connect a device directly to the Internet without adequate additional security components. The different layers and interfaces in the system should use security controls. Robust security means, besides product features, enabling and using the available features and also enforcing their use by company policies. Adequate training is also needed for the personnel accessing and using the system.



Figure 2: Distribution substation example

3.2 Relay communication interfaces

All ports dedicated to station bus communication can be opened and closed when configuring the relay. The HMI port must not be connected to any Ethernet network.

Table 1: Physical ports on the relay's communication cards

Port	Туре	Description
XO	RJ-45	НМІ
X1	RJ-45 or LC	Ethernet (LAN A)
X2	RJ-45 or LC	Ethernet (LAN B)
Х3	RJ-45 or LC	Ethernet (Interlink)
X6	SFP – LC	Protection communication

Table continues on the next page

Port	Туре	Description
X7	FO – ST	Serial communication
X8	TP ¹	Serial communication/IRIG-B

All protocol services, except for IEC 61850, FTP/FTPS and HTTPS, are by default off and do not respond to any protocol requests in the serial or Ethernet ports. IEC 61850, the FTP/FTPS protocol and the rear Ethernet ports are by default activated as those are used for engineering of the protection relay. The HMI port is segregated from the station bus communication.

3.3 TCP/IP-based protocols and used IP ports

The IP port security depends on the specific installation, requirements and existing infrastructure. The required external equipment can be separate devices or devices that combine firewall, router and secure VPN functionality. When the network is divided into security zones, it is done with substation devices having firewall functionality or with dedicated firewall products. Security zone boundaries are inside the substation or between the substation and the outside world.

The relay supports an option with multiple station communication Ethernet ports. The relay responds to the ICMP Echo request (ping).

To set up an IP firewall, the following table summarizes the IP ports used by the device. All closed ports can be opened in the configuration. The ports which are by default open are used for configuring the protection relay.

Port number	Туре	Default state	Description
21	ТСР	Open	Explicit FTP over TLS
22	ТСР	Closed	SSH (HMI only, normally closed)
102	ТСР	Open	IEC 61850
386	LDAP	Open	САМ
443	ТСР	Open	Web server HTTPS
123	UDP	Client service not active by default in relay	SNTP
502	ТСР	Closed	Modbus TCP
514	UDP	Closed	CAL
636	LDAPS	Open	CAM over TLS
2404	ТСР	Closed	IEC 60870-5-104 TCP
20000	ТСР	Closed	DNP3 TCP
20000	UDP	Closed	DNP3 UDP
1468	ТСР	Closed	CAL
4922049235	ТСР	Closed	Ports open on demand for da- ta transfer when FTP PASV com- mand is given

Table 2: IP ports used by the relay

¹ 2- or 4-wire twisted pair

FTP and IEC 61850 are primary services needed for the relay configuration. Additionally, the protection relay uses layer 2 communications in GOOSE, SMV, IEEE 1588 (PTP) and HSR/PRP supervision services, which needs to be taken into account when designing the network.

In addition to the HTTPS and FTPS protocols, the relay supports four Ethernetbased substation automation communication protocols: IEC 61850, Modbus, DNP3 and IEC 60870-5-104.

IEC 61850 is always supported, and the relay can be ordered with one additional station bus protocol. Additional protocols must be enabled in the configuration, otherwise the port used by the communication protocols TCP and UDP is closed and unavailable. If the protocol service is configured, the corresponding port is open all the time. In Modbus, DNP3 and IEC 60870-5-104 it is possible to assign the TCP or UDP port number if required and allow connection requests only from a configured client IP address.

See the technical manual and the corresponding protocol documentation to configure a certain communication protocol.

3.3.1 Ethernet ports

The protection relay supports up to three Ethernet ports at station level depending on the capability of the protection relay and the COM modules in use. These ports provide access to the Ethernet-based protocols supported by the relay such as FTP, FTPS, HTTPS, MMS, Modbus, DNP3 and IEC 60870-5-104.

- Port mode X1: On/Off (On by default)
- Port mode X2: On/Off (On by default redundant)
- Port mode X3: On/Off/Dedicated channel (On by default also known as interlink port)

Dedicated channel mode is used for Dual channel binary signal transfer (BST) operation.

These appear as parameters under **Configuration** > **Communication** > **Ethernet**. In addition, there is an HMI port which has its own IP address and subnet.

The protection relay allows the use of a secondary IP address for the station ports on the communication modules COM1001...COM1003. This secondary IP network is assigned to a single Ethernet port and can be used to make separate networks for different communication protocols or, for example, a separate service network for configuration purposes. Multicast station/bus communication, such as IEC 61850-9-2 LE sampled values and GOOSE, is only supported on the Network 1 interface. The parameters for setting the secondary IP network are located under **Configuration > Communication > Ethernet > Network 2 address**.

Table 3: Secondary IP address parameters

Parameter	Options	Description
Configuration/Communica-	ion/Communica- False (default)	Network 2 disabled
dress/Enable	TRUE	Network 2 enabled
Configuration/Communica- tion/ Ethernet/Network 2 ad- dress/IP address	0.0.0.0	IP address for Network 2

Table continues on the next page

Parameter	Options	Description
Configuration/Communica- tion/ Ethernet/Network 2 ad- dress/IP address	0.0.0.0	Subnet address for Network 2
Configuration/Communica- tion/ Ethernet/Network 2 ad- dress/MAC address	xx-xx-xx-xx-xx	MAC address for Network 2

The IP address for Network 2 is disabled by default settings, and all Ethernet ports are assigned to the same IP address used in the Network 1 address menu **Configuration > Communication > Ethernet > Network 1**. If Network 2 is taken into use by the setting Enable="True" (requires reboot), the interlink port X3 of the COM module is assigned to this second network, using the IP address and subnet parameters in the Network 2 address menu **Configuration > Communication > Ethernet > Network 2 address**.



If the Network 2 interface is enabled, PTP time synchronization and SMV/GOOSE multicast are disabled for that port.



Figure 3: Ethernet modes with Network 1 and Network 2

3.3.2 Protocol control

It is possible to allow or block different protocols for different network interfaces in the protection relay using the parameters in **Configuration > Communication > Protocols > Network1, Configuration > Communication > Protocols > Network2** and **Configuration > Communication > Protocols > HMI Port**.

All protocols are allowed for each network by default, and can be separately disabled.

Parameter	Options	Description
Configuration/Commu-	Off	Denies FTP and FTPS
nication/Protocols/Net- work1/FTP	On	Allows FTP and FTPS
	Secure (Default)	Allows FTPS only
Configuration/Commu-	Off	Denies FTP and FTPS
nication/Protocols/Net- work2/FTP	On	Allows FTP and FTPS
···, · ··-	Secure (Default)	Allows FTPS only
Configuration/Communica-	Off	Denies FTP and FTPS
tion/Protocols/HMI Port/FTP	On	Allows FTP and FTPS
	Secure (Default)	Allows FTPS only
Configuration/Communica-	Off	Denies HTTPS
tion/Protocols/Network1/ HTTPS	On (Default)	Allows HTTPS
Configuration/Communica-	Off	Denies HTTPS
tion/Protocols/Network2/ HTTPS	On (Default)	Allows HTTPS
Configuration/Commu-	Off	Denies IEC 61850 MMS
nication/Protocols/Net- work1/MMS	On (Default)	Allows IEC 61850 MMS
Configuration/Commu-	Off	Denies IEC 61850 MMS
nication/Protocols/Net- work2/MMS	On (Default)	Allows IEC 61850 MMS
Configuration/Communica-	Off	Denies IEC 61850 MMS
tion/Protocols/HMI Port/MMS	On (Default)	Allows IEC 61850 MMS
Configuration/Commu-	Off	Denies DNP3
work1/DNP	On (Default)	Allows DNP3
Configuration/Commu-	Off	Denies DNP3
nication/Protocols/Net- work2/DNP	On (Default)	Allows DNP3
Configuration/Commu-	Off	Denies Modbus
nication/Protocols/Net- work1/Modbus	On (Default)	Allows Modbus
Configuration/Commu-	Off	Denies Modbus
nication/Protocols/Net- work2/Modbus	On (Default)	Allows Modbus
Configuration/Communica-	Off	Denies IEC 60870-5-104
tion/Protocols/Network1/ IEC-60870-5-104	On (Default)	Allows IEC 60870-5-104
Configuration/Communica-	Off	Denies IEC 60870-5-104
tion/Protocols/Network2/ IEC-60870-5-104	On (Default)	Allows IEC 60870-5-104

Table 4: Protocol control in the protection relay

3.3.3 Protocol write access rights

Write access rights are configurable for FTP, MMS, and HTTPS protocols in **Configuration > Authorization**. The write access parameters are used to narrow down services that allow setting changes on different network interfaces. Disabling

the FTP and IEC 61850 MMS write access on Network 1 and 2 prevents the user from updating the configuration to the protection relay from PCM600. Disabling the HTTPS write access prevents the user from writing setting changes from WHMI.

Parameter	Options	Description
Configuration/Authoriza- tion/Network1/FTP write ac-	Off	FTP write access denied for Network 1
cess	On (Default)	FTP write access allowed for Network 1
Configuration/Authoriza- tion/Network1/MMS write	Off	IEC 61850 MMS write access denied for Network 1
access	On (Default)	IEC 61850 MMS write access allowed for Network 1
Configuration/Authoriza- tion/Network1/HTTPS write	Off	HTTPS write access denied for Network 1
access	On (Default)	HTTPS write access allowed for Network 1
Configuration/Authoriza- tion/Network2/FTP write ac-	Off	FTP write access denied for Network 2
cess	On (Default)	FTP write access allowed for Network 2
Configuration/Authoriza- tion/Network2/MMS write	Off	IEC 61850 MMS write access denied for Network 2
access	On (Default)	IEC 61850 MMS write access allowed for Network 2
Configuration/Authoriza- tion/Network2/HTTPS write	Off	HTTPS write access denied for Network 2
access	On (Default)	HTTPS write access allowed for Network 2
Configuration/Authoriza- tion/HMI/FTP write access	Off	FTP write access denied for the HMI port
	On (Default)	FTP write access allowed for the HMI port
Configuration/Authoriza- tion/HMI/MMS write access	Off	IEC 61850 MMS write access denied for the HMI port
	On (Default)	IEC 61850 MMS write access allowed for the HMI port

3.3.4 Ethernet filter and rate limiter

The protection relay offers a bandwidth rate limiting functionality to limit the Ethernet/TCP network traffic. The main purpose for these features is the possibility to divide network segments for different multicast frame types and also limit network congestion and traffic towards the protection relay processing during network attacks (such as a Denial of Service attack) or network configuration issues.

