

RELION® 670 SERIES

# 670 series

## Version 2.1

### Cyber security deployment guideline







Document ID: 1MRK 511 356-UEN  
Issued: March 2019  
Revision: A  
Product version: 2.1

© Copyright 2016 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 and hardware described in this document is furnished under a license and may be used or disclosed only in accordance with the terms of such license.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>) This product includes cryptographic software written/developed by: Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)) and Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

### 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.

### Warranty

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

## Disclaimer

The products are designed to be connected to and to communicate information and data via a network interface. It is the user's sole responsibility to provide and continuously ensure a secure connection between the product and the user's network or any other network (as the case may be). The user shall establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti-virus programs, etc) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB Ltd and its affiliates are not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

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 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.



## 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 2004/108/EC) and concerning electrical equipment for use within specified voltage limits (Low-voltage directive 2006/95/EC). This conformity is the result of tests conducted by ABB 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.

# Table of contents

|                  |  |           |
|------------------|--|-----------|
| <b>Section 1</b> | <b>Introduction.....</b>                           | <b>3</b>  |
| 1.1              | This manual.....                                   | 3         |
| 1.2              | Intended audience.....                             | 3         |
| 1.3              | Product documentation.....                         | 4         |
| 1.3.1            | Product documentation set.....                     | 4         |
| 1.3.2            | Related documents.....                             | 5         |
| 1.4              | Document symbols and conventions.....              | 6         |
| 1.4.1            | Symbols.....                                       | 6         |
| 1.4.2            | Document conventions.....                          | 7         |
| <b>Section 2</b> | <b>Security in Substation Automation.....</b>      | <b>9</b>  |
| 2.1              | General security in Substation Automation.....     | 9         |
| <b>Section 3</b> | <b>Secure system setup.....</b>                    | <b>11</b> |
| 3.1              | Physical interfaces.....                           | 11        |
| 3.2              | Communication ports and services.....              | 11        |
| 3.3              | FTP access with TLS, FTPACCS.....                  | 14        |
| 3.4              | Encryption algorithms.....                         | 14        |
| 3.5              | Denial of service.....                             | 14        |
| 3.6              | Certificate handling.....                          | 15        |
| <b>Section 4</b> | <b>Local user account management.....</b>          | <b>17</b> |
| 4.1              | Authorization.....                                 | 17        |
| 4.2              | Predefined user roles.....                         | 19        |
| 4.3              | Password policies.....                             | 20        |
| 4.4              | IED User management .....                          | 21        |
| 4.4.1            | Starting IED user management.....                  | 22        |
| 4.4.2            | General settings.....                              | 22        |
| 4.4.3            | User profile management.....                       | 23        |
| 4.4.3.1          | Adding new users.....                              | 24        |
| 4.4.3.2          | Adding users to new user roles.....                | 26        |
| 4.4.3.3          | Deleting existing users.....                       | 27        |
| 4.4.3.4          | Changing password.....                             | 29        |
| 4.4.4            | User role management.....                          | 30        |
| 4.4.4.1          | Adding new users to user roles.....                | 30        |
| 4.4.4.2          | Deleting existing User from user roles.....        | 31        |
| 4.4.4.3          | Reusing user accounts.....                         | 31        |
| 4.4.5            | Writing user management settings to the IED.....   | 32        |
| 4.4.6            | Reading user management settings from the IED..... | 32        |
| 4.4.7            | Saving user management settings.....               | 32        |
| <b>Section 5</b> | <b>Central Account Management.....</b>             | <b>35</b> |

|                  |  |           |
|------------------|--|-----------|
| 5.1              | Introduction.....  | 35        |
| 5.2              | Certificate management.....  | 35        |
| 5.2.1            | Creating IED certificates.....   | 36        |
| 5.2.2            | Importing and writing certificates to an IED.....                        | 37        |
| 5.2.3            | Reading certificates from an IED.....                                    | 40        |
| 5.2.4            | Certificate information on local HMI.....                                | 41        |
| 5.2.5            | Invalid certificates .....   | 43        |
| 5.2.6            | Deleting certificates from an IED.....                                   | 44        |
| 5.3              | Activation of Central Account Management.....                            | 45        |
| 5.3.1            | Manual configuration of Central Account Management.....                  | 49        |
| 5.3.2            | Reading configuration from IED.....                                      | 51        |
| 5.3.3            | Deactivation of Central Account Management from PCM600.....              | 51        |
| 5.3.4            | Deactivation of Central Account Management on local HMI.....             | 52        |
| 5.4              | Authorization with Central Account Management enabled IED.....           | 54        |
| 5.5              | Predefined user roles.....   | 56        |
| 5.6              | Password policy settings for Central Account Management enabled IED..... | 58        |
| 5.7              | PCM600 access to Central Account Management enabled IED.....             | 58        |
| 5.7.1            | Changing password.....   | 59        |
| 5.7.2            | Error messages.....  | 60        |
| 5.8              | Trouble shooting Central Account Management.....                         | 62        |
| <b>Section 6</b> | <b>User activity logging.....</b>  | <b>67</b> |
| 6.1              | Activity logging protocol.....   | 67        |
| 6.2              | Activity logging ACTIVLOG.....   | 67        |
| 6.3              | Settings.....  | 67        |
| 6.4              | Generic security application GSAL.....                                   | 68        |
| 6.5              | Security alarm SECALARM.....   | 68        |
| 6.5.1            | Signals.....   | 69        |
| 6.5.2            | Settings.....  | 69        |
| 6.6              | About Security events.....   | 69        |
| 6.7              | Event types.....   | 69        |
| <b>Section 7</b> | <b>Local HMI use.....</b>  | <b>73</b> |
| 7.1              | Logging on.....  | 73        |
| 7.2              | Logging off.....   | 75        |
| 7.3              | Saving settings.....   | 75        |
| 7.4              | Recovering password.....   | 76        |
| 7.5              | Fallback access.....   | 78        |
| <b>Section 8</b> | <b>Standard compliance statement.....</b>                                | <b>79</b> |
| 8.1              | Applicable standards.....  | 79        |
| 8.2              | IEEE1686 compliance.....   | 80        |
| <b>Section 9</b> | <b>Glossary.....</b>   | <b>85</b> |



# Section 1      Introduction

## 1.1      This manual

The cyber security deployment guideline describes the process for handling cyber security when communicating with the IED. Certification, Authorization with role based access control, and product engineering for cyber security related events are described and sorted by function. The guideline can be used as a technical reference during the engineering phase, installation and commissioning phase, and during normal service.

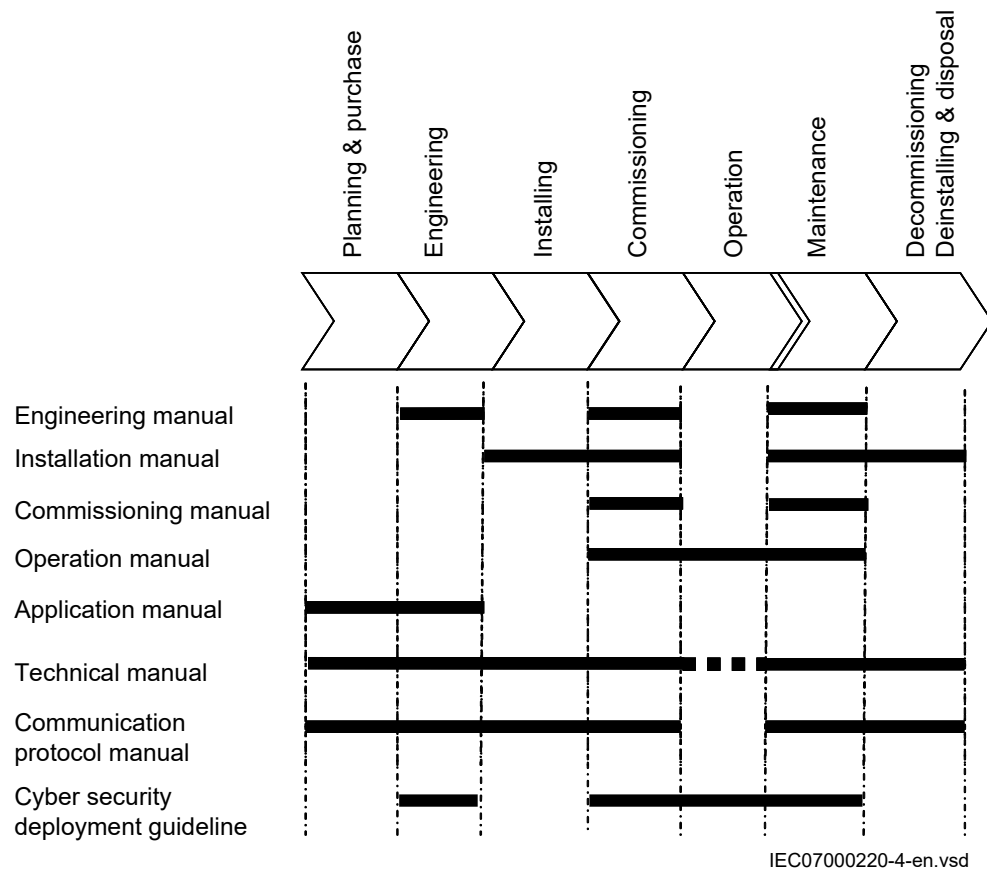
## 1.2      Intended audience

This guideline is intended for the system engineering, commissioning, operation and maintenance personnel handling cyber security during the engineering, installation and commissioning phases, and during normal service.

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

## 1.3 Product documentation

### 1.3.1 Product documentation set



*Figure 1: The intended use of manuals throughout the product lifecycle*

The engineering manual contains instructions on how to engineer the IEDs using the various tools available within the PCM600 software. The manual provides instructions on how to set up a PCM600 project and insert IEDs to the project structure. The manual also recommends a sequence for the engineering of protection and control functions, LHMI functions as well as communication engineering for IEC 60870-5-103, IEC 61850, DNP3, LON and SPA.

The installation manual contains instructions on how to install the IED. The manual provides procedures for mechanical and electrical installation. The chapters are organized in the chronological order in which the IED should be installed.

The commissioning manual contains instructions on how to commission the IED. The manual can also be used by system engineers and maintenance personnel for assistance during the testing phase. The manual provides procedures for the checking of external circuitry and energizing the IED, parameter setting and configuration as well as verifying settings by secondary injection. The manual describes the process of testing an IED in a substation which is not in service. The chapters are organized in the chronological order in which the IED should be commissioned. The relevant procedures may be followed also during the service and maintenance activities.

The operation manual contains instructions on how to operate the IED once it has been commissioned. The manual provides instructions for the monitoring, controlling and setting of the IED. The manual also describes how to identify disturbances and how to view calculated and measured power grid data to determine the cause of a fault.

The application manual contains application descriptions and setting guidelines sorted per function. The manual can be used to find out when and for what purpose a typical protection function can be used. The manual can also provide assistance for calculating settings.

The technical manual contains operation principle descriptions, and lists function blocks, logic diagrams, input and output signals, setting parameters and technical data, sorted per function. The manual can be used as a technical reference during the engineering phase, installation and commissioning phase, and during normal service.

The communication protocol manual describes the communication protocols supported by the IED. The manual concentrates on the vendor-specific implementations.

The point list manual describes the outlook and properties of the data points specific to the IED. The manual should be used in conjunction with the corresponding communication protocol manual.

The cyber security deployment guideline describes the process for handling cyber security when communicating with the IED. Certification, Authorization with role based access control, and product engineering for cyber security related events are described and sorted by function. The guideline can be used as a technical reference during the engineering phase, installation and commissioning phase, and during normal service.

### 1.3.2 Related documents

| Documents related to REB670 | Document numbers |
|-----------------------------|------------------|
| Application manual          | 1MRK 505 337-UEN |
| Commissioning manual        | 1MRK 505 339-UEN |
| Product guide               | 1MRK 505 340-BEN |
| Technical manual            | 1MRK 505 338-UEN |
| Type test certificate       | 1MRK 505 340-TEN |

| Documents related to REC670 | Document numbers |
|-----------------------------|------------------|
| Application manual          | 1MRK 511 358-UEN |
| Commissioning manual        | 1MRK 511 360-UEN |
| Product guide               | 1MRK 511 361-BEN |
| Technical manual            | 1MRK 511 359-UEN |
| Type test certificate       | 1MRK 511 361-TEN |

| Documents related to RED670 | Document numbers |
|-----------------------------|------------------|
| Application manual          | 1MRK 505 343-UEN |
| Commissioning manual        | 1MRK 505 345-UEN |
| Product guide               | 1MRK 505 346-BEN |
| Technical manual            | 1MRK 505 308-UEN |
| Type test certificate       | 1MRK 505 346-TEN |

| Documents related to REG670 | Document numbers |
|-----------------------------|------------------|
| Application manual          | 1MRK 502 065-UEN |
| Commissioning manual        | 1MRK 502 067-UEN |
| Product guide               | 1MRK 502 068-BEN |
| Technical manual            | 1MRK 502 066-UEN |
| Type test certificate       | 1MRK 502 068-TEN |

| Documents related to REL670 | Document numbers |
|-----------------------------|------------------|
| Application manual          | 1MRK 506 353-UEN |
| Commissioning manual        | 1MRK 506 355-UEN |
| Product guide               | 1MRK 506 356-BEN |
| Technical manual            | 1MRK 506 354-UEN |
| Type test certificate       | 1MRK 506 356-TEN |

| Documents related to RET670 | Document numbers |
|-----------------------------|------------------|
| Application manual          | 1MRK 504 152-UEN |
| Commissioning manual        | 1MRK 504 154-UEN |
| Product guide               | 1MRK 504 155-BEN |
| Technical manual            | 1MRK 504 153-UEN |
| Type test certificate       | 1MRK 504 155-TEN |

| Documents related to RES670 | Document numbers |
|-----------------------------|------------------|
| Application manual          | 1MRK 511 364-UEN |
| Commissioning manual        | 1MRK 511 366-UEN |
| Product guide               | 1MRK 511 367-BEN |
| Technical manual            | 1MRK 511 365-UEN |
| Type test certificate       | 1MRK 511 367-TEN |

| Documents related to RER670 | Document numbers |
|-----------------------------|------------------|
| Commissioning manual        | 1MRK 506 361-UEN |
| Product guide               | 1MRK 506 362-BEN |
| Technical manual            | 1MRK 506 360-UEN |
| Type test certificate       | 1MRK 506 362-TEN |

## 1.4 Document symbols and conventions

### 1.4.1 Symbols



The electrical warning icon indicates the presence of a hazard which could result in electrical shock.



The warning icon indicates the presence of a hazard which could result in personal injury.



The caution hot surface icon indicates important information or warning about the temperature of product surfaces.



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. It is important that the user fully complies with all warning and cautionary notices.

## 1.4.2 Document conventions

- Abbreviations and acronyms in this manual are spelled out in the glossary. The glossary also contains definitions of important terms.
- Parameter names are shown in italics.  
For example, the function can be enabled and disabled with the *Operation* setting.
- Each function block symbol shows the available input/output signal.
  - the character ^ in front of an input/output signal name indicates that the signal name may be customized using the PCM600 software.
  - the character \* after an input signal name indicates that the signal must be connected to another function block in the application configuration to achieve a valid application configuration.
- Dimensions are provided both in inches and millimeters. If it is not specifically mentioned then the dimension is in millimeters.



## Section 2      Security in Substation Automation

### 2.1      General security in Substation Automation

The electric power grid has evolved significantly over the past decade thanks to many technological advancements and breakthroughs. As a result, the emerging “smart grid” is quickly becoming a reality. At the heart of these intelligent advancements are specialized IT systems – various control and automation solutions such as substation 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, we offer 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 IEC 60870-5-104, DNP 3.0 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 continual improvement of cyber security solutions specifically for control systems, including substation automation applications.