3.3.4.1 Ethernet filter functionality

As a basic rule for network security configuration, the protection relay offers a port Enabled/Disabled parameter for each Ethernet port. Unused Ethernet ports should be set to the "Disabled" mode. For the active ports, the protection relay has a filtering functionality that can be used to select the traffic forwarded trough different ports. These filters are settable per Ethernet port and they offer the possibility to filter out GOOSE and IEC 61850-9-2 sampled values multicast traffic. An exception to this is the Network2 interface. If enabled, the Network2 interface filters out GOOSE and IEC 61850-9-2 sampled values automatically. The filtering parameter is defined in Ethernet ports menu. For example, for port X1 the filter mode is set via **Configuration > Communication > Ethernet > Filter > Filter mode X1**.

Table 6: Filter mode parameter for port X1

Parameter	Values (Range)	Unit	Step	Default	Description
Filter mode	0=OFF	enum		0=OFF	Filter out se-
X1	(1 1=SMV				lected mes-
	2=GOOSE				sage types
	3=GOOSE				
	and SMV				

The default setting "OFF" means that all network traffic passes through the port. Values "1"..."3" specify the type of traffic filtered out for the port in both incoming and outgoing directions. For example, the setting "1" means that no IEC 61850-9-2 sampled values multicast is sent out to the port nor is incoming SV traffic allowed in.

In normal switch mode, the port filtering mode is defined by the port *Filter* parameter. If the protection relay is in the redundancy HSR or PRP mode, the filtering setting is common for both redundant (LAN A and LAN B) ports, and thus the common value comes from the *Redundancy* parameter via **Configuration** > **Communication** > **Ethernet** > **Filter** > **Filter mode A_B**.

Table 7: Filter mode A_B parameter

Parameter	Value (Range)	Unit	Step	Default	Description
Filter mode	0=OFF	enum		0=OFF	Filter out se-
A_B	1=SMV				lected mes-
	2=GOOSE				sage types
	3=GOOSE				
	and SMV				

The port filtering can be used, for example, in the following cases.

- If a dedicated interlink is needed, for example, for RIO600 and the IEC 61850-9-2 sampled values are not required to flow into the RIO600 device. This can be achieved by setting the filter mode of the port facing towards RIO600 to "1" so that the link between the protection relay and RIO600 forwards GOOSE multicast only. The same principle can be applied to other network links also when IEC 61850-9-2 sampled values are not required.
- If a dedicated process bus is needed for the system, the Ethernet ports reserved for other TCP traffic can use filtering mode "1" to filter out the IEC 61850-9-2

sampled values for rest of the network. This requires a dedicated and physically separated process bus LAN.

3.3.4.2 Ethernet rate limiter

Ethernet traffic bandwidth rates can be limited according to the port by utilizing the Ethernet rate limiter feature. This feature can be used to limit specific types of traffic reaching relay main processor and other parts of the network during abnormal network conditions. The rate limiter parameters are found in the Communications menu and set as Megabits per second. For example, for port X1 the rate limiter parameter is set via **Configuration > Communication > Ethernet > Rate Limiter**.

Table 8: Ethernet rate limiter parameters

Parameter	Values (Range)	Unit	Step	Default	Description
Goose rate Limit X1	0.512 90.000	Mbps	0.016	10	GOOSE rate limit (Mbps) for port X1
SMV rate Lim- it X1	0.512 90.000	Mbps	0.016	70	Multicast sampled value rate limit (Mbps) for port X1
Def. rate Limit X1	0.512 90.000	Mbps	0.016	8	Default rate limit (Mbps) for port X1

The rate limiter functionality for external ports is set off by default. Functionality can be enabled via **Configuration > Communication > Ethernet > Rate limiter > Rate Limit ctrl**.

Table 9: Rate limit control for the external port

Parameter	Values (Range)	Unit	Step	Default	Description
Rate limit ctrl	FALSE=OFF			FALSE=OFF	Rate limit
	TRUE=ON				control

The rate limiter controls the inbound network traffic by internal traffic policers that are settable as maximum bandwidth per frame type. The most common multicast frame types have limits that can be set according to the system bandwidth requirements. The GOOSE rate limit polices all incoming frames with GOOSE destination MAC addresses and drops out the frames exceeding the set bandwidth. The SMV rate limit does the same for all the incoming IEC 61850-9-2 sampled values multicast frames. The default rate limit can be used to control the rest of the unclassified traffic such as network broadcast messages.

In addition to the settable limits, the protection relay has internal non-configurable limits set for Unicast (1 Mbps) and 1588 (1 Mbps) time synchronization frames. These limits are pre-set rational limits based on the estimated maximum requirements for the message type.

Rate limiter diagnostics show the amount of policer activation detections for each Ethernet port. Instead of showing the amount of frames, the number indicates how many times the protection relay has detected policer activation over periodical polling. There is also an alarm signal available for each frame type. The alarm is set TRUE for several seconds if a specific frame type exceeds the set limit Mbps value. For example, for port X1 the rate limiter diagnostics are available via **Monitoring** > **Communication** > **Ethernet** > **Diagnostics** > **X1**.

Parameter	Value (Range)	Unit	Step	Default	Description
Reset coun- ters	FALSE	Boolean		FALSE	Resets coun- ters
	TRUE (=RE- SET)				
GOOSE limit count	01000000		1	0	GOOSE rate limit exceed count
SMV limit count	01000000		1	0	Multicast sampled value rate limit ex- ceed count
Ucast limit count	01000000		1	0	Unicast rate limit exceed count
Def. limit count	01000000		1	0	Default rate limit exceed count
GOOSE limit alarm	FALSE TRUE (=ALARM)	Boolean		FALSE	GOOSE rate limit exceed alarm
SMV limit alarm	FALSE TRUE (=ALARM)	Boolean		FALSE	Multicast sampled val- ues rate limit alarm
Ucast limit alarm	FALSE TRUE (=ALARM)	Boolean		FALSE	Unicast rate limit exceed alarm
Def. limit alarm	FALSE TRUE (=ALARM)	Boolean		FALSE	Default rate limit exceed alarm

Table 10: Rate limiter diagnostics

In addition to the external rate limits, there are also several default internal limits within the protection relay to reduce any unwanted traffic towards the processor. These limits are also controlled via *Rate Limiter general enable* parameter.



Set the bandwidth limit settings to provide some limits for the system needs. It is advisable to leave some gap between the set limit and the actual network utilization to allow any small temporary peaks in traffic. For example, the limit could be set to 5 times the "base network load bandwidth" per frame type.

The Ethernet rate limiter can be used, for example, in the following cases.

- Blocking and mitigating any kind of network cyber attack directed towards the protection relays such as flooding of network with different types of broadcast and multicast frames.
- Blocking and mitigating any kind of network abnormalities such as flooding of multicast or broadcast frames during network configuration errors or topology reconfiguration.

Denial of Service detection

Abnormal network conditions in form of exceeded rate limiter conditions are monitored internally by the DoS detection functionality. The protection relay has two signals to detect these conditions.

- Dos_WARNING
- Dos_Alarm

The signals are also available in Application Configuration as the GSAL function block.

GSAL	9
DO	S_ALARM
DOS_1	WARNING

Figure 4: Function block

The DoS_WARNING signal is activated (set to TRUE) if the protection relay's internal frame rate limiters detect an overflow and thus abnormally large amount of Ethernet traffic. The warning signal stays TRUE as long as the internal limits stay exceeded.

The Dos_ALARM signal is activated when the Dos_WARNING signal has been set for over 2 seconds. In practice, this means that the abnormal network condition has lasted for a while and not returned to normal in a short period of time.

An Admin log security event is generated by the DoS_ALARM signal.

3.3.4.3 RateLimiter settings in a HSR loop redundancy system

When enabling the relays RateLimiter functionality it is important to calculate and adjust the worst case bandwidth usage for different traffic types. Especially attention needs to be used if a loop redundancy protocol such as HSR is used in combination with the RateLimiter. As all the network traffic flows through the relays internal switch it is also being limited by the internal RateLimiter. This means network load in a redundant loop system must be carefully calculated and RateLimiter settings adjusted accordingly. Proper limit values can be very challenging to determine. If there is doubt with the correct settings, it might be best to disable RateLimiter in a HSR-loop relay system to avoid unexpected network issues.

Default policer:

This policer must be set to a worst case traffic load of TCP/Unicast/broadcast traffic flowing through the relay in the HSR loop during a given worst case point-of-time. If system uses many TCP protocols (such as MMS, FTP, HTTPS, Modbus, ..) the traffic bandwidth requirement can be rather high in some cases. Also the parameter value set to the Default policer must be then multiplied by the number of relays in the HSR loop, due to operation principle of HSR protocol, where all network traffic

can flow through a single HSR networking node, thus flowing through the same Default policer. If unsure about worst case bandwidth usage it can be advisable to set the value to e.g. maximum value. Some examples of typical maximum momentary network load of different TCP protocols (values can vary depending on relay etc.):

- WHMI max worst case bandwidth 10-11 Mbps (during communication initialization)
- FTP max worst case bandwidth ~5 Mbps (during file upload)
- MMS max worst case bandwidth 1.5 3 Mbps (during client connection initialization)
- Modbus max worst case bandwidth: less than 1 Mbps

GOOSE/SMV policer:

These multicast policers must be set to worst case maximum GOOSE/SMV packet load inside the HSR loop. Again, in HSR loop it must be considered that the policer does not only limit the GOOSE/SMV traffic to the single network node, but it limits the multicast traffic flowing through the relay to the rest of devices in the loop. Thus a large enough value must be set to allow all multicast flow without packet drops.