ABB fully understands the importance of cyber security and its role in advancing the security of substation automation systems. 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 such as NERC-CIP, IEEE 1686 and BDEW Whitepaper. We support verified third-party security patches and antivirus software to protect station computers from viruses and other types of attacks. Cyber security can also be improved by preventing the unauthorized use of removable media (such as USB memory sticks) in station computers. We have built additional security mechanisms into our products. Those offer advanced account management, secure communication, and detailed security audit trails. This makes it easier for our customers to address NERC CIP requirements and maintain compliance standards.

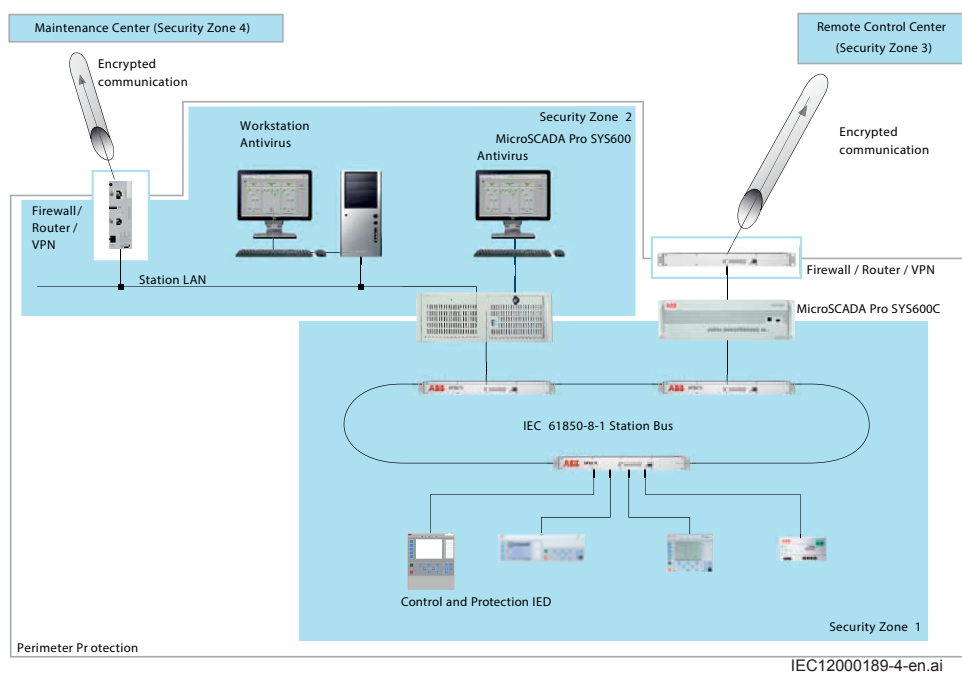


Figure 2: System architecture for substation automation system



## Section 3 Secure system setup

### 3.1 Physical interfaces

To reduce exposure for cyber-attacks and thus comply with cyber security requirements, it must be possible to prevent services in the IED from operating on other physical interfaces than the ones specified by the vendor or by the owner.

### 3.2 Communication ports and services

The port security guideline cannot suggest concrete products for a secure system setup. This must be decided within the specific project, requirements and existing infrastructure.

The ports used in the IED series to set up a firewall are given in table 1. The ports are listed in ascending order. The column "Default state" defines whether a port is open or closed by default. All ports that are closed can be opened as described in the comment column in the table. Front refers to the physical front port. On the rear side of the IED there are four network interfaces labeled 301, 302, 303 and 304. If there is an OEM02 module installed there are two additional optical network interfaces on the rear side, they are labeled 3061 and 3062. The protocol availability on these ports can be configured using the Ethernet configuration tool.

ABB recommends using common security measures, like firewalls, up-to-date anti-virus software, etc. to protect the IED and the equipment around it.



It is recommended to deactivate the Access points and protocols that are not in use to increase cyber security.

Table 1: Available ports

| Port  | Protocol | Default state | Front | 301 | 302 | 303 | 304 | 3061 | 3062 | Service                                 | Comment  |
|-------|----------|---------------|-------|-----|-----|-----|-----|------|------|---|--|
| 21    | TCP      | open          | OFF   | OFF | OFF | OFF | OFF | OFF  | OFF  | FTP                                     | File transfer protocol                         |
| 21    | TCP      | open          | ON    | ON  | ON  | ON  | ON  | OFF  | OFF  | FTPS                                    | Explicit FTP over TLS                          |
| 102   | TCP      | closed        | OFF   | OFF | OFF | OFF | OFF | OFF  | OFF  | IEC 61850 (MMS)                         | MMS communication                              |
| 123   | UDP      | closed        | OFF   | OFF | OFF | OFF | OFF | OFF  | OFF  | SNTP                                    | Enabled when IED is configured as SNTP master. |
| 2102  | TCP      | open          | ON    | ON  | ON  | ON  | ON  | OFF  | OFF  | PCM Access (IED configuration protocol) | IED configuration protocol                     |
| 20000 | TCP      | closed        | OFF   | OFF | OFF | OFF | OFF | OFF  | OFF  | DNP3.0                                  | DNP3.0 DNP communication only                  |

Table continues on next page

| Port                | Protocol | Default state | Front | 301 | 302 | 303 | 304 | 3061 | 3062 | Service     | Comment   |
|---------------------|----------|---------------|-------|-----|-----|-----|-----|------|------|-------------|---|
| 20 000              | UDP      | closed        | OFF   | OFF | OFF | OFF | OFF | OFF  | OFF  | DNP3.0      | DNP3.0 DNP communication only                               |
| 49152               | UDP      | closed        | ON    | ON  | ON  | ON  | ON  | OFF  | OFF  | SNTP Client | Enabled when IED is configured as SNTP client.              |
| 49220<br>—<br>49235 | TCP      | closed        | ON    | ON  | ON  | ON  | ON  | OFF  | OFF  | FTPS        | TCP data ports for FTP PASV command. Ports opens on demand. |

In addition to FTP, SPA, and IED configuration protocol, the IEDs support the following Ethernet communication protocols:

- IEC 61850
- DNP3.0
- IEEE1344/C37.118

These communication protocols are enabled by configuration. This means that the port is closed and unavailable if the configuration of the IED series does not contain a communication line of the protocol. If a protocol is configured, the corresponding port is open all the time.



See the IED series technical manual and the corresponding protocol documentation on how to configure a certain communication protocol.

There are some restrictions and dependencies:

- The port used for IEC 61850 (default TCP port 102) is fixed and cannot be changed.
- The ports used for DNP3 are configurable. The communication protocol DNP3 could operate on UDP (default port 20 000) or TCP (default port 20 000). It is defined in the configuration which type of Ethernet communication is used. Only one type is possible at a time.
- The port used for FTP (default TCP port 21) can be changed in the IED if needed by a 3rd party FTP client.
- The port range used for FTP PASV command is fixed and cannot be changed. The maximum number of simultaneous ports is 16.
- The port used for SNTP when IED is configured as SNTP Client can be changed in the IED.



If the FTP port is changed, PCM600 cannot be used as it cannot be configured to use other IP-ports than port 21 for FTP.

Two ports are used by PCM600 to communicate with the IED. An IED configuration protocol (TCP port 2102) and FTP. The port used by the IED configuration protocol is fixed and cannot be changed. For uploading disturbance records (DR), the FTP port is used.

IP routing is not possible via any of the physical interfaces.

Some IP ports are not possible to use in all physical interfaces.

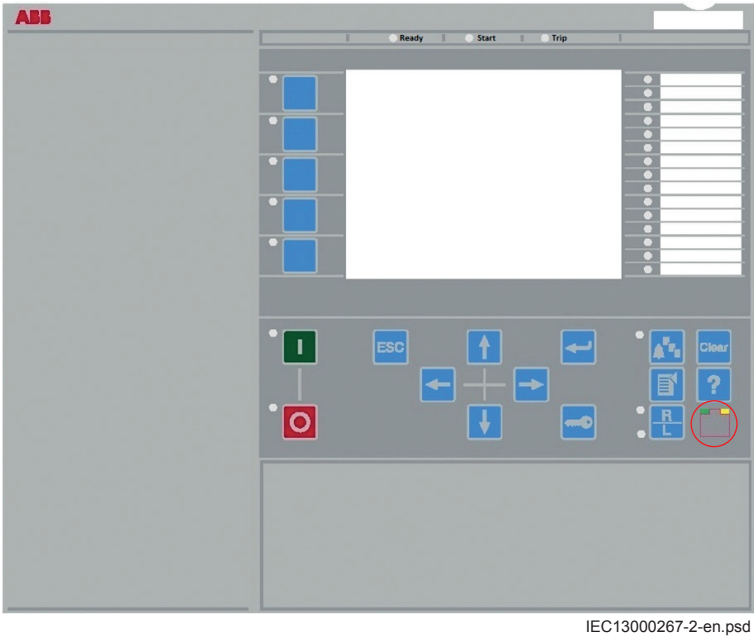


Figure 3: Ethernet port used for PCM600 only, front view

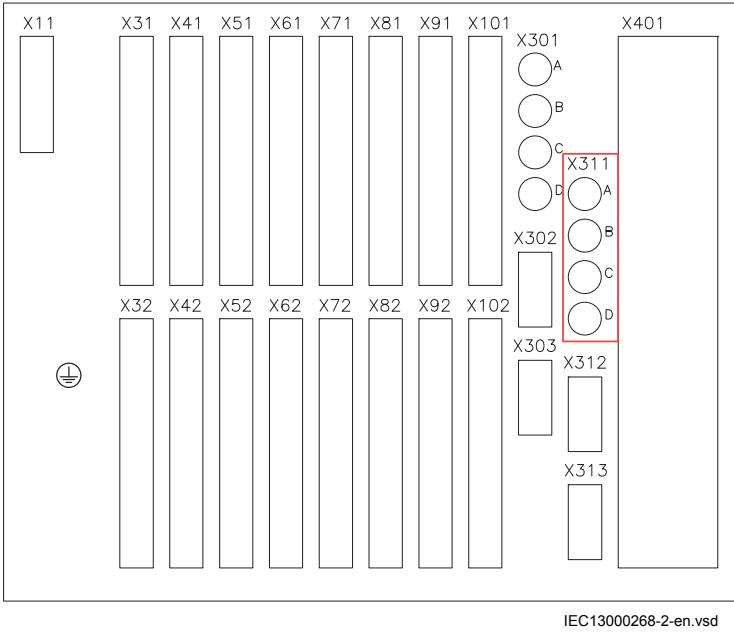


Figure 4: Optical ethernet ports, position X311, rear view

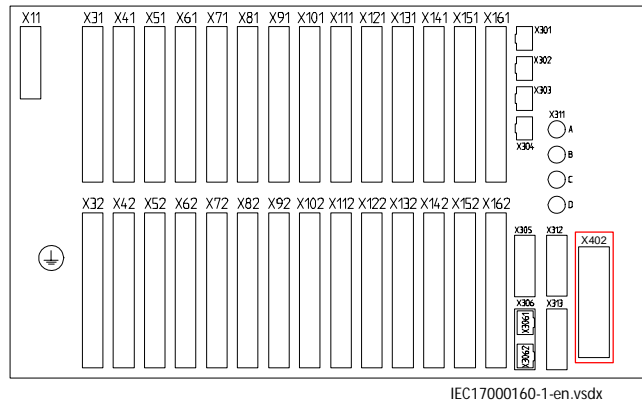


Figure 5: Electrical RJ45 Ethernet port, position X402, rear view

### 3.3 FTP access with TLS, FTPACCS

The FTP Client defaults to the best possible security mode when trying to negotiate with TLS.

The automatic negotiation mode acts on configured port number 21 and server features, it tries to negotiate with explicit TLS via AUTH TLS. If the specified port is any other, it tries to negotiate in a similar way.

Using FTP without TLS encryption gives the FTP client reduced capabilities. This mode is only for accessing disturbance recorder data from the IED.



If normal FTP is required to read out disturbance recordings, create a specific account for this purpose with rights only to do File transfer. The password of this user will be exposed in clear text on the wire.

### 3.4 Encryption algorithms

TLS connections are encrypted with AES 256 if possible or AES 128 as a minimum. At startup a negotiation decides between these two options.

No passwords are stored in clear text within the IED. A hashed representation of the passwords with SHA 256 is stored in the IED. These are not accessible from outside via any ports.



Supported TLS version is TLS 1.0.

### 3.5 Denial of service

The denial of service function is designed to limit the CPU load that can be produced by the Ethernet network traffic on the IED. The communication facilities must not be allowed to compromise the primary functionality of the device. All inbound network traffic is quota controlled, so that a too heavy network load can be controlled. Heavy network load might for instance be the result of malfunctioning equipment connected to the network.

The denial of service functions DOSFRNT, DOSLANAB, DOSLANCD measure the IED load from communication and, if necessary, limits it from jeopardizing the IED's control and protection functionality due to a high CPU load. The function has the following outputs:

- LINKUP indicates the Ethernet link status
- WARNING indicates that the data rate is approaching 3000 frames/s
- ALARM indicates that the IED limits the IP-communication

For more information see related documents in the *Introduction* section in this manual.

## 3.6 Certificate handling

A self-signed certificate is signed by the IED. Certificates use encryption to provide secure communication over the network. Certificate encryption strength depends on the certificate authority (CA). A self-signed X.509 certificate and an RSA key-pair with key-length of 2048 bits will be generated by the IED. The RSA key stored in the certificate is used to establish secure communication.

The certificate is always trusted during communication between the IED and PCM600.

If Windows is configured to use UAC High the certificate have to be manually trusted in a dialog box.



This certificate handling changes with Central Account Management and the possibility to use other certificates but self-signed in the IED.



## Section 4 Local user account management

### 4.1 Authorization

User roles with different user rights are predefined in the IED. It is recommended to use user defined users instead of the predefined built-in users.

The IED users can be created, deleted and edited only with PCM600. One user can belong to one or several user roles. By default, the users in Table 2 are created in the IED, and when creating new users, the predefined roles from Table 3 can be used.



At delivery, the IED user has full access as SuperUser until users are created with PCM600.

Table 2: Default users

| User name     | User rights   |
|---------------|---|
| SuperUser     | Full rights, only presented in LHMI. LHMI is logged on by default until other users are defined                           |
| Guest         | Only read rights, only presented in LHMI. LHMI is logged on by default when other users are defined (same as VIEWER)      |
| Administrator | Full rights. Password: Administrator. This user has to be used when reading out disturbances with third party FTP-client. |

Table 3: Predefined user roles according to IEC 62351-8

| User roles    | Role explanation       | User rights  |
|---------------|------------------------|--|
| VIEWER        | Viewer                 | Can read parameters and browse the menus from LHMI   |
| OPERATOR      | Operator               | Can read parameters and browse the menus as well as perform control actions  |
| ENGINEER      | Engineer               | Can create and load configurations and change settings for the IED and also run commands and manage disturbances   |
| INSTALLER     | Installer              | Can load configurations and change settings for the IED  |
| SECADM        | Security administrator | Can change role assignments and security settings. Can deploy certificates.  |
| SECAUD        | Security auditor       | Can view audit logs  |
| RBACMNT       | RBAC management        | Can change role assignment   |
| ADMINISTRATOR | Administrator rights   | Sum of all rights for SECADM, SECAUD and RBACMNT<br><br><div data-bbox="821 1731 901 1809" data-label="Image"> </div> This User role is vendor specific and not defined in IEC 62351-8 |



Changes in user management settings do **not** cause an IED reboot.



After three consecutive failed login attempts the user will be locked out for ten minutes before a new attempt to login can be performed. This time is settable 10 minutes to 60 minutes.



The PCM600 tool caches the login credentials after successful login for 15 minutes. During that time no more login will be necessary.

Table 4: Authority-related IED functions

| Function                        | Description   |
|---------------------------------|---|
| Authority status<br>ATHSTAT     | This function is an indication function block for user logon activity. User denied attempt to log-on and user successful logon are reported.  |
| Authority check<br>ATHCHCK      | To safeguard the interests of our customers, both the IED and the tools that are accessing the IED are protected, by means of authorization handling. The authorization handling of the IED and the PCM600 is implemented at both access points to the IED: <ul style="list-style-type: none"> <li>local, through the local HMI</li> <li>remote, through the communication ports</li> </ul> <p>The IED users can be created, deleted and edited only in the CAM server.</p> |
| Authority management<br>AUTHMAN | This function enables/disables the maintenance menu. It also controls the maintenance menu log on time out.   |

For more information on Authority management AUTHMAN, Authority status ATHSTAT, and Authority check ATHCHCK functions, see Chapter Basic IED functions in technical manual.

At delivery, the IED has a default user defined with full access rights. PCM600 uses this default user to access the IED. This user is automatically removed in IED when users are defined via the IED Users tool in PCM600.

Default User ID: Administrator

Password: Administrator



It is strongly recommended to define users via the IED Users tool in PCM600.



Only characters A - Z, a - z and 0 - 9 shall be used in user names. User names are not case sensitive. For passwords see the Password policies in PCM600.



## 4.2 Predefined user roles

There are different roles of users that can access or operate different areas of the IED and tool functionalities.



Ensure that the user logged on to the IED has the required access when writing particular data to the IED from PCM600. For more information about setting user access rights, see the PCM600 documentation.

The meaning of the legends used in the table:

- X= Full access rights
- R= Only reading rights
- - = No access rights

Table 5: Predefined user roles according to IEC 62351-8

| Access rights                  | VIEWER | OPERATOR | ENGINEER | INSTALLER | SECADM | SECAUD | RBACMNT | ADMINISTRATOR |
|--------------------------------|--------|----------|----------|-----------|--------|--------|---------|---------------|
| Config – Basic                 | -      | -        | X        | X         | -      | -      | -       | -             |
| Config – Advanced              | -      | -        | X        | X         | -      | -      | -       | -             |
| FileTransfer – Tools           | -      | -        | X        | X         | -      | -      | -       | -             |
| UserAdministration             | -      | -        | -        | -         | X      | -      | X       | X             |
| Setting – Basic                | R      | -        | X        | X         | -      | -      | -       | -             |
| Setting – Advanced             | R      | -        | X        | X         | -      | -      | -       | -             |
| Control – Basic                | -      | X        | X        | -         | -      | -      | -       | -             |
| Control – Advanced             | -      | X        | X        | -         | -      | -      | -       | -             |
| IEDCmd – Basic                 | -      | X        | X        | -         | -      | -      | -       | -             |
| IEDCmd – Advanced              | -      | -        | X        | -         | -      | -      | -       | -             |
| FileTransfer – Limited         | -      | X        | X        | X         | X      | X      | X       | X             |
| DB Access normal               | -      | X        | X        | X         | X      | X      | X       | X             |
| Audit log read                 | -      | -        | -        | -         | -      | X      | -       | X             |
| Setting – Change Setting Group | -      | X        | X        | X         | -      | -      | -       | -             |
| Security Advanced              | -      | -        | -        | -         | -      | X      | -       | X             |

Table 6: Access rights explanation

| Access rights                  | Explanation  |
|--------------------------------|--|
| Config – Basic                 | Configuration – Basic is intended for engineers that only adapt an existing configuration e.g. the I/O-Configuration using SMT                   |
| Config – Advanced              | Configuration – Advanced is intended for engineers that do the whole application engineering and using e.g. ACT                                  |
| FileTransfer – Tools           | FileTransfer – Tools is used for some configuration files for the configuration and shall have the same value as Config – Advanced               |
| UserAdministration             | UserAdministration is used to handle user management e.g. adding new user  |
| Setting – Basic                | Setting – Basic is used for basic settings e.g. control settings and limit supervision   |
| Setting – Advanced             | Setting – Advanced is used for the relay engineer to set settings e.g. for the protection functions  |
| Control – Basic                | Control – Basic is used for a normal operator without possibility to bypass safety functions e.g. interlock or synchro-check bypass              |
| Control – Advanced             | Control – Advanced is used for an operator that is trusted to do process commands that can be dangerous  |
| IEDCmd – Basic                 | IEDCmd – Basic is used for commands to the IED that are not critical e.g. Clear LEDs, manual triggering of disturbances                          |
| IEDCmd – Advanced              | IEDCmd – Advanced is used for commands to the IED that can hide information e.g. Clear disturbance record  |
| FileTransfer – Limited         | FileTransfer - Limited is used for access to disturbance files e.g. through FTP  |
| DB Access normal               | Database access for normal user. This is needed for all users that access data from PCM  |
| Audit log read                 | Audit log read allows reading the audit log from the IED   |
| Setting – Change Setting Group | Setting – Change Setting Group is separated to be able to include the possibility to change the setting group without changing any other setting |
| Security Advanced              | Security Advanced is the privilege required to do some of the more advanced security-related settings  |

IED users can be created, deleted and edited only with the IED Users tool within PCM600. From the LHMI, no users can be created nor changed.



First user created must be appointed the role SECADM to be able to write users, created in PCM600, to the IED.



In order to allow the IED to communicate with PCM600 when users are defined via the IED Users tool, the access rights “UserAdministration” and “FileTransfer — Limited” must be applied to at least one user.



“DB Access normal” and “File Transfer — Limited” are required for PCM600 access to the IED.

## 4.3 Password policies

Only ASCII characters are allowed when typing username or password. Currently passwords in the range 32-126 and 192-383 (ASCII ranges, decimal) are supported.

Password policies are set in the IED Users tool in PCM600. There are several options for forcing the password safer.

- Minimum length of password (1 - 18)
- Require lowercase letters ( a - z )
- Require uppercase letters ( A - Z )
- Require numeric letters ( 0 - 9 )
- Require special characters ( !@#+"\*%&/=? )
- Password expiry time (default 90 days)



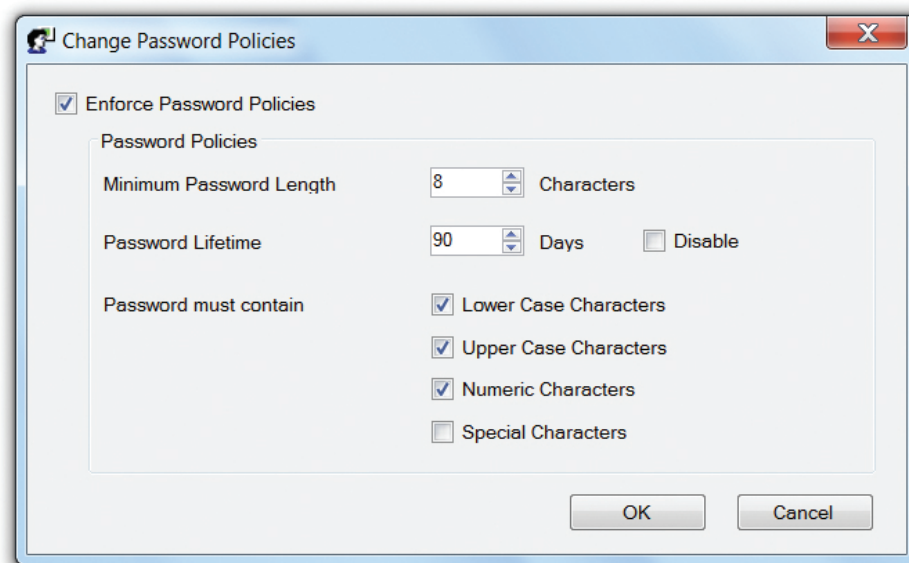
To achieve IEEE 1686 conformity, a password with a minimum length of 8 characters must be used, and the square Enforce Password Policies shall be ticked.



After password expiry the user is still able to login, but a warning dialog will be displayed on the Local HMI. Also a security event will be issued.



Figure 6: Password expiry warning dialog



IEC13000027-2-en.psd

Figure 7: Change Password Policies dialog box in IED Users tool in PCM600

## 4.4 IED User management

The IED Users tool in PCM600 is used for editing user profiles and role assignments.

In the IED Users tool, the data can be retrieved from an IED or data can be written to an IED if permitted. The data from an IED can be saved to the project database.



Always use **Read User Management Settings from IED** before making any changes when managing user profiles. If this is not done password changes made by users may be lost!



Nothing is changed in the IED until a “writing-to-IED operation” is performed.

### 4.4.1 Starting IED user management

- Connect the PC to the IED
- Start PCM600
- Select an IED in the plant structure
- Select **Tools/IED Users** or,
- Right-click an IED in the plant structure and select **IED Users**  
The IED User dialog box appears.

### 4.4.2 General settings

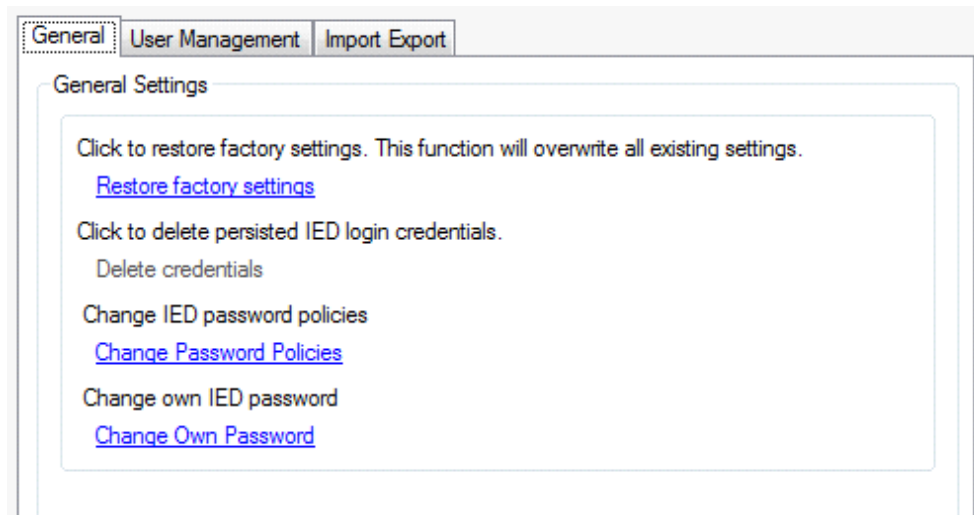
In the **General** tab, by clicking **Restore factory settings** the default users can be restored in the IED Users tool. For the IED series this means reverting back to the factory delivered users. Performing this operation does not remove the users in the IED. Nothing is changed in the IED until a “writing-to-IED operation” is performed.



This is **not** the same action as **Revert to IED defaults** in the recovery menu.

The previous administrator user ID and password have to be given so that the writing toward the IED can be done.

Editing can be continued by clicking on **Restore factory settings** when not connected to the IED.



IEC13000017-2-en.vsd

Figure 8: General tab

### 4.4.3 User profile management

In the **User Management** tab, the user profiles of the selected IED can be edited. New users can be created, existing users can be deleted and different user group members can be edited.



A user profile must always belong to at least one user group.

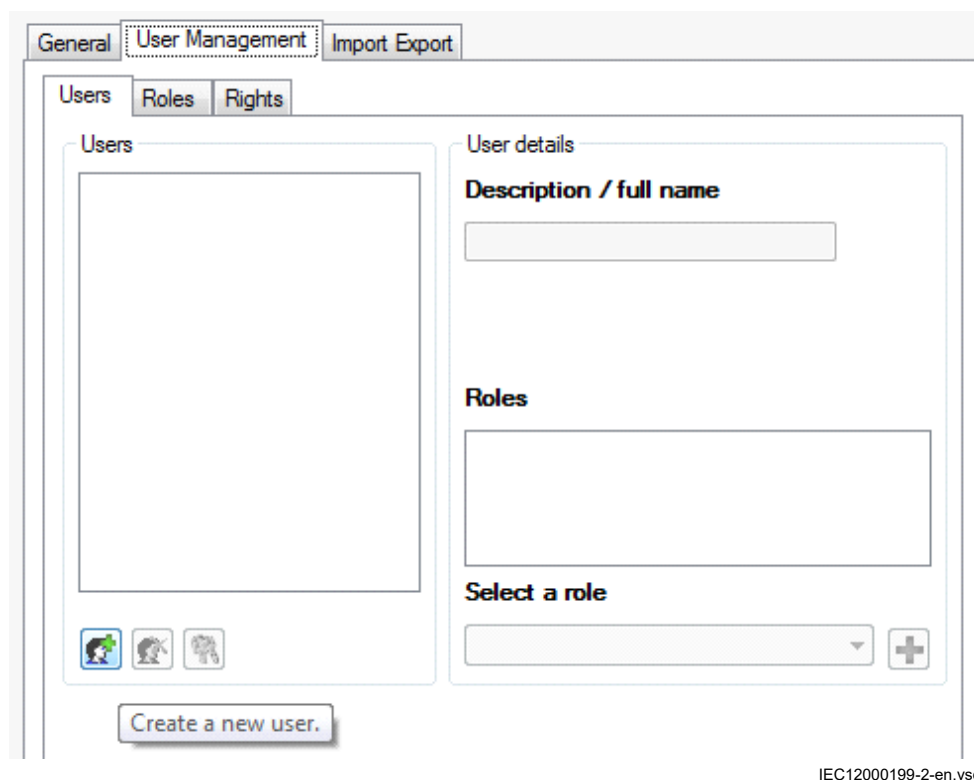
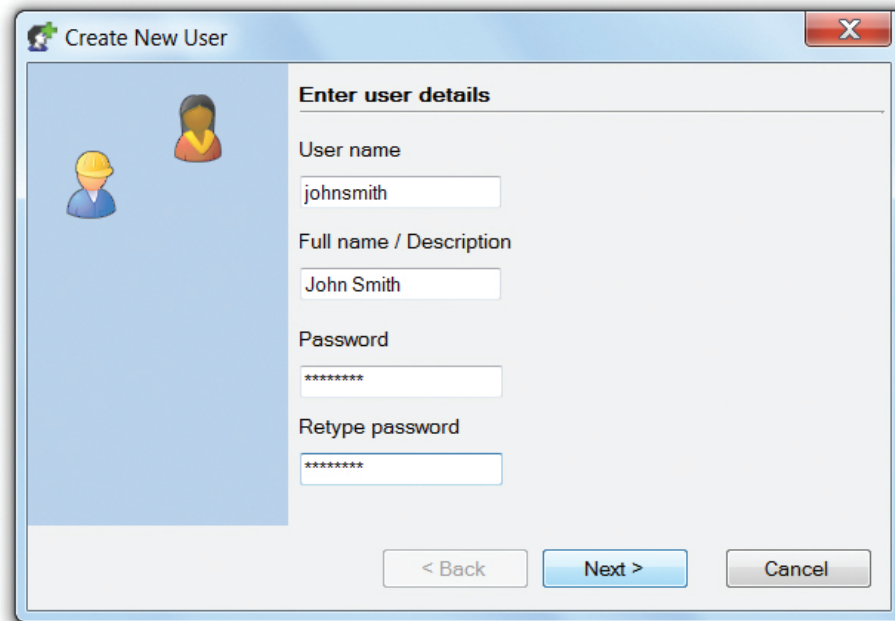


Figure 9: Create new user

#### 4.4.3.1 Adding new users

1. Click  in the **Users** tab to open the wizard.



The 'Create New User' dialog box is shown with the 'Enter user details' tab selected. On the left, there are two user icons: a male worker in a blue shirt and yellow hard hat, and a female worker in a red shirt. The right side contains the following fields:

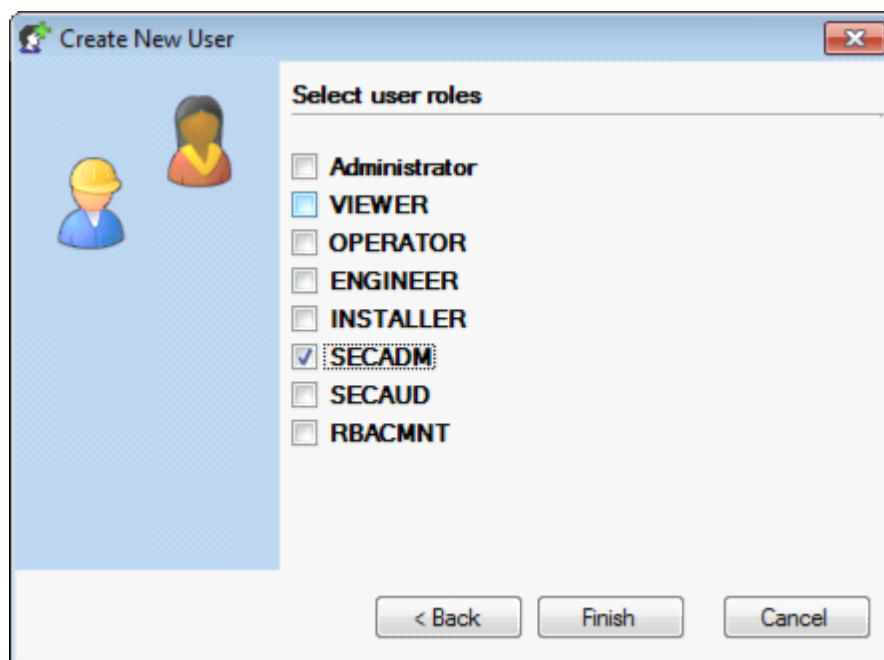
- User name:** johnsmith
- Full name / Description:** John Smith
- Password:** \*\*\*\*\*
- Retype password:** \*\*\*\*\*

At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

IEC12000200-2-en.psd

Figure 10: Create new user

- Follow the instructions in the wizard to define a user name, password and user role. Select at least one user role where the defined user belongs. The user profile can be seen in the **User details** field.