Diagnostics:

When enabling the RateLimiter it is important to understand the side-effect of having too small bandwidth limits in the relay. When the RateLimiter bandwidth threshold is exceeded the relay drops packets for the rest of the policing period. This may look like an intermittent networking issue from system point-of-view due to randomly dropped packets. Thus, when RateLimiter is enabled in the relay, it is important to monitor for possible packet drops from HMI and GSAL DoS warning/alarm output signals for any violations of the configured policing limits. Especially this is important with loop redundancy scheme such as HSR, where a sufficient bandwidth threshold can be difficult to determine. In case where there is uncertainty if the bandwidth limit is set high enough or not, it is better to set the policer limit too high than too low, to avoid intermittent networking issues, and unnecessary network troubleshooting, or disable RateLimiter completely.

3.4 Secure communication

The protection relay supports encrypted communication service according to IEC 62351-3 in secure communication based on TLS encryption for WHMI and file transfer. There is a dedicated parameter to enable secure communication service for the FTP protocol on each network interface in the relay. If this parameter is set to "Secure" in the relay, FTP requires TLS encryption support from the clients, which means that the client must use FTPS only. PCM600 supports FTPS and is able to download and upload configuration files in encrypted format from the relay. WHMI must always be connected from a Web browser using the HTTPS protocol.



REX640 supports TLS versions 1.2.

The parameter controlling the FTP and HTTPS communication is "On" by default. It can be accessed via the HMI paths **Configuration > Communication > Protocols > Network1, Configuration > Communication > Protocols > Network2** and **Configuration > Communication > Protocols > HMI Port**.

Parameter	Options	Description
Communication/Proto- cols/Network1/FTP	Off	Denies FTP and FTPS
	On	Allows FTP and FTPS
	Secure (Default)	Allows FTPS only
Communication/Proto- cols/Network2/FTP	Off	Denies FTP and FTPS
	On	Allows FTP and FTPS
	Secure (Default)	Allows FTPS only
Communication/Proto- cols/HMIPort/FTP	Off	Denies FTP and FTPS
	On	Allows FTP and FTPS
	Secure (Default)	Allows FTPS only
Communication/Proto-	Off	Denies HTTPS
cols/Network1/HTTPS	On (Default)	Allows HTTPS
Communication/Proto-	Off	Denies HTTPS
cols/Network2/HTTPS	On (Default)	Allows HTTPS

Table 11: Secure communication

DNP3 and IEC 60870-5-104 communication protocols can be configured to use secure authentication or secure authentication with TLS encryption. The secure communication enabling parameters can be accessed via **Configuration** > **Communication** > **Protocols** > **Secure IEC104 (n)** > **General** > **Protocol Sec Mode** for IEC 60870-5-104 and **Configuration** > **Communication** > **Protocols** > **SDNP3.0 (n)** > **General** > **Protocol Sec Mode** for DNP3.

Table 12: Secure authentication

Parameter	Options	Description
Configuration\Communica- tion\Protocols\SDNP3.0 (n)	Off (Default)	Non-secure DNP3 communi- cation
\General\Protocol Sec Mode	App. authentication	Enables application layer end- to- end cryptographic au- thentication
	TLS and appl.auth	Enables application layer end- to- end cryptographic au- thentication and TLS
Configuration\Communica- tion\Protocols\Secure IEC104 (n)\General\Protocol Sec Mode	Off (Default)	Non-secure IEC 60870-5-104 communication
	App. authentication	Enables application layer end- to- end cryptographic au- thentication
	TLS and appl.auth	Enables application layer end- to- end cryptographic au- thentication and TLS



See the communication protocol manuals for more information on how to configure secure communication over IEC 60870-5-104 and DNP3.

Shortcut menu setting *FTP Mode* (see *Figure 5*) specifies the FTP security mode in which PCM600 tries to communicate with the IED. The default mode is always FTPS. With the FTPS option, *Security Mode* is set to "Automatic". With the FTP option, *Security Mode* is set to "None". If the IED has been configured to use the secure

È Substation È Voltage Leve È Bay È Bay È Say È Say	Collapse Signal Monitoring Disturbance Handling Event Viewer Parameter Setting Application Configuration Signal Matrix Graphical Display Editor HMI Event Filtering IED Users			
<u></u>	Communication Management Ethernet Configuration			
E	IED Summary			
She .	Account Management			
	Set Technical Key in IED			
	Update IED			
	License Update			
	Fault Records			
	Load Profiles			
	FTP Mode	•	1	FTPS
	Create Template			FTP

mode (see *Table 11*) and PCM600 nonsecure, the connection is automatically tried with secure mode.

Figure 5: FTP Mode setting



IEC 61850 MMS and Modbus protocols are not secure as such. If these protocols are used, eavesdroppers on the local substation network are able to understand the communication exchange happening with the protection relay.



It is recommended to connect to the local substation network via a VPN tunnel when accessing the protection relay from the untrusted network if a secure communication protocol is not used. This ensures that the communication with the protection relay is encrypted and not understandable outside the local substation network.

3.4.1 Certificate handling

The secure protocols in the protection relay use public key certificates for encryption and secure identification. These certificates bind together a public key with an identity, that is, information such as the name of an organization, their address and so on. The server certificate used by the protection relay when delivered from the factory is generated by the relay itself as a self-signed certificate and not issued by any certification authority (CA).

Certificates use encryption to provide secure communication over the network. An X.509 certificate and an RSA key pair with a key length of 1024 or 2048 bits is used by the protection relay. It is strongly recommended to set the key size to 2048 bits. The RSA key stored in the certificate is used to establish secure communication.

The certificate is used to verify that a public key belongs to an identity. In case of secure communication, the protection relay presents the certificate to the party with whom secure communication needs to be established giving the public key and the identity of the relay. The public key is one part of an asymmetric key algorithm in which one key is used to encrypt message and another key is used to decrypt it. The public-private key pair (asymmetric key) is used to exchange the symmetric key, which is used to encrypt and decrypt the data that is exchanged between server and client.

Messages encrypted with the public key can only be decrypted with the other part of the algorithm, the private key. Public and private keys are related mathematically and represent a cryptographic key pair. The private key is kept secret and stored safely in the protection relay, while the public key may be widely distributed.

The protection relay certificate has to be manually trusted in a separate dialog box when self-signed certificates or manually generated external certificates are used. Once this is done, the certificate is trusted in the communication between the relay and PCM600. For example, when the WHMI is used, the certificate signed by the protection relay must be accepted in the Web browser when opening the connection to WHMI. This is not required in the case of CA-signed certificates automatically generated and updated in the protection relay as part of the public key infrastructure.

3.4.1.1 Certificate acquisition

The certificate used by the device can be acquired in three ways: Self-signed certificate can be generated by the device itself, the certificate can be manually inserted into the device, or it can be automatically acquired through Public Key Infrastructure (PKI).

Self-signed certificate

The self-signed certificate is generated by the relay itself when the relay is started for the first time and no other certificates are already present in the relay. This acts as a factory default certificate to support secure communication. The validity for self-signed certificates is 50 years. This self-signed X.509 certificate uses an RSA key pair with a key length of 2048 bits.

Manual external certificate update

The certificate can be generated from e.g. a third-party PKI infrastructure and imported to the protection relay using the Import and Write certificates functionality of Account Management in PCM600. This also overwrites any



existing certificates in the relay. The format of the certificates is PKCS#12. The recommended key length is 2048 bits.

Figure 6: Manual external certificate update to the protection relay

Automatic provisioning

The device can also acquire the certificate automatically from Public Key Infrastructure (PKI). This requires the device to be enrolled into a PKI system with Simple Certificate Enrollment Protocol (SCEP). SCEP is configured with account management tool and this procedure is covered in more detail in the Public key infrastructure section.

This mechanism uses the PKI framework according to the IEC 62351-9 standard. CA and RA servers should be set up in the network. The CA and RA can be in the same server.

3.4.1.2 Public key infrastructure

Public key infrastructure (PKI) is a framework that consists of secure policies, encryption mechanisms and applications that generate, store, and manage keys. PKI also provides procedures to generate, distribute, and use keys and certificates. PKI can provide a mechanism to publish the public keys that are part of public key cryptography.



Figure 7: Example of a PKI architecture with protection relays

3.4.1.3 Certification authority

The certification authority (CA) is a trusted third party that authenticates entities taking part in an electronic transaction. To authenticate an entity, the CA issues a digital certificate. This certificate is a digital document that establishes the credentials of the entities participating in a transaction.

The digital certificates issued by CAs contain information, such as the name of the subscriber, the public and the private key of the subscriber, and the issuing CAs public key.

The CA uses its own procedures to validate certificate requests. These procedures depend on an organization policy and the infrastructure available to validate the request. If the request is validated, the CA issues the certificate.

Server authentication is based on the server's authentication certificate. Clients can identify the server by its certificate and can choose to communicate with authenticated servers.

3.4.1.4 Registration authority

Registration authority (RA) is an authority in a network that verifies the user requests for a digital certificate and tells the certificate authority to issue it. RAs are part of a public key infrastructure.

3.4.1.5 Automatic certificate provisioning via SCEP

The certificate is automatically generated from the CA server and signed by CA as soon as the CA server is online and IED Key Management has been configured in

Account Management in PCM600. This certificate overwrites the default certificate used for TLS communication in the relay.

Three aspects of certificate management are covered in the protection relay:

- Certificate enrollment: The relay requests the server certificate from the CA server for the first time.
- Certificate renewal: The renewal process begins 30 days before the certificate expires. During this time, a certificate renewal request is attempted every 24 hours if the server is not online.
- Certificate revocation list (CRL): List of revoked certificates is automatically downloaded during successful enrollment or certificate renewal. The CRL update is also attempted once every 24 hours, if the current CRL has expired.

In case of enrollment and renewal, the protection relay first sends a certificate request to the RA server which verifies this certificate request and asks the CA server to issue the certificate to the relay. In the case of CRL the relay requests a new CRL from the CRL distribution point.

For the protection relay to automatically obtain and handle renewal of the CA signed device certificate, the PKIGSAL1 component needs to be instantiated in Application Configuration in PCM600 and the following parameters need to be configured in the IED Key Management section of Account Management in PCM600 and written into the protection relay. The key length of the RSA key pair can be selected in Account Management in PCM600. The recommended key length is 2048 bits.

Parameter	Options	Description
РКІ	Enabled	Makes the protection relay automatically ob- tain and renew the CA-signed certificate
	Disabled (default)	Certificates need to be manually updated in the protection relay
Common name	User-entered value	Common name for the certificate request
Organization	User-entered value	Organization requesting the certificate
Organizational unit	User-entered value	Organizational unit of the organization
Locality	User-entered value	Location where the certificate is stored.
State/province	User-entered value	State/province of the location where the certif- icate is stored.
Country	User-entered value	Country where the certificate is stored.
Subject alternative name	User-entered value	Subject alternative names separated with sem- icolon. Max 6.
Server IP address	User-entered value	IP address of the RA server
Server address	User-entered value	The full URL of the RA server
Port number	User-entered value	Port number to be used in the RA server

Table 13: Configuring PKI

Table continues on the next page

Parameter	Options	Description
Thumbprint	User-entered value	Needs to be the same as
		Thumbprint generated in the CA server – it needs to be copied from the CA server and entered here by the person configuring the cer- tificates for the protection relay
Name	User-entered value	Name of the CA
Server response time- out (s)	User-entered value	How long the CA server waits for the protec- tion relay's response before timing out
Key length	1024	Key length of 1024 bits is used for encryp- tion/decryption
	2048 (default)	Key length of 2048 bits is used for encryp- tion/decryption - recommended
Enrollment password	User-entered value	This needs to be the same as the enrollment password generated in the CA server – it needs to be copied from the CA server and entered here by the person configuring the certificates for the protection relay

The certificate provisioned by the PKI can be deleted from the protection relay by disabling the PKI in IED Key Management tool. The relay generates a new self-signed certificate to replace the signed certificates in use.

3.5 Time synchronization

Time synchronization is a key element of cybersecurity as many functions depend on correct standard time. Time is essential for certificate expiration and renewal and security logging.

The protection relay uses UTC time to provide a temporal order among a set of events. However, timestamps may be presented in a time zone and optionally adjusted by daylight saving time. As events are stored and transferred with UTC timestamps, changing time zone or DST settings always presents them correctly.

To maintain correct time in the real-time clock, a time synchronization method is required. A time server must obtain the time from a trusted source of time, traceable to a standard time source, an atomic clock. Time master supervision function shall be deployed or an event shall be used to supervise that time synchronization is able to receive time from the time server. Time server redundancy is recommended.

The PTP time synchronization method has an additional benefit enabling devices to synchronize each other. Thus, if the time server with reference time source is lost, rest of the devices start drifting as a team. However, this is acceptable only for a short holdover time period and must not be used as a permanent setup. When assessing order of events among the team of protection relays, it is still an advantage if timestamps can be compared across the devices. The device with the best local oscillator shall be elected by the BMC algorithm as the grandmaster for the team which can be prioritized with the PTP priority 2 setting. Ethernet protocol-based time synchronization methods are not secure protocols; only IRIG-B as a physically separate signal is considered secure. The time server for Ethernet synchronization methods shall reside on a local LAN.

3.6 Encryption algorithms

TLS connections are encrypted with AES 256. No passwords are stored in clear text within the Device. A hashed representation of the passwords with SHA384 is stored.

REX640 supports TLS versions 1.2.

4 User management

4.1 Local user account management

Four factory default user accounts have been predefined each with different rights and default passwords. The roles for these four user accounts are the same as the username.

- VIEWER
- OPERATOR
- ENGINEER
- ADMINISTRATOR

The default passwords in the protection relay delivered from the factory can be changed with Administrator user rights or by the users themselves. Relay user passwords can be changed using the LHMI or IED Users in PCM600.

In addition to the default user accounts, eight predefined roles can be assigned to users (including the default roles described above). It is required to login as an Administrator in PCM600 to be able to add custom roles and map them to user rights.

Each protection relay supports 20 roles and 50 user accounts. All roles except ADMINISTRATOR can be modified and each role can have up to 10 rights. Each user account except ADMINISTRATOR can be mapped to a maximum of five roles.

IED Users in PCM600 is used to manage the local user accounts.

- User accounts can be created under any role.
- Only Administrator can create user accounts and update the roles-to-rights mapping.
- Administrator needs to share the default password generated for the user account by the tool with the users and recommend the user to change the password.
- The password of the user accounts can be changed by the users themselves from here or from LHMI.
- Administrator can reset the passwords of the users.

The user account information is then written to the protection relay from IED Users in PCM600. The user account information is securely maintained in a local database in the protection relay.

Any user logging into the protection relay from LHMI, WHMI (HTTPS) or PCM600 (FTPS and MMS) is authenticated based on the user account information and the rights of this user depend on the rights configured for the role of that user.

Role	Description
VIEWER	Can be used to view which objects are present within the logical device
SECAUD	Can be used for record handling and to view audit logs
OPERATOR	Can be used to view which objects are present within the logical device as well as to perform control operations such as opening or closing the circuit breaker
INSTALLER	Can be used to view which objects are present within the logical device as well as to write files and configure the server locally or remotely
ENGINEER	Can be used to view which objects are present within the logical device as well as to make parameter setting and con- figuration changes in addition to having full access to the data sets and files
RBACMNT	Can be used to manage the roles-to-rights mapping
SECADM	Can be used to perform security management such as roles- to-rights mapping and to change security settings such as certificates for subject authentication
ADMINISTRATOR	Superset of all the roles

Table 14: Description of default user roles

Table 15 describes the default mapping of all the user rights associated with all the roles in the protection relay. This mapping can be modified according to the user requirements.

Table 15: Default roles-to-rights mapping

	VIEWER	OPERATOR	ENGINEER	INSTALLER	SECADM	SECAUD	RBACMNT	ADMINISTRATOR
Alarm list	R	W	R	R	W	W	R	W
Basic monitoring	W	W	W	W	W	W	W	W
Configuration and Setting Change	R	R	w	w	R	R	R	w
Control Operations	R	W	W	R	R	R	R	W
Local HMI Advanced	R	R	R	R	R	R	R	R
Local HMI Basic	R	-	-	-	-	-	-	-
Record Handling	R	R	W	W	W	W	R	W
Security Management	-	-	-	-	W	W	R	W
System update	-	-	W	R	W	R	R	W
Test Mode	-	-	W	R	R	R	R	W
User Management	-	-	-	-	W	W	W	W

User account information can be exported from IED Users in PCM600 to an encrypted file which can then be imported into another protection relay.



User authorization is disabled by default for the LHMI and can be enabled with the *Local override* parameter via the menu path **Configuration** > **Authorization** > **Passwords**. WHMI always requires authentication. Changes in user management settings do not cause the protection relay to reboot. The changes are taken into use immediately after committing the changed settings on the menu root level. When the *Local override* parameter is enabled, the Local User Account Management comes into use unless Central Account Management is enabled

If the *Remote override* parameter from the **Configuration** > **Authorization** > **Passwords** menu has been disabled, all MMS communication (like communication with SCADA) requires authentication using the correct password. Remote override is enabled by default. *Remote override* does not impact FTP/FTPS clients like PCM600 and HTTPS clients like WHMI. Username and password are always required for communication with the relay over FTP/FTPS and HTTPS protocols.



If the PCM600 authentication has been enabled in PCM600 System Settings, a relay user can be linked to the current PCM600 user by selecting the **Remember me** check box in the **Login** dialog. After that, the user credentials are no longer asked at tool communication as logging in PCM600 also provides the authentication credentials to the protection relay.



The Administrator user shall not be allowed to delete the last ADMINISTRATOR user and itself. FTP/FTPS logins are done by entering the username and password; there is no role selection required. The highest role for the username is automatically selected by the protection relay. Performing the Restore Factory settings operation in IED Users in PCM600 restores user accounts to the factory user accounts. The read rights in the roles-to-rights role mapping can be disabled but the read rights are always restored when the roles are read from the protection relay in the Roles to Rights mapping section of IED Users or Account Management Tool in PCM600.

4.1.1 Password policies

Passwords are settable for user accounts in all roles. Only the following characters are accepted.

- Numbers 0-9
- Letters a-z, A-Z
- Space
- Special characters !"#%&'()*+´-./:;<=>?@[\]^_`{|}~

By default, the password policies in the protection relay are as follows:

- Minimum password length: 6
- Maximum password length: 20
- Minimum uppercase characters: 0
- Minimum numeric: 0
- Minimum special characters: 0

The protection relays are delivered from the factory with default passwords. It is required to change the default passwords.
Table 16: Predefined users	, their passwords and roles
----------------------------	-----------------------------

Username	Password	Predefined role
VIEWER	remote0001	VIEWER
OPERATOR	remote0002	OPERATOR
ENGINEER	remote0003	ENGINEER
ADMINISTRATOR	remote0004	ADMINISTRATOR

The following enforcing rules of the password policies can be customized in IED Users in PCM600.

- Option of enabling or disabling password policies (disabling sets default policies as described above)
- Minimum password length
- Use of uppercase characters
- Use of lowercase characters
- Use of numbers
- Use of special characters

It is required to login as an Administrator in PCM600 in order to change the password policies.