The 'Create New User' dialog box is shown with the 'Select user roles' tab selected. On the left, the same two user icons are present. The right side contains a list of roles with checkboxes:

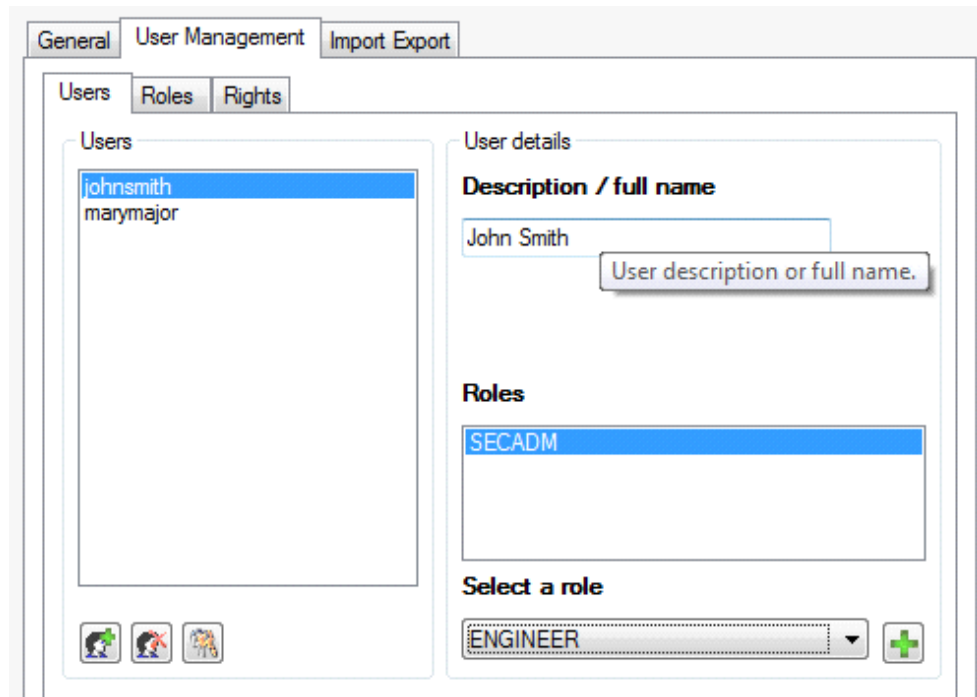
- ☐ Administrator
- ☐ VIEWER
- ☐ OPERATOR
- ☐ ENGINEER
- ☐ INSTALLER
- ☒ SECADM
- ☐ SECAUD
- ☐ RBACMNT

At the bottom right, there are three buttons: '< Back', 'Finish', and 'Cancel'.

IEC12000201-3-en.vsd

Figure 11: Select user role


- Select the user from the user list and type a new name or description in the **Description/ full name** field to change the name or description of the user.



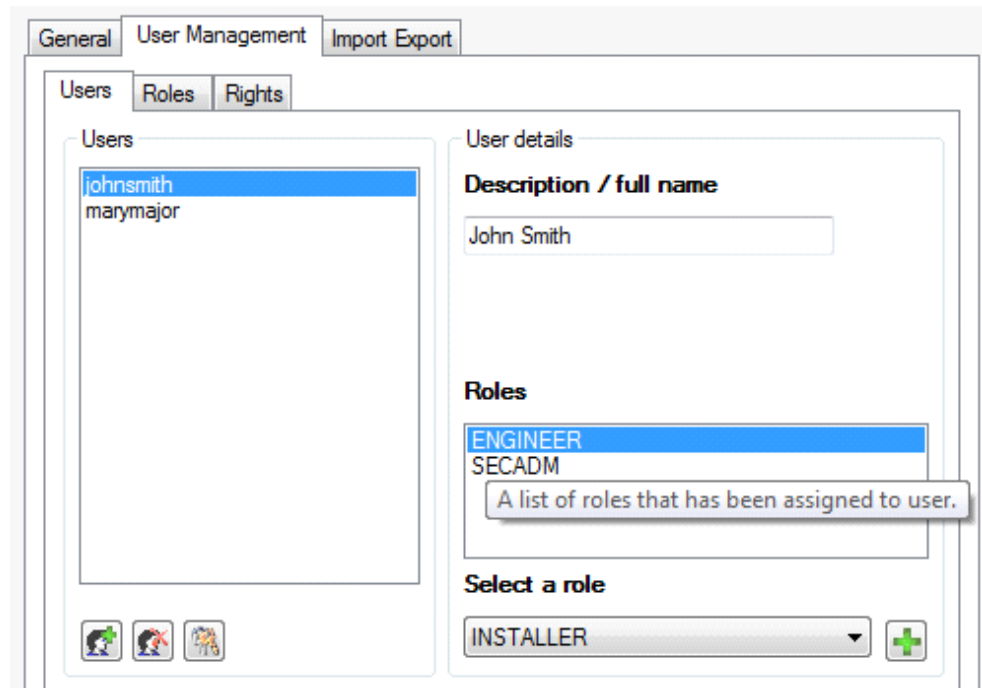
IEC12000202-2-en.vsd

Figure 12: Enter description

#### 4.4.3.2 Adding users to new user roles

1. Select the user from the **Users** list.
  2. Select the new role from the **Select a role** list.
  3. Click .
- Information about the roles to which the user belongs to can be seen in the **User details** area.



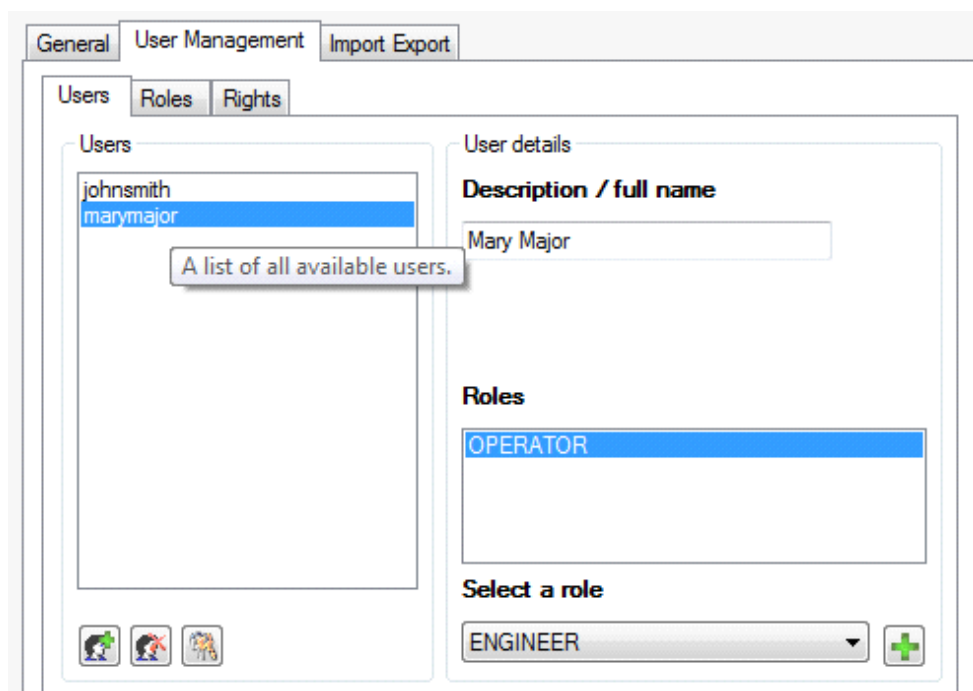


IEC12000203-2-en.vsd

*Figure 13: Adding user*

#### 4.4.3.3 Deleting existing users

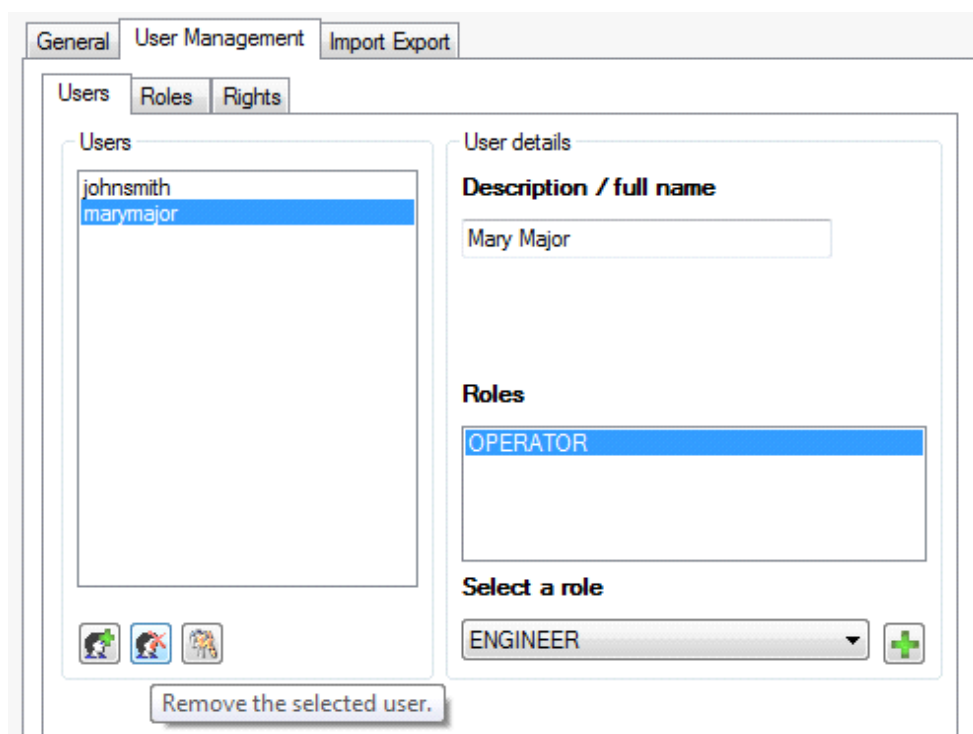
1. Select the user from the **Users** list.



IEC12000204-2-en.vsd

Figure 14: Select user to be deleted

2. Click .

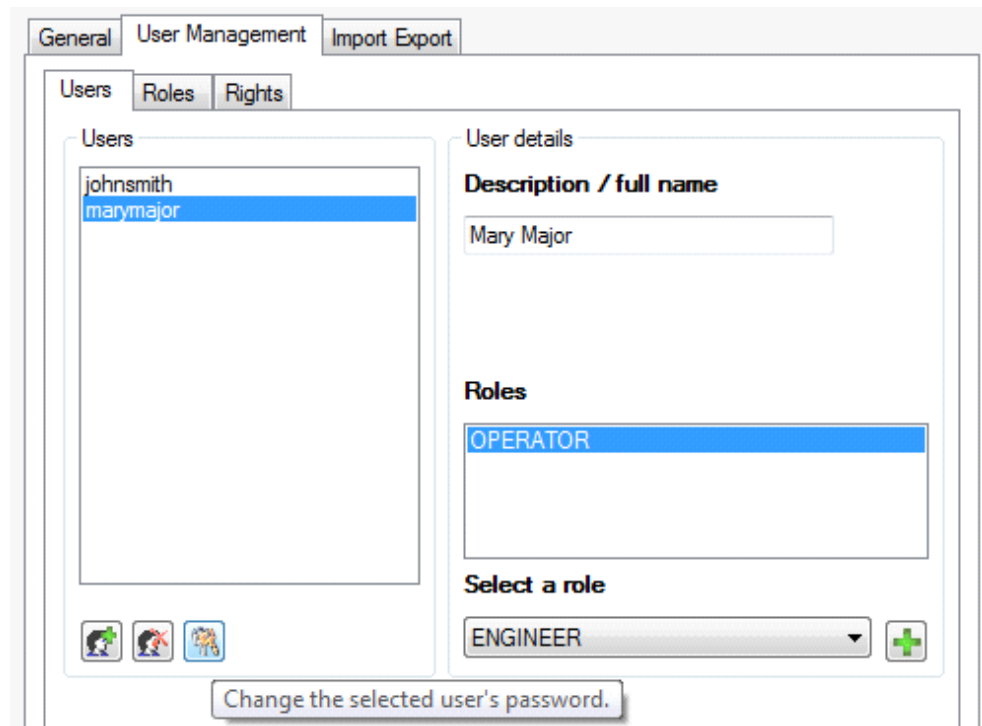


IEC12000205-2-en.vsd

Figure 15: Delete existing user


#### 4.4.3.4 Changing password

1. Select the user from the **Users** list.



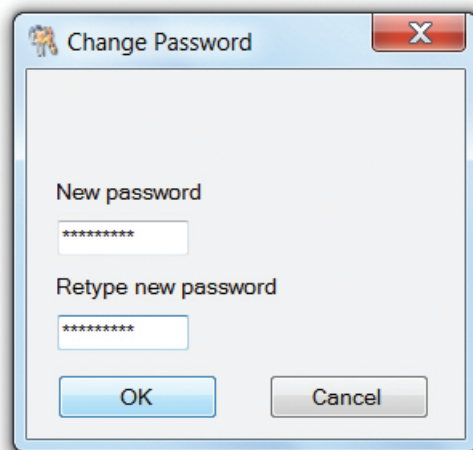
IEC12000206-2-en.vsd

Figure 16: Select user

2. Click .
3. Type the old password once and the new password twice in the required fields. The passwords can be saved in the project database or sent directly to the IED.



No passwords are stored in clear text within the IED. A hash representation of the passwords is stored in the IED and it is not accessible from outside via any ports.