Each user can change their own password, but only Administrator can reset the passwords of other users.

On Factory restore, factory default usernames, passwords and password policies are restored.



User authorization is disabled by default and can be enabled via the LHMI **Configuration > Authorization > Passwords**.



For user authorization for PCM600, see the PCM600 documentation.



Policy change and configuration is not allowed when the protection relay is in offline mode in PCM600.



If the last ADMINISTRATOR password is lost, contact ABB's technical customer support to retrieve the administrator level access.

4.2 Central account management

The user accounts and roles can be created and authenticated centrally in a central account management (CAM) server using the LDAP protocol. CAM can be activated in the protection relay from Account Management in PCM600 or LHMI.

A CAM server can be an Active Directory (AD) server such as Windows AD. There can also be a secondary/redundant CAM server configured which can act as a backup

CAM server if the primary CAM server is not accessible. Normally, an AD server use the LDAP protocol for central authentication.

The protection relay is the CAM client. It can maintain its own replica database of the user accounts and roles configured in the CAM server. This CAM replica database acts as a backup authentication mechanism if both CAM servers (primary and secondary) are not accessible from the protection relay.

Each protection relay supports 20 roles and 50 user accounts in the CAM replica database. Each user account can be mapped to a maximum of five roles.



In CAM servers, the "Group" term is used when an Active Directory (AD) server acts as CAM server. The protection relay internally views the groups as roles.

4.2.1 Central account management server

The central account management (CAM) server is maintained by the central Administrator who manages the user accounts. The CAM server is used to

- Create and maintain user accounts and role information
- Authenticate user accounts when the user logs in to the protection relay from the LHMI or WHMI (HTTPS protocol) or PCM600 (FTPS protocol)



If the AD server is configured as the CAM server, the password expiry needs to be handled at the system level by the Administrator. Expired passwords cannot be changed from the protection relay's LHMI or WHMI if an AD server is configured as the CAM server.

4.2.2 CAM client – protection relay

4.2.2.1 Central account management configuration in protection relay

Central account management (CAM) can be configured in the protection relay in two ways once user accounts and roles or groups are created in the CAM server.

Common step for a system with any CAM server

The CAM configuration can be manually updated in Account Management in PCM600 and written to the protection relay for the protection relay to be able to communicate with the CAM server.

Table 17: CAM server (e.g Active Directory) parameters configured in Account Management in PCM600

Parameter	Options	Description
Device CAM mode	Enabled	Authentication done from the CAM server
	Disabled (Default)	Authentication done from the local user ac- count management database
LDAP Server 1	User-entered value	IP address of CAM server 1
LDAP Server 2	User-entered value	IP address of CAM server 2

Parameter	Options	Description
Base DN	User-entered value	Base DN for the CAM server
Replication Group	User-entered value	Determines which users need to be replica- ted in the protection relay (not applicable if an Active Directory server acts as CAM serv- er)
Replication interval	User-entered value	Determines how often the replication takes place

4.2.2.2 Central account management monitoring in protection relay

The following information is displayed in the LHMI under **Monitoring** > **IED Status** > **CAM** for easy identification of the authentication mechanism used in the protection relay and its status.

- UAM mode
 - "Central" denotes that authentication happens from the CAM server.
 - "Local" denotes that authentication happens from local user account management.
- CAM server 1: Displays the status of the primary CAM server, whether it is online or offline.
- CAM server 2: Displays the status of the secondary/redundant CAM server, whether it is online or offline.

4.2.3 Authentication in central account management mode

This chapter describes the authentication mechanism when the protection relay is in the central account management (CAM) mode.

- Once the CAM configuration is written to the protection relay, users logging in to the protection relay from LHMI, WHMI (HTTPS protocol) or PCM600 (FTPS protocol) are authenticated by the CAM server.
- When AD server is used as a CAM server, it is not possible to change the password from the WHMI or LHMI. It is recommended to disable the option in the AD server which forces the password change when logging in for the first time.
- In order for CAM to get activated when an AD server is used as a CAM server, the test for CAM connection by using the username and password supplied when writing the CAM configuration should be successful. Otherwise the authentication mechanism reverts to using the local user account management.
 - The protection relay stores the user account information for every successful login with the AD server in a cache since the AD server does not support replication. Up to 50 encrypted and securely stored user account records can be stored in the protection relay.
- When the CAM server goes offline, for example, due to network issues and the backup CAM server is also unavailable or the protection relay is offline, user authentication is done from the local AD cache when the AD server is used as the CAM server.
- Communication with CAM servers happens over LDAP or LDAPS.
- A user account is locked out for 30 seconds after five unsuccessful login attempts. A security log event is logged to record this.



MMS authentication does not work when the CAM mode is enabled in the relay because the IEC 61850 MMS protocol does not support username and role for login.

Password change is possible only when the CAM server is online and the changes made in the LHMI are also reflected in the CAM server.



The password policies for CAM depend on the CAM server.



When the protection relay is in the CAM mode and an AD server is acting as the CAM server, the "Full name" configured in the AD server should be used as the username when logging into the protection relay.



In case CAM with AD has been configured in the protection relay, a user with ADMINITRATOR privileges can delete any user credentials stored in the protection relay's cache by navigating via LHMI or WHMI to **Configuration > Authorization > CAM > Clear AD userlist**.

4.2.3.1 Creating a one-time password

If the ADMINISTRATOR password is lost and there is no user account available to be used for logging into the protection relay, a one-time password can be generated.



The IP address 192.168.0.254 in the steps below is the default address. If a custom IP address has been defined, it should be used instead.

- 1. Connect a computer to the HMI port of the protection relay.
- 2. Open a Web browser and go to #https://192.168.0.254/OTP.html/EN-
- 3. Forward the displayed OTP related information to ABB's technical customer support to receive a one-time password.
- 4. Reset the ADMINISTRATOR password.
 - a) Open #https://192.168.0.254/OTP.html/EN-.
 - b) Type the ADMINISTRATOR username with capital letters.
 - c) Type the one-time password.
 - d) Click **Reset**.



Once the OTP is used to reset the protections relays' user accounts (that is, the user accounts are reverted to factory defaults), the previous Local User Account Management/CAM configuration is lost and needs to be reconfigured from the Account Management Tool in PCM600.

4.2.4 User account creation and authentication

When a new user account is created in the central account management (CAM) server and the relay is configured so that authentication happens from the CAM server, several steps are needed to complete the user configuration. See the engineering manual for a detailed description and screenshots.

• The CAM configuration is written to the protection relays.



The configuration details can be edited in Account Management in PCM600 at any time and written to the relay.

The user logging into the protection relay is authenticated by the primary or secondary CAM server; if the CAM server is not available, the user is authenticated from the CAM replica database.

4.2.5 Central account management and certificates

The protection relay can obtain and renew the device certificate automatically by enabling and configuring the PKI parameters in the protection relay. CAM can be configured to work with a CAM server like an AD server.

Mechanism for device	CAM server		
certificate generation	Generic CAM server	AD server	
Self-signed certificate	х	х	
Manual external certificate	х	х	
Automatic external certifi- cate (PKI)	x	х	

Table 18: CAM servers and supported device certificates

4.3 Local user account management and central account management

The choice of the user management mechanism is up to what the system user wants. Central account management has a lot of benefits over local user account management.

- Authentication of the protection relays configured for central account management (CAM) happens from a central server.
- User accounts and role information can be centrally created and maintained this means that changing existing user accounts is easy and needs to be done only on one server.
- User accounts can be configured in multiple protection relays at the same time.
- Password change handing is straightforward.
- Backup CAM servers can be configured if the primary CAM server is down.

4.4 Login banner

Local HMI and web HMI provide capability to display system use notification message before authentication. System use notification can be configured in PCM600 Account Management.

Elements in the system use notification message are:

- Individual is accessing a system owned by the asset owner
- System usage may be monitored, recorded and subject to audit
- Unauthorized use of the system is prohibited and subject to criminal and/or civil penalties
- Password change handling is straightforward
- Use of the system indicates consent to monitoring and recording.

4.5 System use notification

When a component provides local human user access/HMI, it shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.

5 Security logging

5.1 Security log

The protection relay offers a large set of event-logging functions. Critical system and protection relay security-related events are logged to a separate nonvolatile security log for the administrator.

Security log is a chronological record of system activities that allows the reconstruction and examination of the sequence of system and security-related events and changes in the protection relay. Both security log events and process-related events can be examined and analyzed in a consistent method with the help of Event List in LHMI and WHMI and Event Viewer in PCM600.

The protection relay stores 2048 security log events to the nonvolatile security log. Additionally, 1024 process events are stored in a nonvolatile event list. Both the security log and the event list work according to the FIFO principle. The nonvolatile memory does not need battery backup nor regular component change to maintain the memory storage.

Security log events related to user activity are defined according to the IEEE 1686-2013 standard. The logging is based on predefined user names and roles. The user security log events are accessible with IEC 61850-8-1, PCM600, LHMI and WHMI.

Security log events can be classified based on the severity as security events or alarms.

PCM600 Event Viewer can be used to view the security log events and processrelated events. Security log events are visible through a dedicated Security events view. Since only the administrator has the right to read security log, authorization must be used in PCM600. The security log cannot be reset, but PCM600 Event Viewer can filter data.

5.2 Central Activity Logging

The security log events can be reported from the relay to a Central Activity Logging (CAL) server in Syslog format. The relay is the CAL client and it sends the events to a CAL server or any other tool capable of handling the Syslog format.

There can be a maximum of two CAL servers connected to the protection relay at any time. To enable logging of the security log events to a Syslog server, the User Activity Logging feature needs to be enabled in the protection relay and parameters need to be set for each UAL server where it is required to send the security log events.