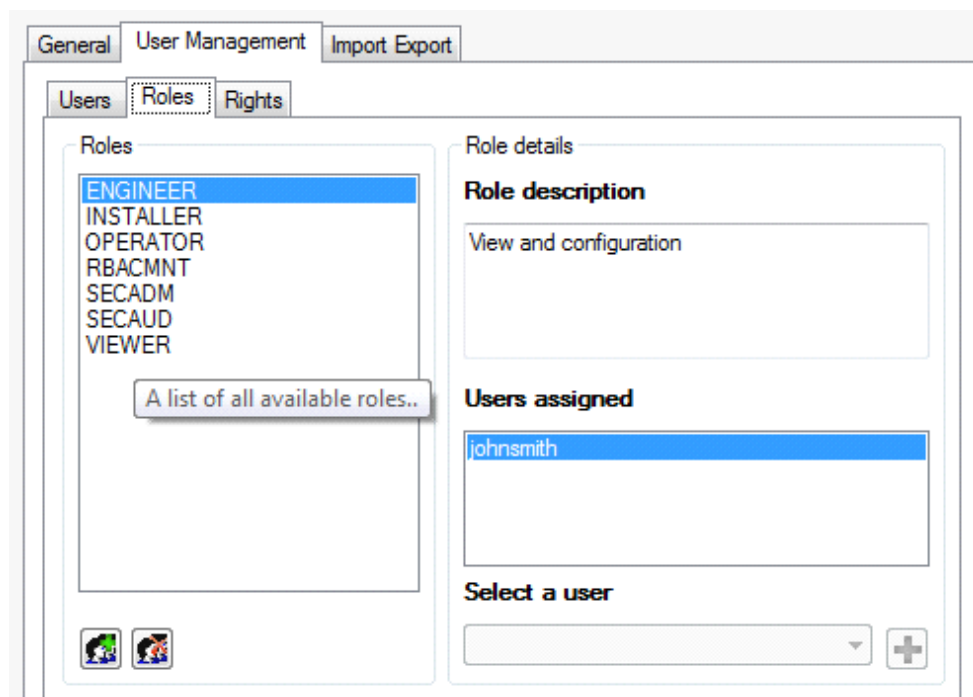


IEC12000207-2-en.psd

Figure 17: Change password

## 4.4.4 User role management


In the **Roles** tab, the user roles can be modified. The user's memberships to specific roles can be modified with a list of available user roles and users.



IEC12000208-2-en.vsd

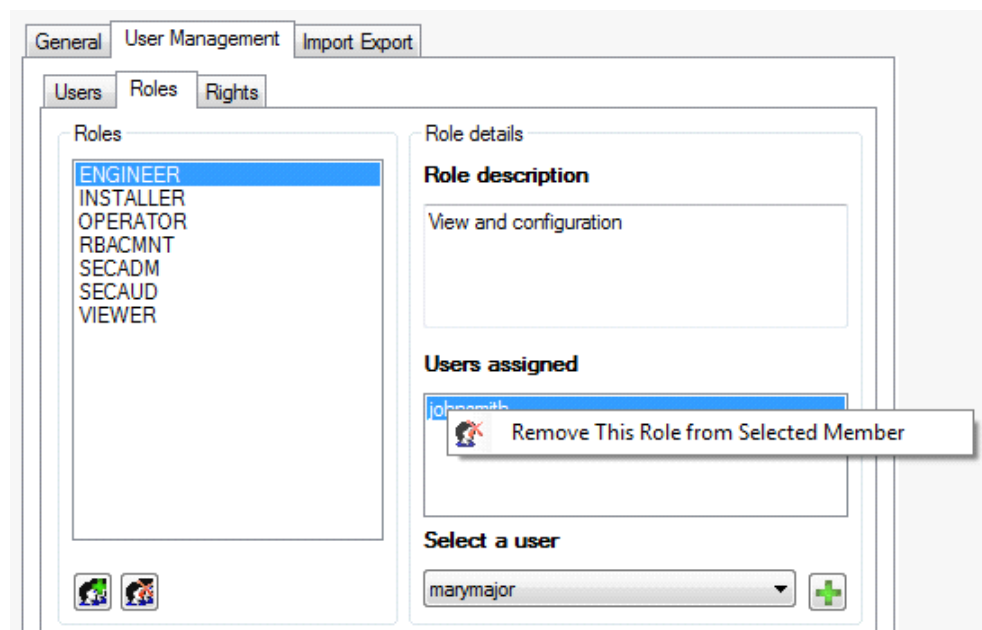
Figure 18: Editing users

### 4.4.4.1 Adding new users to user roles

1. Select the required role from the **Roles** list.  
The role profile can be seen under the **Role details** field.
2. Select the new user from the **Select a user** list.
3. Click .  
The new user is shown in the **Users assigned** list.

#### 4.4.4.2 Deleting existing User from user roles

1. Right-click the user in the **Users assigned** list.
2. Select **Remove This Role from Selected Member**.



IEC12000210-2-en.vsd

Figure 19: Remove Role from User

#### 4.4.4.3 Reusing user accounts

IED user account data can be exported from one IED and imported to another. The data is stored in an encrypted file.

Exported passwords are hashed and not in clear text.

To export IED user account data from an IED

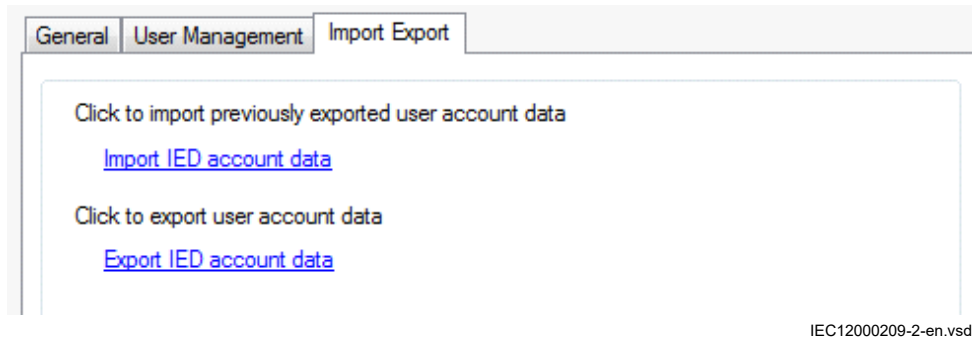
1. Click the **Import Export** tab in the IED User tool in PCM600.
2. Click **Export IED account data**.

The user account data is exported to a file with user defined filename and location.

Import IED user rights to an IED

1. Click **Import IED account data**.
2. Open the previously exported file.

Only users who have the right to change the user account data in PCM600 are allowed to export and import.

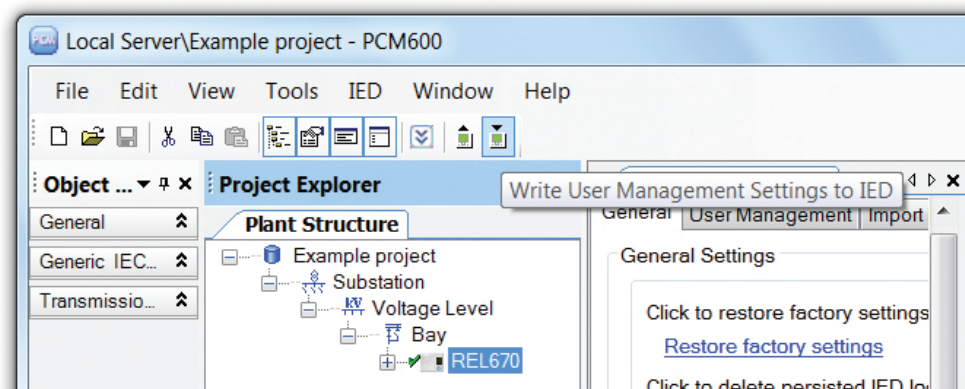


IEC12000209-2-en.vsd

Figure 20: Importing and exporting user account data

#### 4.4.5 Writing user management settings to the IED

- Click the **Write User Management Settings to IED** button on the toolbar.



IEC12000211-2-en.psd

Figure 21: Write to IED



The data is saved when writing to the IED starts.

#### 4.4.6 Reading user management settings from the IED

- Click the **Read User Management Settings from IED** button on the toolbar.

#### 4.4.7 Saving user management settings

- Select **File/Save** from the menu.
- Click the **Save** toolbar button.



The save function is enabled only if the data has changed.





## Section 5 Central Account Management

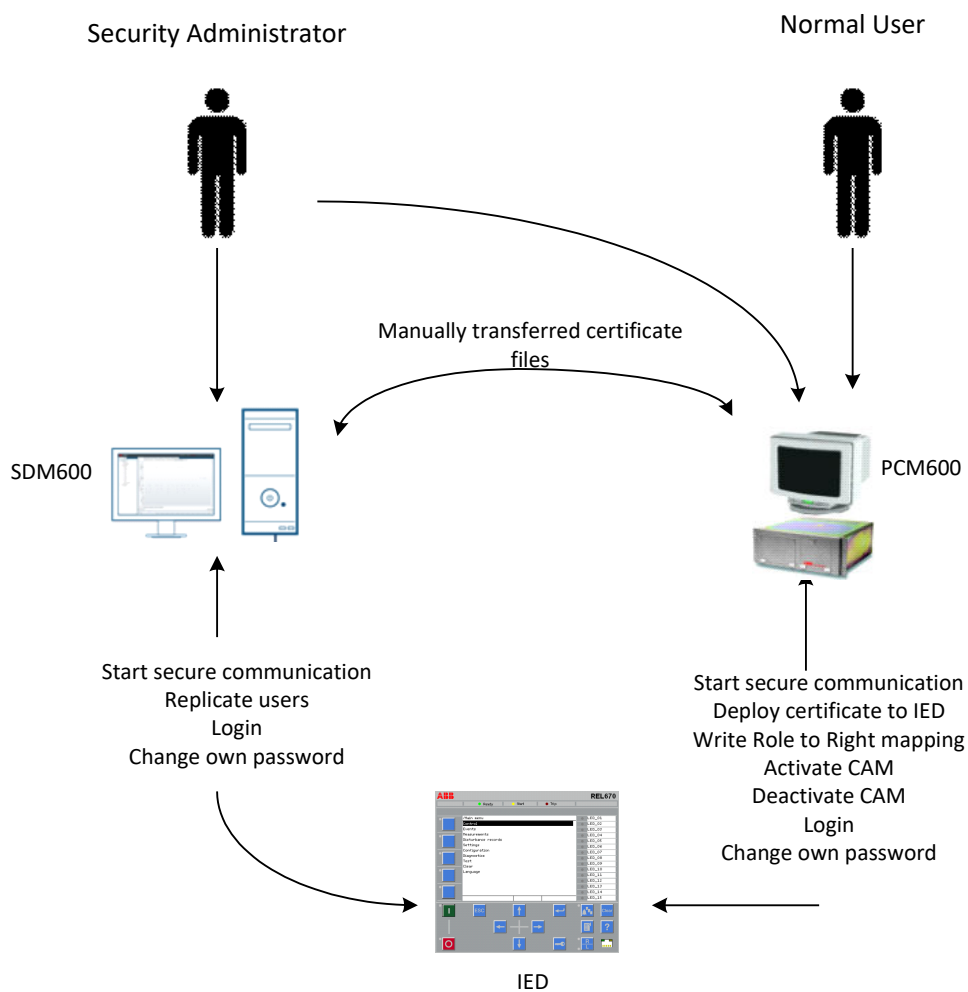
### 5.1 Introduction

Central Account Management is an authentication infrastructure that offers a secure solution for enforcing access control to IEDs and other systems within a substation. This incorporates management of user accounts, roles and certificates and the distribution of such, a procedure completely transparent to the user.



In this manual the LDAP server software description and handling is based on SDM600, which is an ABB product. Other Central Account Management software can be used, provided it has sufficient functionality.

### 5.2 Certificate management



IEC15000368-1-en.vsd

Figure 22: Overview of the functionality between the products in the system.

Before any distribution of users and roles can take place, a trust relation must be established. The CAM server, such as the SDM600, also acts as a CA meaning that it is able to issue digital certificates. Each device, such as an IED, will have its own unique device certificate, one which must be imported into the PCM600 configuration and then written to the IED. At this point trust is automatically established directly between the CAM server and the IED. The Security Administrator is responsible for this setup.

## 5.2.1 Creating IED certificates

As mention above, SDM600 can be used to create IED certificates. Below follows a short guide on how to create device certificates.

1. In PCM600, export the Substation Configuration Description (SCD).

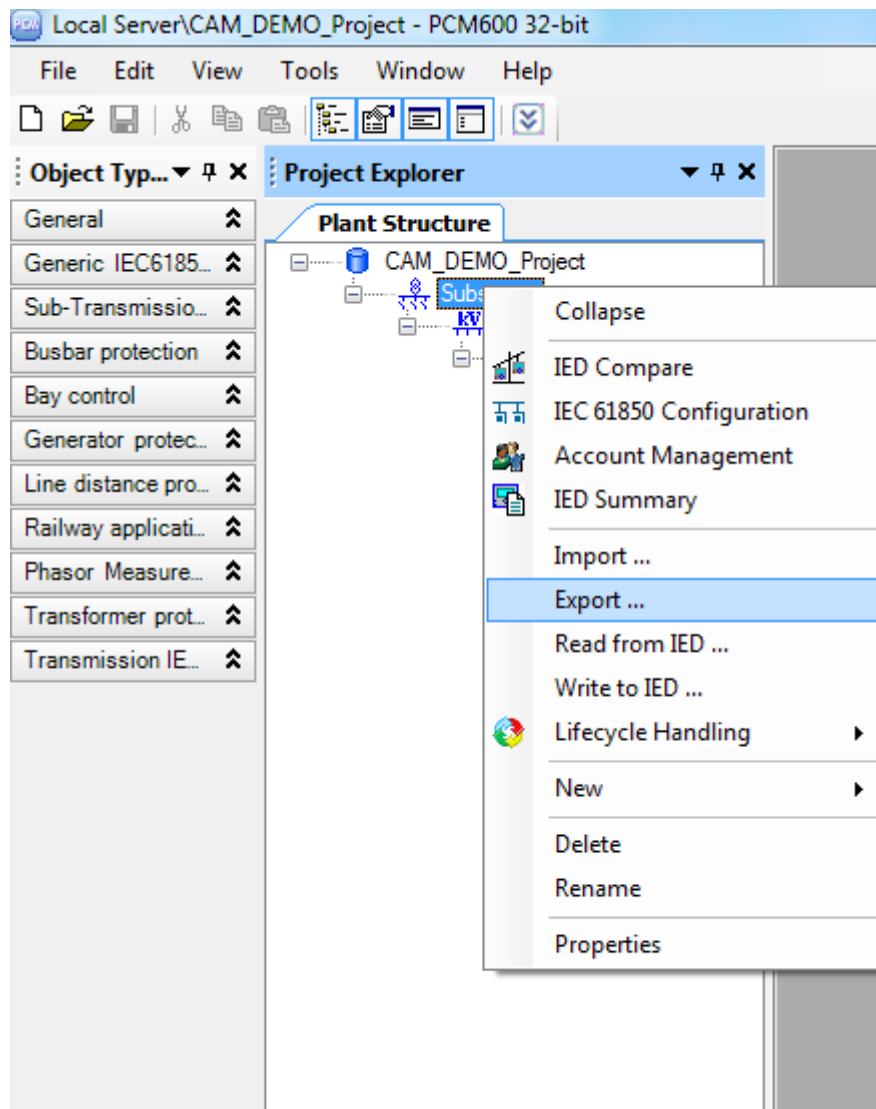


Figure 23: Export SCD file

Generate the SCD file from PCM600

2. In SDM600, import SCD via the Load Structure tool. Refer to **Setting Up the SDM600 Structure** in the SDM600 User Manual.
3. Update "Alternative IP Addresses" with all configured interfaces on the device.