Parameter	Options	Description
Enable UAL	Enable	Enables user activity logging at the CAL server
	Disable (Default)	Disables user activity logging at the CAL server
Server IP	User-entered value	IP address of the CAL server
Communication type	UDP (Default)	Uses UDP for communication with the CAL server
	ТСР	Uses TCP for communication with the CAL server
Communication port	514 (Default)	Port used for UDP
	1468	Port used for TCP

This can be done in **Configuration** > **User Activity Log** from LHMI, WHMI or Parameter Setting in PCM600. The CAL server also needs to be configured with the details of the relay.

- *Port number*: Same as the port number set in the relay
- *IP address*: IP address of the relay from which the CAL server receives the log events

The events logged into the Syslog server have the following information:

- Date and time when the event occurred
- Event ID: Each event has a unique security ID
- Serial number (SOE number): This is a sequential number which indicates the sequence of occurrence of the event
- User and role name: The user who performed the event and the role associated with that user
- Severity: Whether it is a security event or alert
- Extra Info: Contains additional useful information about the event



If an event occurs while communication with the CAL server is inaccessible, the events are not retransmitted. In this case, use Event Viewer in PCM600 to read out the activity logging from the protection relay.



The protection relay supports Syslog version 1.

5.3 Security log events

Table 20: Security log events

Event Id	Event text	Security log	Syslog	Trigger
1110	Log-in successful	Event	5 - Notice	Login to relay
1130	Log-in failed - Wrong credentials	Event	5 - Notice	Fail a login at- tempt
1210	Log-out (user log- ged out)	Event	5 - Notice	User logs out
1220	Log-out by user in- activity (timeout)	Event	5 - Notice	User logged out due to time out
1370	Viewed Security Event logs success- fully	Event	5 - Notice	Security log ac- cessed
1380	Parameter changed successfully	Event	5 - Notice	Parameter changed
1460	Parameter change failed - no rights	Alarm	1 - Alert	Attempt to change parame- ter without ac- cess
1470	Parameter change failed - out of range	Event	5 - Notice	Attempt to change parame- ter out of range
1520	Software updated successfully	Event	5 - Notice	Update SW through FUT
1610	Device software update failed	Event	5 - Notice	Failed to update SW through FUT
1680	Disturbance re- cords deleted suc- cessfully	Event	5 - Notice	Delete Disturb- ance records
1687	Fault records cleared successfully	Event	5 - Notice	Delete Fault re- cords
1688	Load Profile re- cords cleared suc- cessfully	Event	5 - Notice	Delete Load Pro- file records
1730	Admin password reset to factory de- fault	Alarm	1 - Alert	Restore IED users through OTP
2110	User account cre- ated successfully	Event	5 - Notice	New account cre- ated with PCM

Event Id	Event text	Security log	Syslog	Trigger
1120	User account de- leted successfully	Event	5 - Notice	Account deleted with PCM
2160	New role assigned to user successfully	Event	5 - Notice	Add new role to user account
2170	User role assign- ment removed suc- cessfully	Event	5 - Notice	Remove role from user ac- count
2180	New role created successfully	Event	5 - Notice	Create new user role
2190	Role deleted suc- cessfully	Event	5 - Notice	Delete existing user role
2210	User password changed success- fully	Event	5 - Notice	Attempt to change pass- word
2220	Change of user password failed	Event	5 - Notice	Attempt to change pass- word to some- thing which doesn't follow policies
3290	Ethernet connec- tion failure	Alarm	1 - Alert	Fails to connect external server (for example PKI)
5120	Reset trips	Event	5 - Notice	Clear trip indica- tions from the re- lay
5270	System startup	Alarm	1 - Alert	Boot the relay (Can only been seen in security log)
6110	Test Mode started successfully	Event	5 - Notice	Start relay test mode
6120	Test Mode ended successfully	Event	5 - Notice	End relay test mode
6130	Control operation performed success- fully	Event	5 - Notice	Perform some control operation
6220	Source time sync operation success- ful	Event	5 - Notice	Enable Time syn- chronization
6320	Source time sync operation failed	Event	5 - Notice	Enable Time syn- chronization

Event Id	Event text	Security log	Syslog	Trigger
7310	Hardware change detected	Alarm	1 - Alert	Error/Change in IO configuration detected
8020	Date and time set successfully	Event	5 - Notice	Set Date/Time in relay
8030	New certificate generated success- fully	Event	5 - Notice	Disable PKI con- figuration
8070	System restore per- formed successful- ly	Event	5 - Notice	Restore factory settings (Securi- ty log only)
9010	Flooding attack de- tected	Alarm	1 - Alert	Start a flooding attack
9710	Transfer CRL into the entity success- fully	Alarm	1 - Alert	CRL transferred successfully from PKI server
9810	Failed to transfer the CRL into the device	Alarm	1 - Alert	CRL transfer fails from PKI server
9830	CRL expired	Event	5 - Notice	CRL has expired
13200	Configuration transferred to the device successfully	Event	5 - Notice	Update SCL/GDE configuration
13210	Configuration transfer to the de- vice started	Event	5 - Notice	SCL configura- tion transfer started
13520	Certificates trans- ferred to the device successfully	Event	5 - Notice	PKI certificate transferred to device success- fully
14200	Failed to transfer configuration to the device	Event	5 - Notice	SCL/GDE config- uration transfer fails
14520	Failed to transfer certificates to the device	Event	5 - Notice	PKI certificate transfer fails
20001	Secure Authentica- tion Unexpected message	Event	5 - Notice	IEC104/DNP3 Se- cure Authentica- tion Unexpected message
20003	Secure Authentica- tion Session key ne- gotiation failed	Alarm	1 - Alert	IEC104/DNP3 Se- cure Authentica-

Event Id	Event text	Security log	Syslog	Trigger
				tion Session key negotiation failed
20006	Secure Authentica- tion Update key ne- gotiation failed	Alarm	1 - Alert	IEC104/DNP3 Se- cure Authentica- tion Update key negotiation failed
20011	Secure Authentica- tion Error message received	Event	5 - Notice	IEC104/DNP3 Se- cure Authentica- tion Error mes- sage received
20012	Secure Authentica- tion Error message sent	Event	5 - Notice	IEC104/DNP3 Se- cure Authentica- tion Error mes- sage sent
20100	Secure Authentica- tion Authorization failed	Event	5 - Notice	IEC104/DNP3 Se- cure Authentica- tion Authoriza- tion failed
20101	Secure Authentica- tion Authentication failed	Event	5 - Notice	IEC104/DNP3 Se- cure Authentica- tion Authentica- tion failed
20102	Secure Authentica- tion Session rekey authn failures	Alarm	1 - Alert	IEC104/DNP3 Se- cure Authentica- tion Session re- key authn failures
20688	Event records cleared	Event	5 - Notice	Clear relay event records
22180	Role rights modi- fied	Event	5 - Notice	Modify role rights with PCM600
3901	CAM configuration enabled	Alarm	1 - Alert	Enable CAM suc- cessfully
3902	CAM configuration disabled	Alarm	1 - Alert	Disable CAM suc- cessfully

6 Using the HMI

6.1 Using local HMI

To use the LHMI, logging in and authorization are required. Password authorization is disabled by default for a paired LHMI and can be enabled via the LHMI.



To enable password authorization, select **Configuration** > **Authorization** > **Passwords**. Set the *Local override* parameter to "False".

SHMI supports the same functionality as the LHMI. See the operation manual for more information on login, logout and the pairing process.

6.1.1 Connecting local HMI

1. Connect the HMI to the protection relay via the HMI port and provide the IP address of the protection relay's HMI port.



Figure 8: Setting the relay's IP address

A dialog box opens asking if the relay connection is trusted.

2. Verify the certificate details and click **Trust this Relay**.

		1/2	
	Is this relay o	connection truste	d?
Relay Connection De	etails		
Address: Relay Name: Organization: Valid From: Valid Until: Country: Certificate Thumbprint: Certificate Issuer:	192.168.0.254 ABB-IED-1VHA123456R2 ABB 2020-01-15 15:33:50 2070-01-03 15:33:50 FI 6577655FCE5ADCB0627 ABB	1C90CEE53F3D95C43BBDB	
	Tri	ust this Relay	Change Relay Address

Figure 9: Verifying the certificate details

6.1.2 Logging in

1. Once the HMI is connected to the relay, tap the **LOGIN** icon on the menu bar.



Figure 10: Logging in to local HMI

2. Acknowledge the login banner notification if displayed.

Login

Only authorized personel are allowed to login to this system. Any unauthorized use is strictly prohibited and will be legally prosecuted. If unsure, please do not attempt to login.



Figure 11: Login banner in local HMI



User Editable login banner provides a way to display a definitive warning to any possible intruders that may want to access your system that certain types of activity are illegal, but at the same time, it also advises the authorized and legitimate users of their obligations relating to acceptable use of the computerized or networked environment(s) as is required by IEC 62443-4-2 Component Requirement 1.12 System use notification.

3. Provide the username and password in the dialog box.



Keep the SHIFT key pressed for two seconds to switch from typing in lowercase to typing in uppercase, and vice versa.

REX Feed	(640 er +J02		C	Overv	iew			0	9.06. 11:1	.201 9 %	8					LOGI	N	R	Ŷ	A 0	=	=
	GENERAT	FOR B	REA					æ	Lc	ogi	n					×					۲	
			I		Us	erna	me															
			I		Ρ	assw	vord															
-				_	_	1		_	_		_	_	_	_	_	_				_		
		q	v	V	е		r	1	t	7	/	ι	l		i	C		p)			
		ĉ	ì	s	;	d	1	f	Ç	J	h			j	ł	٢						
				Z		x		0	v	/	b			n	n	n		<	<u>ि</u>	<		
	12	3			,													N	le	xt		

Figure 12: Providing the user credentials

The user is logged in to the protection relay and the username is displayed on the menu bar of the HMI.



Figure 13: Logged in user

After a successful authentication to one relay, the SHMI tries to automatically log in to the other relays using the same username, password and role. If the login fails, username and password are asked again.

If the login fails because all sessions are in use, an error message is shown on the login page.

REX640 Feeder +J02	Timeline	10.04.2019 16:06 🕱	?	🗘 LC	DGIN		
(Login Failed: The maximum numb has been reached	er of logged	in users		ОК		Q
		• PHLPTOC1, S	START, L1,L	2			
		• PHHPTOC1, :	START, L1				
		• PHLPTOC1, C	OPERATE, L	1,L2,L3			
		+1018 Events					
	PHPTOV1, 100%, 0s				• DSTPD	IS1, 100%, 0.0)24s
	• PHPTOV1, 100%, 0s						
	+8 Fault Records						
		• 020A0012	, 1000, Man	ual			
		• 020A00	13, 1000, U1	1 (AIM0010)			
		+9 Dis	turbance Re	ecords			
	2018 -		-		_1 8	2019	

Figure 14: Local HMI error message

6.1.3 Logging out

- 1. Tap the username on the menu bar.
- 2. Tap Log out.



Figure 15: Logging out



Logging out from the SHMI automatically results in a logout from all of the connected relays.



Changing the password causes an immediate logout. Changing password is not available in the logout menu when the navigation page is open. Navigate to a relay and use the logout menu in the relay's HMI to change the password.



If the HMI and the protection relay have not been paired and there is no user activity for the duration set in **Configuration** > **Web HMI timeout**, the HMI session is logged out. By default, the timeout duration is three minutes.

6.1.4 Pairing HMI with protection relay

It is possible to work with the LHMI by connecting the LHMI to the protection relay and then logging in without pairing the LHMI and the protection relay. In this case, the LHMI acts as a remote client: the user privileges are similar to those of the Web HMI and operations, such as control operations, are restricted.

If the LHMI and the protection relay are paired, the LHMI acts as a local client: all operations allowed for an LHMI are allowed in the protection relay, which recognizes the LHMI as a local client in all subsequent connections.



To use the LHMI, logging in and authorization are required. Password authorization is disabled by default and can be enabled via the LHMI. To enable password authorization, select **Configuration** > **Authorization** > **Passwords**. Set the parameter *Local override* to "False".

- 1. Connect the LHMI to the protection relay and log in to the protection relay in the LHMI.
- 2. Tap the menu option in the top right corner of the LHMI and tap **Pair With Relay**.

Pair Pan	el & Relay	02.04.2018 14:22 🏂	(1		≣
				ഗ Pair With Relay	y
			L/R State		~
Device Information			Language		~

Figure 16: Pairing the LHMI with the relay

A dialog box opens to confirm pairing the LHMI with the protection relay.

REX640 Pair Pa	anel & Relay	24.01.2020 17:10 🏂		$\left \frac{L}{R} \Delta_0 \right \equiv$
Т	his panel	is not paired wit	h the relay!	
Relay Details				
Serial Number: Certificate Issuer: Valid From: Valid Until: Certificate Thumbprint: Panel Certificate De	1VHA123456R2 ABB 15.01.2020 15:: 03.01.2070 15:: 6577655FCE5A tails	Relay Address: 33:50 33:50 DCB06271C90CEE53F3D95C4	192.168.0.254 43BBDB	
Certificate Thumbprint:	755F3C416EFE	4401F40BE5BCF554E3D7EE48	45930	
		Pair		Skip Pairing

Figure 17: Confirming LHMI pairing with the protection relay (after login)

The LHMI also automatically asks for pairing once the LHMI is connected to the protection relay. The **Pair** option is available if the user is logged in to the protection relay in the LHMI.

REX640 REX640	Pair Pa	nel & Relay	24.01.2020 17:08 🔀			$\frac{1}{R}$	≡
	TI	his panel	is not paired wi	th the relay	!		
	Please	login as ADN	INISTRATOR to pair t	he HMI with the	relay.		
Relay Detail	s						
Seria Certifica V V Certificate Th Panel Certifi Certificate Th	I Number: tte Issuer: alid From: 'alid Until: umbprint: icate Det umbprint:	1VHA123456R2 ABB 15.01.2020 15:: 03.01.2070 15:: 6577655FCE5A ails 755F3C416EFE	2 Relay Address 33:50 33:50 JDCB06271C90CEE53F3D956 3401F40BE5BCF554E3D7EE4	: 192.168.0.254 C43BBDB 1845930			
			Pair		Skip Pa	iring	

Figure 18: Pairing the LHMI with the protection relay (without login)

6.2 Using Web HMI

6.2.1 Connecting to Web HMI

Connection to WHMI can be established using different communication card ports or the LHMI service port. WHMI is disabled by default and can be enabled with a setting parameter. As only secure communication is supported for the WHMI, it must be accessed from a Web browser using the HTTPS protocol. Three simultaneous LHMI and WHMI sessions are supported.

 To enable the WHMI, select Configuration > HMI > Web HMI mode and set the parameter to "On".

- 2. Reboot the relay for the change to take effect.
- 3. Log in with the proper user rights to use the WHMI.

If the WHMI is accessed through the LHMI service port, use the corresponding IP address of the relay communication port. The IP address can be obtained via the Engineer pages. Tap the relay's name on the LHMI menu bar to open the Relay address dialog box.



To establish a remote WHMI connection to the protection relay, contact the network administrator to check the company rules for IP and remote connections.



HTTPS is enabled for all ports by default. To disable the HTTPS for station ports, select **Communication** > **Protocols** > **Network1** > **HTTPS** or **Communication** > **Protocols** > **Network2** > **HTTPS** and set the parameter to "Off". HTTPS is always enabled for the X0/HMI port.



The WHMI write access can be limited with the parameter *HTTPS* write access in **Configuration** > **Authorization** > **Network1** or **Configuration** > **Authorization** > **Network2**.

Disable the Web browser proxy settings or make an exception to the proxy rules to allow the protection relay's WHMI connection, for example, by including the relay's IP address in **Internet Options** > **Connections** > **LAN Settings** > **Advanced** > **Exceptions**.

6.2.2 Logging in

- 1. Open a Web browser.
- 2. Type the protection relay's IP address in the address bar and press ENTER.

3. Acknowledge the login banner notification if displayed.



Figure 19: Login banner in WebHMI



User Editable login banner provides a way to display a definitive warning to any possible intruders that may want to access your system that certain types of activity are illegal, but at the same time, it also advises the authorized and legitimate users of their obligations relating to acceptable use of the computerized or networked environment(s) as is required by IEC 62443-4-2 Component Requirement 1.12 System use notification.

4. Type the username.

5. Type the password.

Login	
Username	
Username	
Password	
Password	
Log in	

Figure 20: Entering username and password to use the Web HMI

If logging in fails because all sessions are used, an error message is shown on the login page.

Log	in
Usern	ame
ADM	IINISTRATOR
Passw	ord
•••••	
\otimes	Login Failed: The maximum number of logged in users has been reached
L	og in
L	og in

Figure 21: Web HMI error message

6. Select the role if an additional view opens.

This view opens if there are several user roles configured.

Login	
Select role	
VIEWER	~
Select	

Figure 22: Selecting user role

The progress indicator is displayed until the WHMI opens and the dashboard view is shown.



It is recommended to disable the auto-complete feature, which is usually enabled by default, in the Web browser to prevent the usernames and passwords from being stored in the browser's cache.

6.2.3 Logging out

•

The user is logged out after session timeout. The timeout can be set in **Configuration > HMI > HMI timeout**.

To log out manually, click on the menu bar.



If password authorization is enabled (*Local override* is set to "False") and there is no user activity for the duration set in **Configuration** > **HMI** > **HMI timeout**, the LHMI session is logged out. By default, the timeout duration is three minutes.

7 Protection of relay and system configuration

7.1 Backup files

Backups are not directly part of the cyber security but they are important for speeding up the recovery process, for example, in case of failure of the protection relay. Backups need to be updated when there are changes in configuration.

7.1.1 Creating a backup from the relay configuration

1. Use the "Read from IED" function from the IED context menu in PCM600 to back up the relay configuration.



User authorization is needed before using the tool.

2. Enter the user credentials if the default administrator password has been changed.

Administrator or engineer credentials are needed for authorization.

7.1.2 Creating a backup from the PCM600 project

Backup from the PCM600 project is made by exporting the project.

- On the File menu, click Open > Manage Project to open the project management.
- 2. Select the project from the Currently available projects dialog box.
- 3. Right-click the project and select **Export Project** to open the **Create target file for the project export** dialog box.
- 4. Browse the target location and type the name for the exported file. All project related data is compressed and saved to one file, which is named and located according to the definitions.

7.2 Restoring factory settings

In case of configuration data loss or any other file system error that prevents the protection relay from working properly, the whole file system can be restored to the original factory state. All default settings and configuration files stored in the factory are restored. Only the ADMINISTRATOR can restore the factory settings.

• Select **Configuration** > **General** > **Factory setting** to restore factory settings.

The protection relay restores the factory settings and restarts. Restoring takes 1...3 minutes.



Avoid unnecessary restoring of factory settings, because all the parameter settings written to the relay will be overwritten with the default values. During normal use, a sudden change of the settings can cause a protection function to trip.

7.3 Restoring relay backup from local HMI

1. Connect the LHMI to the relay

REX640 09.06.2022 Pair Panel & Relay n REX640 16:30 This panel is not paired with the relay! **Relay Details** Relay Address: 192.168.2.10 Serial Number: 1VHA123456R2 Certificate Issuer: Valid From: 31.05.2022 17:02:06 Valid Until: 19.05.2072 17:02:06 Certificate Thumbprint: **Panel Certificate Details** Certificate Thumbprint: 755F3C416EFB401F40BE5BCF554E3D7EE4845930 Pair Skip Pairing

2. In the Pair Panel & Relay dialog box, tap Pair.



The **Restore Configuration** dialog box automatically opens if the LHMI has a compatible backup available.

REX640 REX640	Restore Configuration	21.01.2010 04:52 🕱	$\frac{L}{R}$ $\mathbf{A_0}$ \equiv
------------------	-----------------------	-----------------------	---------------------------------------

Restore saved configuration?