4. Generate certificates in the Central Account Management server for all IEDs
5. Export the certificate or the configuration package from the Central Account Management server.
6. Use PCM600 to load the certificate and configuration into the correct IED



IED deploys only certificates bundled in a PKCS#12 file format.

SDM600 allows user to set key length of the certificates that needs to be deployed in IED. While it may be prudent to use a larger key size, it would also mean it requires a considerable longer time for the TLS handshake (between IED and tools/ Central Account Management servers) before any secure communication starts. We recommend to deploy certificates with key length of 2048 in the IED. NSA (National Security Agency) recommendation is that RSA keys of 2048 bit key size is acceptable.



IED will use the certificate imported via PCM600 to automatically access to the SDM600 server. This certificate is also used as a server certificate to secure communication of FTP and ODBC protocols. However, it is possible to deploy server certificates (External) for FTP and ODBC protocol. PCM600 does not support this feature.

The security administrator uses a 3rd party FTP client to transfer the pkcs#12 package to **certificates/import/external** and use the SITE cmd "PKCS12Install <path to file> <KEK>" to activate the external certificate

## 5.2.2 Importing and writing certificates to an IED

The following are the steps to import and write certificates to the IED.

1. Connect PC to the IED.
  2. Start PCM600, open project.
  3. Select **VoltageLevel**, **Bay** or **IED** in the plant structure.
  4. Select **Tools/Account Management** or right click on **VoltageLevel**, **Bay** or **IED** in the plant structure and select **Account Management**
- The Account Management dialog will appear as shown below

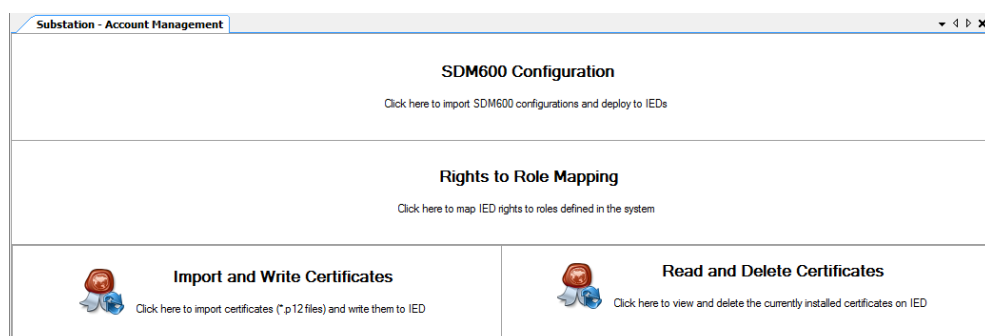


Figure 24: Account Management Tool in PCM

5. Select the **Import and Write Certificates** option.
6. Select those IEDs to which certificates needs to be written.

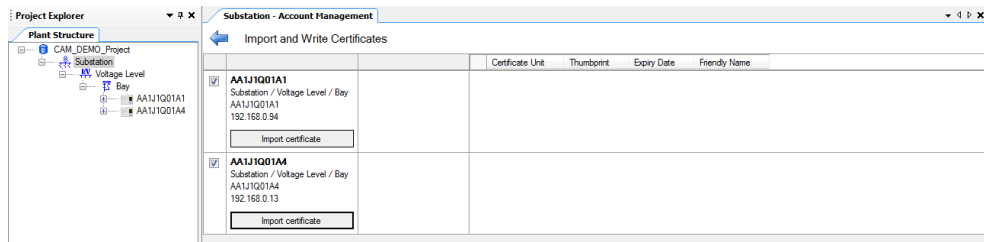


Figure 25: Import and Write certificates tool view in PCM600

7. Select ☒ **Enabled** for those IEDs to which certificates needs to be written
8. Click on **Import certificate** button.

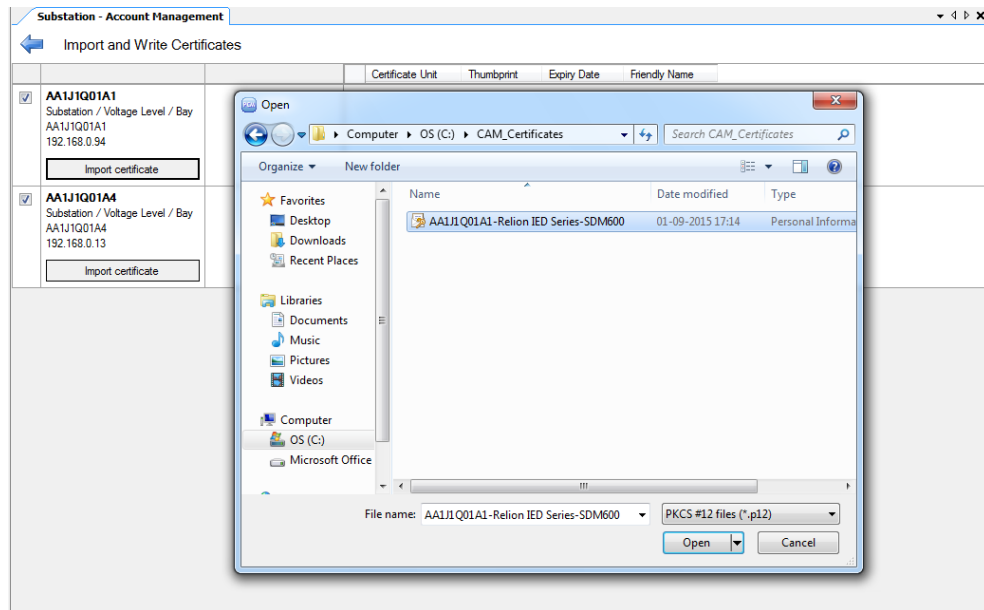


Figure 26: Importing certificate (p12) file

9. If certificate is password protected the user will be prompted to enter the password.
  - 9.1. Select **CAM** as the **Certificate Unit**.
  - 9.2. Click the **OK** button.

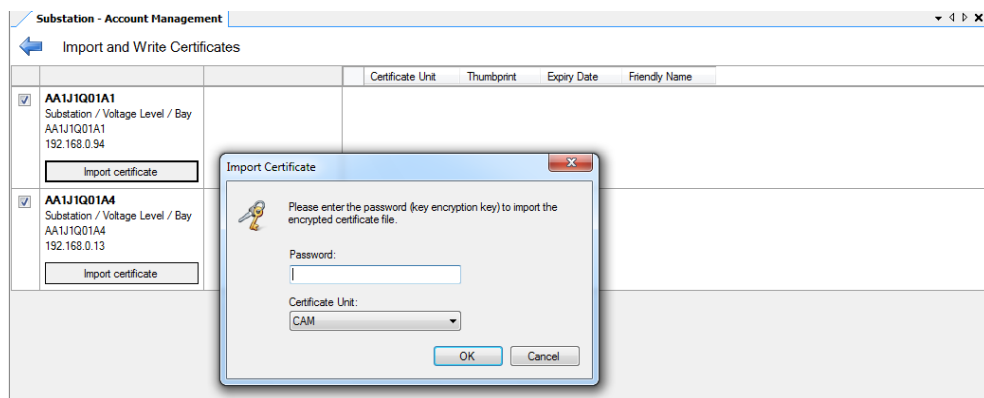


Figure 27: Entering password of a certificate



Only CAM certificates can be written from PCM600 to IED.

#### 10. Select certificate

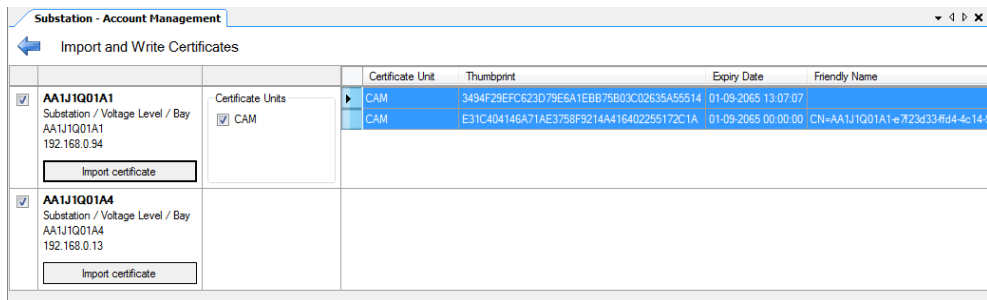

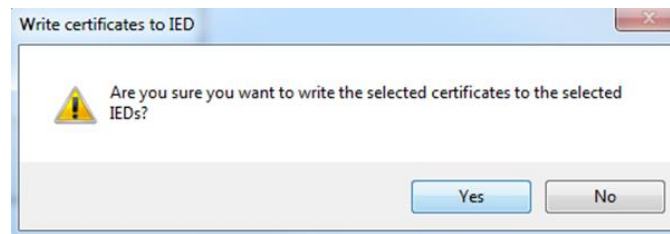


Figure 28: Chosen certificate

11. Click  button to write certificate(s) for the enabled IEDs and click **Yes** in the confirmation dialog



IEC15000352.vsdX

Figure 29: Write certificate confirmation dialog

12. The process and the status of the writing is indicated in the **Account Management** tab.

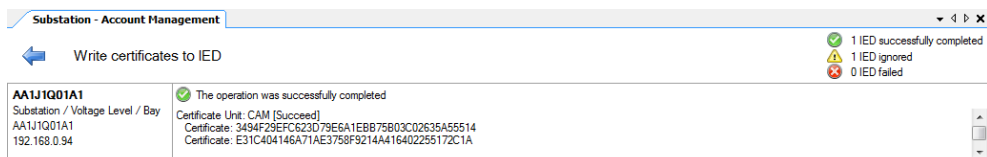


Figure 30: Result of written certificates



When Central Account Management is enabled in IED, and if user deploys an invalid certificate in to an IED (e.g.: SDM600 certificate of another SDM server, than the one that is configured in the IED), then replication will fail at the time when IED tries to replicate. However, Central Account Management still remains to be enabled in the IED.

In this situation, IED will fall back to replica users if Replication is enabled. Then, the certificates can be re-deployed if the SECADM is part of the replicated users. Otherwise, Central Account Management should be deactivated through Maintenance menu, "Disable CAM and Delete Certificates" option.



In the case that Replication is disabled in the IED, the IED will be locked out and the only way to get out of this situation is through Maintenance menu, "Disable CAM and Delete Certificates" option.

## 5.2.3 Reading certificates from an IED

The following are the steps to read certificates from an IED:

1. Connect PC to the IED
2. Start PCM600, open project
3. Select **Voltage Level** or **Bay** or **IED** in the plant structure.
4. Select **Tools/Account Management** or
5. Right click on **Voltage Level** or **Bay** or **IED** in the plant structure and select **Account Management**

The Account Management dialog will appear as shown below.

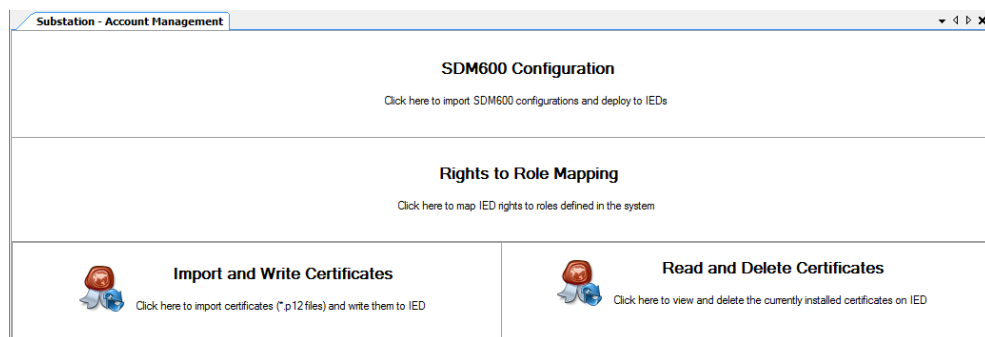


Figure 31: Account Management Tool in PCM

6. Select the **Read and Delete Certificates** option.

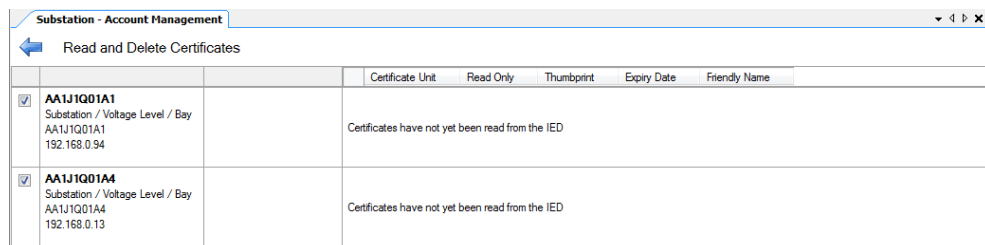



Figure 32: Read and Delete Certificates view in PCM600

7. Select ☒ **Enabled** for those IEDs from which certificates needs to be read.
8. Click  button to read certificates from the IED

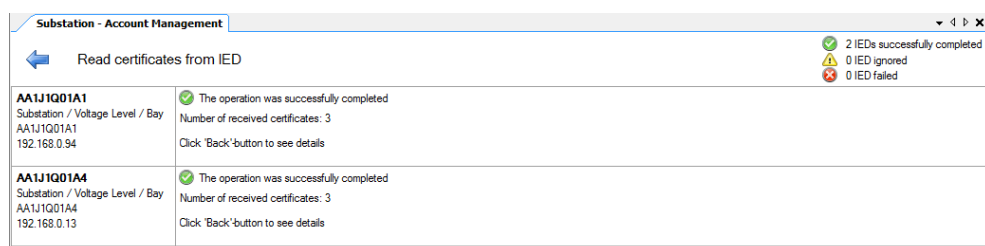


Figure 33: Reading certificates from IED

9.

Click the  button to view certificates that are read from the IED.

| Substation - Account Management  |   |                  |           |  |                     |
|--|---|------------------|-----------|--|---------------------|
| Read and Delete Certificates   |   |                  |           |  |                     |
|  |   | Certificate Unit | Read Only | Thumbprint                               | Expiry Date         |
| <input checked="" type="checkbox"/> AA1J1Q01A1<br>Substation / Voltage Level / Bay<br>AA1J1Q01A1<br>192.168.0.94 | Certificate Units<br><input type="checkbox"/> Internal<br><input checked="" type="checkbox"/> CAM | Internal         | Yes       | C5F9E487C2D104BC4072E67886C1E2B06C683A95 | 14-10-2065 14:54:34 |
|  |   | CAM              | No        | 3494F29EFC623D79E6A1EBB75B03C02635A55514 | 01-09-2065 13:07:07 |
|  |   | CAM              | No        | E31C404146A71AE3758F9214A416402255172C1A | 01-09-2065 00:00:00 |
| <input checked="" type="checkbox"/> AA1J1Q01A4<br>Substation / Voltage Level / Bay<br>AA1J1Q01A4<br>192.168.0.13 | Certificate Units<br><input type="checkbox"/> Internal<br><input checked="" type="checkbox"/> CAM | Internal         | Yes       | D80709DE4C215E0FF3CB5A20160E5D65FE9F8C   | 15-11-2065 19:50:27 |
|  |   | CAM              | No        | DF920DE72A912B502D5B572E9D87B0F593089084 | 08-10-2065 12:00:38 |
|  |   | CAM              | No        | 0C976EF7A56E47918876C3353BAE00A940122D8F | 08-10-2065 00:00:00 |

Figure 34: Certificates that are read from the IED

10. Double click on a **Certificate Unit** to view the details of it or
11. Right click on a **Certificate Unit** and select **Properties**

|   | Certificate Unit | Read Only | Thumbprint                               | Expiry Date         |
|---|------------------|-----------|--|---------------------|
| ▶ | Internal         | Yes       | C5F9E487C2D104BC4072E67886C1E2B06C683A95 | 14-10-2065 14:54:34 |
|   | CAM              | No        | 3494F29EFC623D79E6A1EBB75B03C02635A55514 | 01-09-2065 13:07:07 |
|   | CAM              | No        | E31C404146A71AE3758F9214A416402255172C1A | 01-09-2065 00:00:00 |

Substation - Account Management

Read and Delete Certificates

|  | Certificate Unit  | Read Only | Thumbprint | Expiry Date                              | Friendly Name       |
|--|---|-----------|------------|--|---------------------|
| <input checked="" type="checkbox"/> AA1J1Q01A1<br>Substation / Voltage Level / Bay<br>AA1J1Q01A1<br>192.168.0.94 | Certificate Units<br><input type="checkbox"/> Internal<br><input checked="" type="checkbox"/> CAM | Internal  | Yes        | C5F9E487C2D104BC4072E67886C1E2B06C683A95 | 14-10-2065 14:54:34 |
|  |   | CAM       | No         | 3494F29EFC623D79E6A1EBB75B03C02635A55514 | 01-09-2065 13:07:07 |
|  |   | CAM       | No         | E31C404146A71AE3758F9214A416402255172C1A | 01-09-2065 00:00:00 |
| <input checked="" type="checkbox"/> AA1J1Q01A4<br>Substation / Voltage Level / Bay<br>AA1J1Q01A4<br>192.168.0.13 | Certificate Units<br><input type="checkbox"/> Internal<br><input checked="" type="checkbox"/> CAM | Internal  | Yes        | D80709DE4C215E0FF3CB5A20160E5D65FE9F8C   | 15-11-2065 19:50:27 |
|  |   | CAM       | No         | DF920DE72A912B502D5B572E9D87B0F593089084 | 08-10-2065 12:00:38 |
|  |   | CAM       | No         | 0C976EF7A56E47918876C3353BAE00A940122D8F | 08-10-2065 00:00:00 |

**Certificate**

General Details Certification Path

**Certificate Information**

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: AA1J1Q01A1

Issued by: AA1J1Q01A1

Valid from 13- 10- 2015 to 14- 10- 2065

Install Certificate... Issuer Statement

Learn more about [certificates](#)

OK

Figure 35: Viewing details of certificate of an IED in PCM600

## 5.2.4 Certificate information on local HMI

Information about the currently installed certificates can be found in the local HMI by traversing the menu tree by using the arrow keys. **Main menu/Diagnostics/Communication**

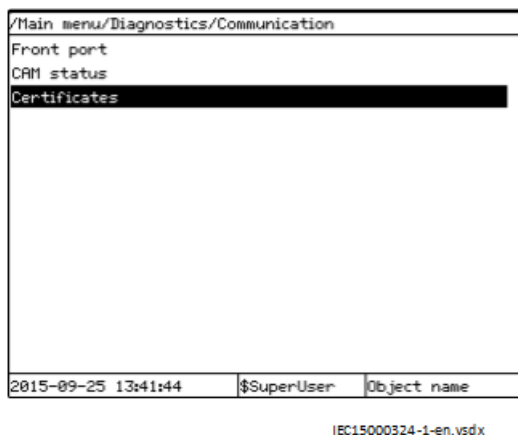



Figure 36: Certificates view

In the Certificates view certificate information is grouped according to usage. Selecting CAM and pressing  will show information about the certificates used for Central Account Management.

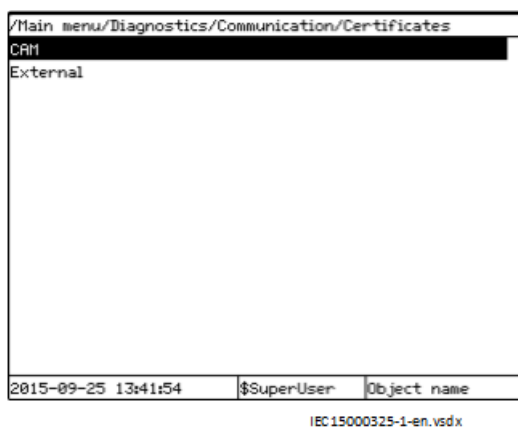


Figure 37: Certificate information for CAM certificates

Only the categories with installed certificates are shown. If no external or CAM certificates are installed then a category named internal is shown which lists the certificates generated by the device.

In figure 38 two certificates are shown for the selected usage.

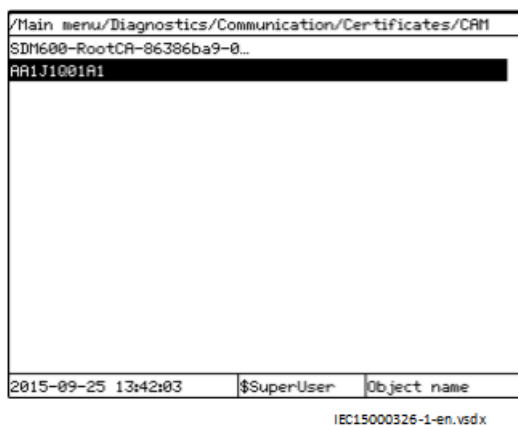




Figure 38: CAM certificates



By pressing  on a menu item without information in the right field more information will be shown. For instance, by pressing  in the **Issued to** menu item shown in figure 39 below, more information will be shown as in figure 40 below.

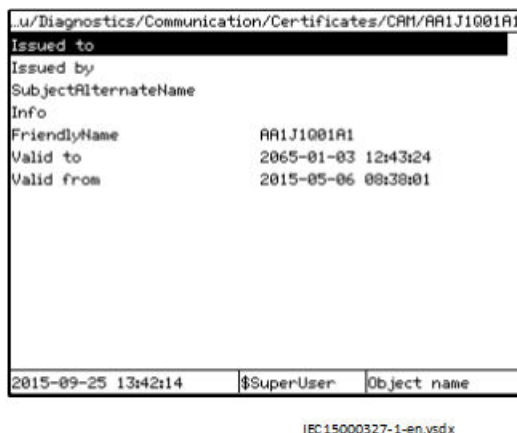


Figure 39: Detailed certificate information

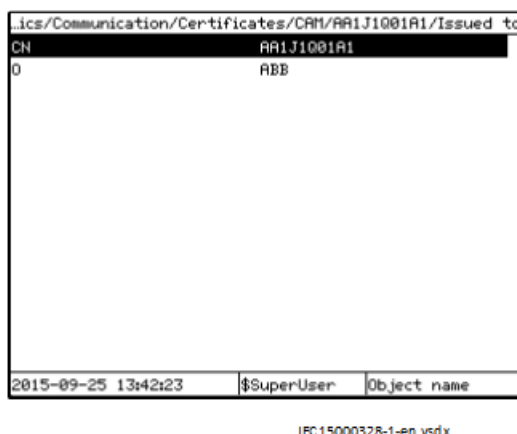


Figure 40: Certificate issued to

## 5.2.5 Invalid certificates

The certificate can be invalid for different reasons, e.g. if the certificate has expired. In this case, if the IED is using a self-signed certificate, it will generate a new self signed certificate. Otherwise, when IED is using a certificate generated by SDM600, it is required that the security administrator generates new certificates and re-deploy them using PCM600. If the certificate has expired, PCM600 will issue a warning to the user about connecting to a device with expired certificate. SDM600 will reject user authentication with expired certificate.

If the replication is enabled and server rejects the authentication (due to expired certificate) then the user is allowed to login using the replicated data. IED will raise a security event 30 days before the certificate will expire and continue till the expiry date once every day.

There are two main cases when the IED access the server:

1. When a cyclic replication is done
2. When a user should be authenticated or change the password

These two cases are different in that sense that one has an ongoing user interaction, while the other occurs cyclically without user interaction.

In both cases a security event will be generated in the IED. If user interaction is involved, a generic connection problem message will be presented.

## 5.2.6 Deleting certificates from an IED



Deletion of certificates from IED is possible only after reading certificates from IED.

1. Select the Certificate Units that needs to be deleted.

|  | Certificate Unit | Read Only | Thumbprint                               | Expiry Date         | Friendly Name  |
|--|------------------|-----------|--|---------------------|----------------|
| AA1J1Q01A1<br>Substation / Voltage Level / Bay<br>AA1J1Q01A1<br>192.168.0.94 | Internal         | Yes       | CF9F497CDD1D46C4072E67898C1E260C83495    | 14-10-2065 14:54:38 | AA1J1Q01A1_SRV |
|  | CAM              | No        | 3494F29EFC623079E6A1EBB75803C02635A55514 | 01-09-2065 13:07:07 | AA1J1Q01A1-e7  |
| AA1J1Q01A4<br>Substation / Voltage Level / Bay<br>AA1J1Q01A4<br>192.168.0.13 | Internal         | Yes       | 0807D5D5E4C215E0FF63B504201B8E5C8F6E5F8C | 15-11-2065 19:50:22 | AA1J1Q01A4_SRV |
|  | CAM              | No        | DF32DDE72A912B502D5B572E9087B0F593089084 | 08-10-2065 12:00:38 | AA1J1Q01A4-ca  |

2. Click on the delete-button in the toolbar.



IEC15000343-1-en.vsdX

A confirmation dialog appears

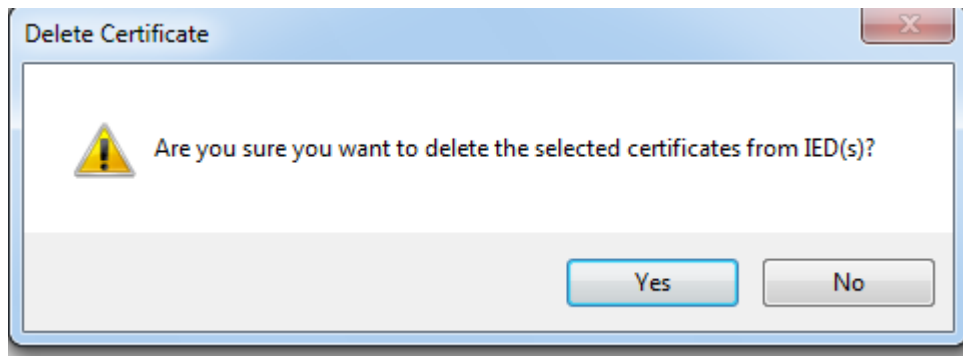


Figure 41: Certificate deletion confirmation dialog

3. Click on the **Yes** button to confirm the deletion.

The certificates are deleted from the IED, confirmation of this can be seen in the tool.

|  | Certificate Unit                                 | Read Only | Thumbprint | Expiry Date | Friendly Name |
|--|--|-----------|------------|-------------|---------------|
| AA1J1Q01A1<br>Substation / Voltage Level / Bay<br>AA1J1Q01A1<br>192.168.0.94 | Certificates have not yet been read from the IED |           |            |             |               |
| AA1J1Q01A4<br>Substation / Voltage Level / Bay<br>AA1J1Q01A4<br>192.168.0.13 | Certificates have not yet been read from the IED |           |            |             |               |

Figure 42: Deletion of certificates from an IED



Only CAM certificates can be deleted from PCM600.



It will not be possible to delete **Internal** and **External** certificates from PCM600



When IED is in Central Account Management mode, it is not recommended to remove Central Account Management certificates from the IED, because this action could cause connectivity problems between Central Account Management server (SDM600) and IED.

## 5.3 Activation of Central Account Management

Central Account Management on the IED must be activated from PCM600. The following are the steps to activate Central Account management on the IED:

1. Connect PC to the IED
2. Start PCM600, open project
3. Right click at **Substation** and select **Export** to export project SCD file

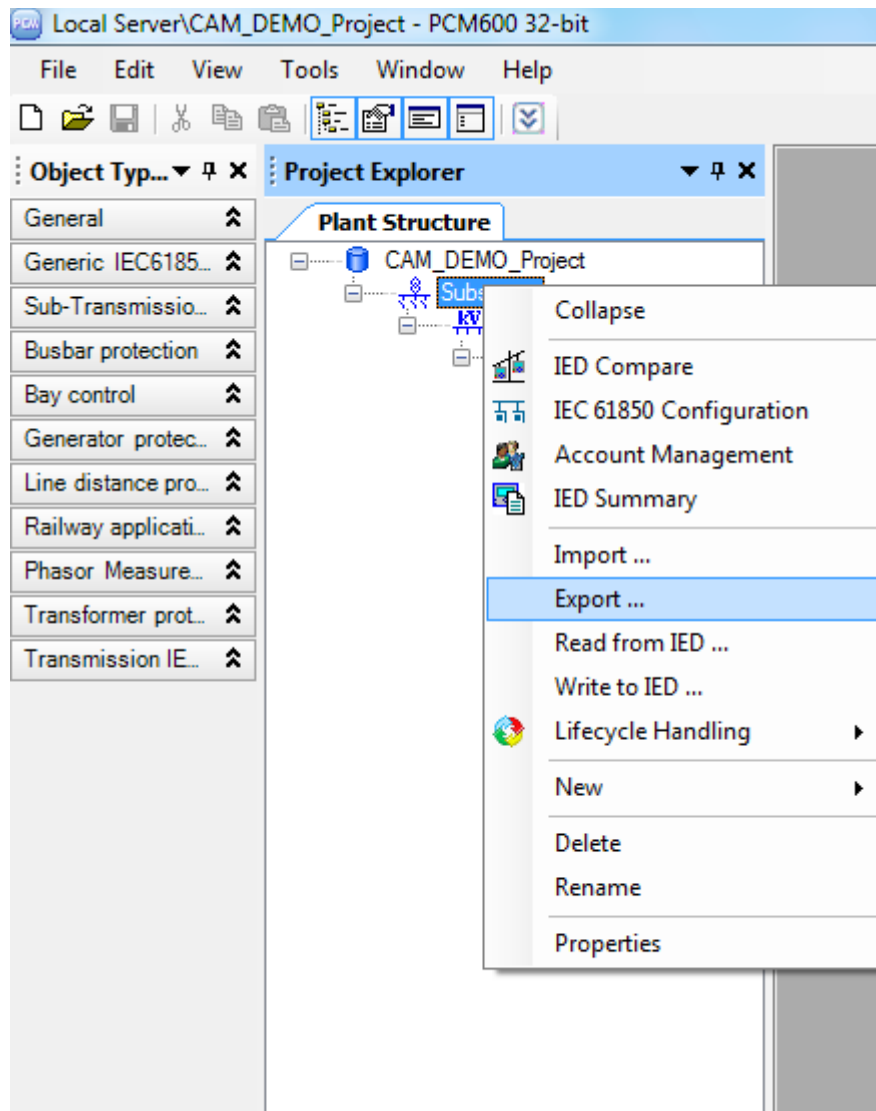


Figure 43: Export SCD file

4. Import project SCD file in SDM600 and generate **CAM configuration package**.



Please refer to SDM600 documentation for the detailed steps to generate CAM configuration package from SCD file.