This display panel has previously been used with another relay with the same composition. The configuration of that relay was saved in this panel and can be written to this new relay.

Note! Relay device certificate needs to be restored manually in case it has been changed.

Do you want to write the saved configuration to the relay?

Write Configuration to Relay	Details	Discard & Continue

Figure 24: Restoring saved configuration

3. Tap **Details** to see the differences in product and system identifiers between the backup and the new relay.

REX640 REX640	Restore Configur	ration	21.01.2010 04:53 %			≡
Relay Informa	tion B	ackup Value in	LHMI	Relay Value		
Туре	R	EX640		REX640		
Product version	1			1		
Serial number	1	VHA123457R2		1VHA123456R2		
Production date	14	4.12.2017 00:00:0	0.000	14.12.2017 00:00:00.0	00	
SW version	bi	uild.2316		build.2316		
SW date	2	5.03.2019 20:28:0	0.000	25.03.2019 20:28:00.0	00	
SW number	21	RAA00XXXX		2RAA00XXXX		
Interface level	0			0		
Order code	R	EX640_10001		REX640_10001		
Composition cod	e +(P.	EX640B10NN COM2+BIO1+AIM 2+CMP1+LNG1+S	1+PSM2+APP1+AP SCT1+MCT1+PCL1	REX640B10NN +COM2+BIO1+AIM1+F +APP3+APP4+APP5+A APP9+APP10+APP11+ P14+CMP1+LNG1+SC	2SM2+APP1+APP PP6+APP7+APP APP12+APP13+/ T1+MCT1+PCL1	2 8+ AP
				_		
Write Config	juration to Relay		Details	Discard &	& Continue	
		(

Figure 25: Viewing the details of the backup and the new relay

LHMI restores the relay backup if the relay's serial number is different from that in the backup and the composition code of the relay contains all the options in the backup. The relay's composition code may contain more options.

4. Tap **Write Configuration to Relay**. The relay boots so that the new configuration can be taken into use.



Figure 26: Relay rebooting



The following dialog box appears when the relay backup is restored.

Figure 27: Backup restoring succeeds

If errors occur, the error details are shown.



Figure 28: Backup restoring fails

7.4

Restoring relay backup from switchgear HMI



This chapter describes how configuration backup is restored from SHMI.

As a precondition for restoring a backup from the SHMI, the replacement relay's license must include the same or wider capabilities than the faulty relay's license. The replacement relay must have the same HW modules in the same slots as the faulty relay although the other HW modules may differ.

- 1. Configure the faulty relay's network address to the replacement relay, and connect it to the station network so that it can be reached by the SHMI. The network address can be set by using the WHMI.
- 2. Go to the SHMI's navigation page and tap the menu button.
- 3. Tap Connect External.
- 4. Type the replacement relay's IP address and pair with the relay. The replacement relay's HMI opens on the SHMI.
- 5. On the HMI view, tap the menu button and select **Testing and Commissioning and Restore**.
- 6. Select a backup to be restored from the list of available backups and tap **Restore**.

If the Restore selection is not enabled, the relay is incompatible with the selected backup.

7.5 Restoring the administrator password

If authentication is enabled in the protection relay and the ADMINISTRATOR password is lost, it is no longer possible to change passwords or operate the relay with full access rights.

• Contact ABB technical customer support to retrieve back the administrator level access to the protection relay. See *Chapter 4.2.3.1 Creating a one-time password*.

7.6 Decommissioning

If the protection relay needs to be decommissioned, all sensitive information needs to be deleted from the relay as well as from PCM600.

7.6.1 Deleting sensitive information from the protection relay

• Delete the device certificate from the Account Management Tool in PCM600 by clicking the option of deleting the certificate.



Only ADMINISTRATOR can delete the certificate.

- Delete the CA certificate from the Account Management Tool in PCM600 by clicking the option of deleting the certificate if an external certificate has been manually or automatically configured in the protection relay.
- Delete user credentials stored in the protection relay's cache via the LHMI or WHMI path Configuration > Authorization > CAM > Clear AD userlist if CAM with AD was configured in the protection relay.



Only ADMINISTRATOR can delete the user credentials.

- Delete the configuration and updated settings by using the factory restore operation and revert the protection relay to the factory default.
- Delete disturbance records.
 - In LHMI or WHMI, navigate to the **Disturbance Records** page via the menu, select all disturbance records and delete them.
 - In PCM600, open the Disturbance Handling tool and clear the disturbance records. It is required to log in as a user whose role is mapped to the Record handling right.
- Clear audit logs by performing the factory restore operation.
- Delete the PCM600 project and the PCM600 specific stored files.
 - 1. Delete the disturbance records from the Disturbance Handling tool.
 - 2. Delete the device certificates in PCM600 by opening the MMC.exe
 - application in Windows and navigating to Console Root > Certificates - Current User > PCM Permanent Trust > Certificates.

Console1 - [Console Root\Certificat	es - Current User\PCM Permaner	nt Trust\Certificates]				×
🔚 File Action View Favorites	Window Help				-	e ×
🗢 🄿 🙇 🖬 🔏 🖬 🗙 🖬						
Console Root	Issued To	Issued By	Expiration Date	Intended Purpo	Actions	
Certificates - Current User	R ABB_IED_1VHR91184374	ABB_IED_1VHR91184374	12/6/2045	<all></all>	Certificates	
Personal Trusted Root Certification.					More Actions	•
Enterprise Trust					ABB_IED_1VHR91184374	
Intermediate Certification Trusted Publishers Trusted Publishers Trusted Publishers Third-Party Root Certificate Trusted People Other People McAfee Trust Certificates PCM Permanent Trust Certificates PCM Session Trust Certificate Enrollment Req Smart Card Trusted Roots	<	11	-		More Actions	•

Figure 29: Deleting device certificates in PCM600



Restoring factory settings deletes the device certificate, CA certificate, Active Directory information cache, configuration and settings, disturbance records and audit logs from the protection relay.

8 Standard compliance statement

8.1 Application standards

Cyber security issues have been subject to the standardization initiatives by ISA, IEEE and IEC for some time and ABB is actively involved in all these organizations helping to define and implement the cyber security standards for power and industrial control systems.

Some of the most important cyber security standards for substation automation, such as IEC 62351 and IEC 62443 (former ISA S99), are still under active development. ABB is participating in the development by delegating subject matter experts to the committees working on standards. Since the standards are still under development, ABB strongly recommends using the existing common security measures as available on the market, for example, VPN for secure Ethernet communication.

Standard	Main focus	Status
NERC CIP v5	NERC CIP cyber security regulation for North American power utilities	Released, ongoing
IEC 62351	Data and communications security	Partly released, ongoing
IEEE 1686	IEEE standard for substation intelligent electronic devices (IEDs) cyber security capabilities	Finalized

Table 21: Cyber security standards

ABB has identified cyber security as a key requirement and has developed a large number of product features to support international cyber security standards such as NERC-CIP and IEEE1686 as well as local activities like the German BDEW white paper.

The two standards IEC 62351 and IEC 62443 are still under revision. Nevertheless, ABB considers these standards already today as a guideline in implementing product features or system architectures.

9 Glossary

AD	Active directory
CA	Certification authority
CAL	Central activity logging
CAM	Centralized account management
DNP3	A distributed network protocol originally developed by Westronic. The DNP3 Users Group has the ownership of the protocol and assumes responsibility for its evolution.
DST	Daylight-saving time
EMC	Electromagnetic compatibility
Ethernet	A standard for connecting a family of frame-based computer networking technologies into a LAN.
FIFO	First in, first out
FTP	File transfer protocol
FTPS	FTP secure
GOOSE	Generic object-oriented substation event
НМІ	Human-machine interface
HSR	High-availability seamless redundancy
HTTPS	Hypertext transfer protocol secure
IEC	International Electrotechnical Commission
IEC 60870-5-104	Network access for IEC 60870-5-101
IEC 61850	International standard for substation communication and modeling
IEC 61850-8-1	A communication protocol based on the IEC 61850 standard series
IEC 61850-9-2	A communication protocol based on the IEC 61850 standard series
IEC 61850-9-2 LE	Lite Edition of IEC 61850-9-2 offering process bus interface
IED	Intelligent electronic device
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IEEE 1588	Standard for a Precision Clock Synchronization Protocol for networked measurement and control systems
IEEE 1686	Standard for Substation Intelligent Electronic Devices' (IEDs') Cyber Se- curity Capabilities
IRIG-B	Inter-range instrumentation group's time code format B
LAN	Local area network
LC	Connector type for glass fiber cable, IEC 61754-20
LHMI	Local human-machine interface
MMS	1. Manufacturing message specification
	2. Metering management system

Modbus	A serial communication protocol developed by the Modicon company in 1979. Originally used for communication in PLCs and RTU devices.
NERC CIP	North American Electric Reliability Corporation - Critical Infrastructure Protection
ΟΤΡ	One-time password
PCM600	Protection and control IED manager
PKI	Public key infrastructure
PRP	Parallel redundancy protocol
РТР	Precision time protocol
RA	Registration authority
RIO600	Remote I/O unit
RJ-45	Galvanic connector type
SCADA	Supervision, control and data acquisition
SHMI	Switchgear HMI
SI	Sensor input
SMV	Sampled measured values
SNTP	Simple network time protocol
SSH	Secure shell
ST	Connector type for glass fiber cable
ТСР	Transmission control protocol
TCP/IP	Transmission control protocol/Internet protocol
TLS	Transport layer security
ТР	Disturbance data recorded with or without trip bit
UDP	User datagram protocol
UTC	Coordinated universal time
VPN	Virtual private network
WHMI	Web human-machine interface



ABB Distribution Solutions
Digital Substation Products
P.O. Box 699
FI-65101 VAASA, Finland
Phone +358 10 22 11

www.abb.com/mediumvoltage www.abb.com/relion www.abb.com/substationautomation