5. From PCM600, select **Voltage Level** or Bay or IED in the plant structure
6. Select **Tools/Account Management**
7. Right click on Voltage Level or Bay or IED in the plant structure and select **Account Management**. The Account Management dialog will appear as shown below

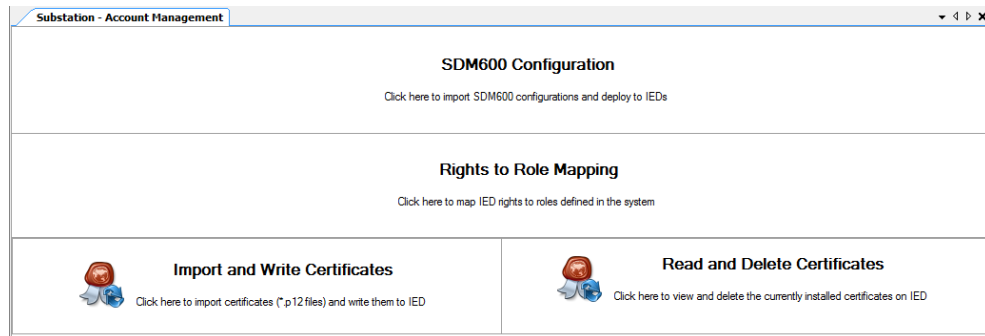


Figure 44: Account Management Tool in PCM

8. Click on **SDM600 Configuration** button, to open SDM600 configuration tool.

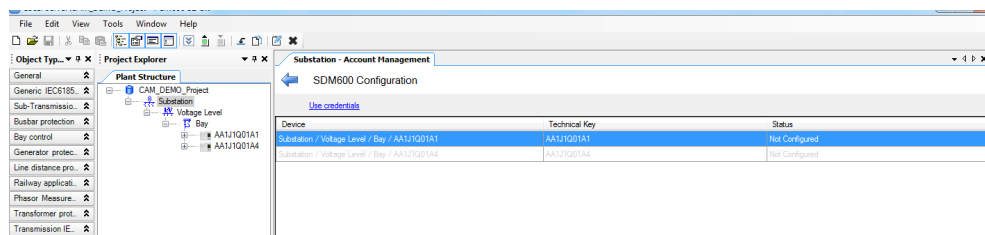


Figure 45: Import SDM600 configuration

- 9.



From Tool bar, click  to import **SDM600 configuration zip file** that is generated above at step #4.

10. If the SDM600 configuration zip file/certificate is protected with password (KEK), then the user will be prompted to enter password.

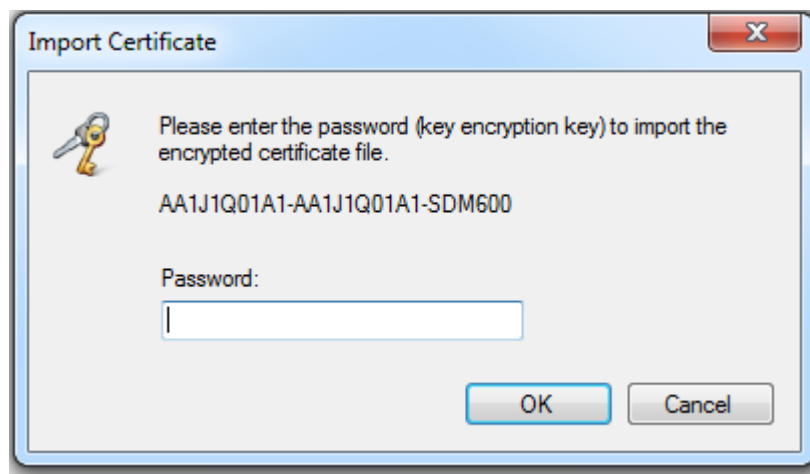


Figure 46: Password for the certificate package

11. **Import Summary** dialog will show the actions performed on each IED in the plant structure.

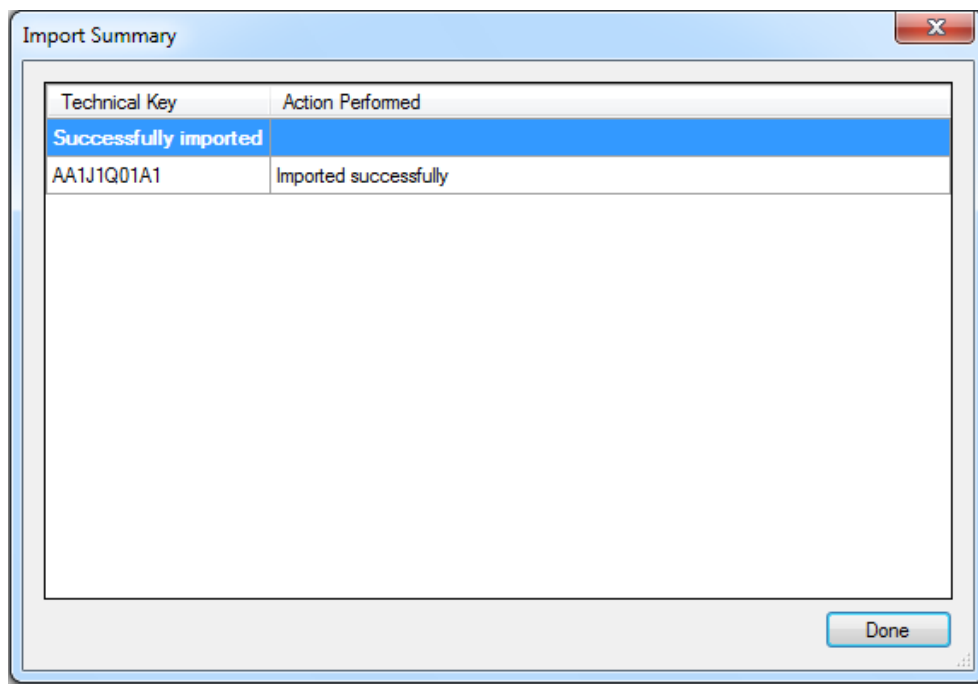


Figure 47: SDM600 configuration import results

12. Click on **Done** button.
13. In **Account management** tool, select the IED(s) for which **Central Account Management** needs to be activated.
14. To enable Central Account Management for the selected IED(s), from Toolbar, click



button.

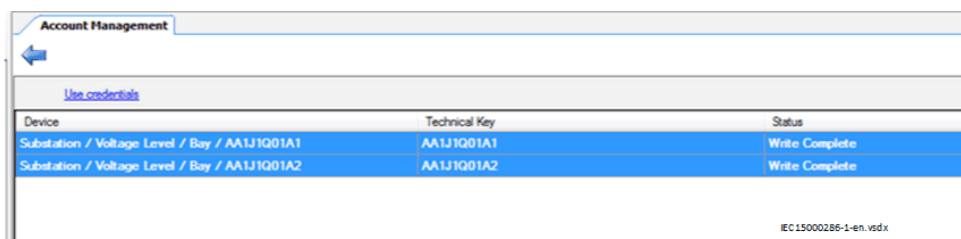


Figure 48: Writing Central Account Management to IED

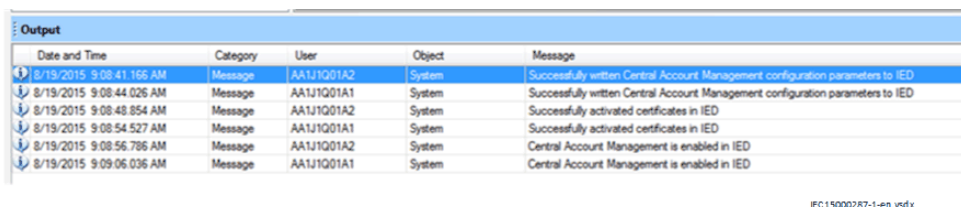


Figure 49: Central Account Management write status

When Central Account Management is set to active, the IED will do the following:

- Verify the configuration to secure that SDM600 can be accessed.
- Replicate the defined user group from SDM600 to the IED. At least one user must be replicated.



The maximum number of replicated users supported by the IED is 100. If replication group is empty or contains more than 100 users, the Central Account Management will fail.



It is recommended to define replication groups in SDM600 and associate them to the devices when CAM configuration is created. One replication group can be used in several devices. SDM600 has the possibility to replicate all users from the server however this is not consider a good security practice and it reduces the maximum number of replicated users.



If replication is disabled and the Central Account Management server is not reachable, the user will not be able to login to the IED. Replication support is only available if the customer is using SDM600. If the customer is using LDAP servers other than SDM600 no user replication is possible. . The replication support must be disabled to enable CAM in the IED



The configuration for Central Account Management is handled by a new tool in PCM600. The possibility to enable/disable replication is done in a checkbox (*Replication*) in the tool.

When this is successfully done, the IED will indicate that Central Account Management as active. In addition the IED will delete any users locally defined in the IED by PCM600 user tool.

If the Central Account Management activation fails, the activate parameter will be reset and Central Account Management must be activated again and a failure message will be indicated in PCM Output window.

When Central Account Management is activated, any ongoing sessions with the IED will continue until they are closed.

### 5.3.1 Manual configuration of Central Account Management

It is possible to edit Central Account Management configuration parameters and modify them (if needed) in PCM600. In order to edit configuration parameters, right click on the **Device** and select **Edit** as shown below.

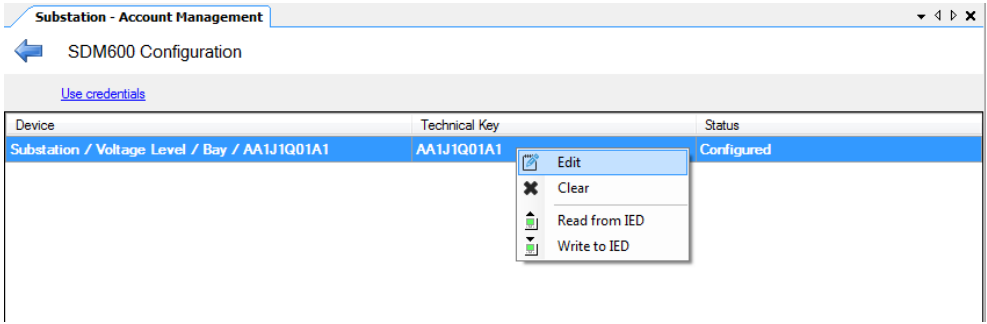


Figure 50: Edit configuration

The following screen appears, where in which user can edit the Central Account Management configuration parameters and/or manually change the certificate.

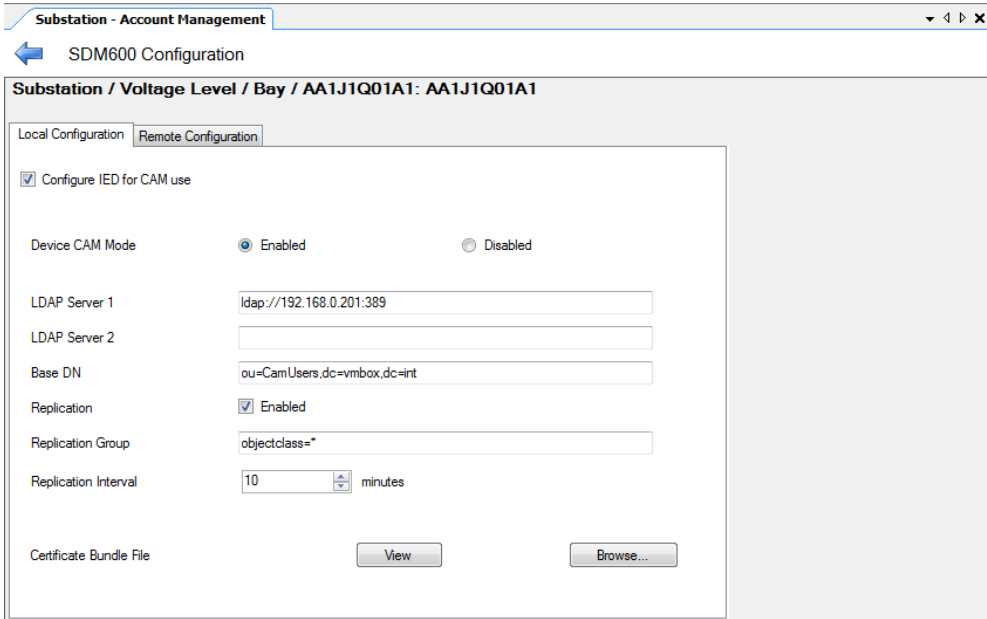


Figure 51: Local configuration

**Local Configuration** tab indicates the configuration that currently exists in PCM600.

**Remote Configuration** tab indicates the configuration that currently exists in the IED.



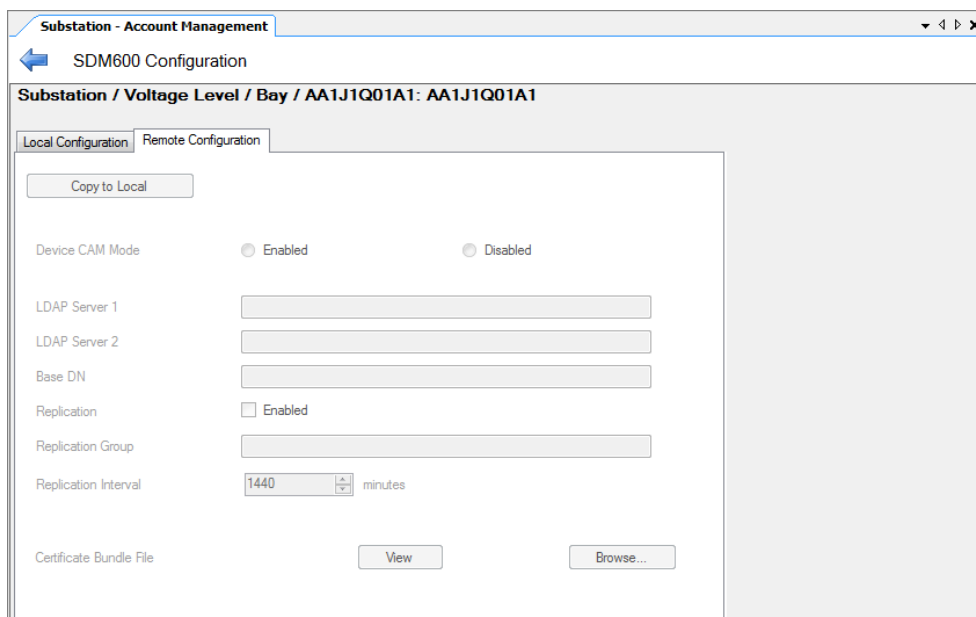


Figure 52: Remote configuration



**Remote Configuration** tab will have the configuration only if **Read Central Account Management Configuration** from the IED as described in section [Reading configuration from IED](#) is performed.

### 5.3.2 Reading configuration from IED

It is possible to read Central Account Management configuration from the IED by right clicking on the **Device** and selecting **Read from IED**.

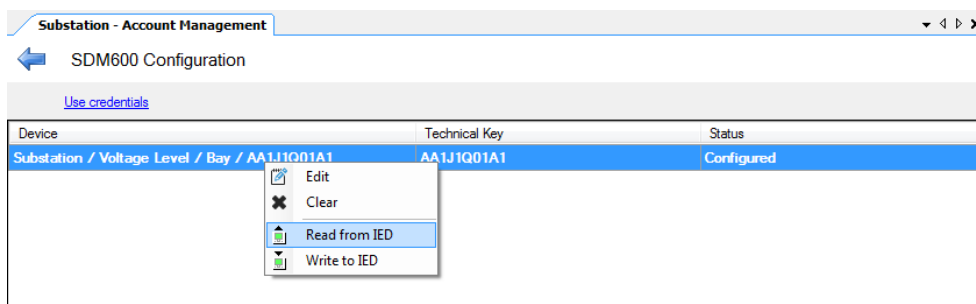


Figure 53: Read configuration from IED

### 5.3.3 Deactivation of Central Account Management from PCM600

When Central Account Management is switched off in the IED, the IED will go back to be open. There will not be any IED users defined even if that was the case when Central Account Management was activated.

Instead the built-in, factory default users will be reactivated.

1. Right click on the **Device** in Account Management tool and select **Edit** as shown in figure [53](#)

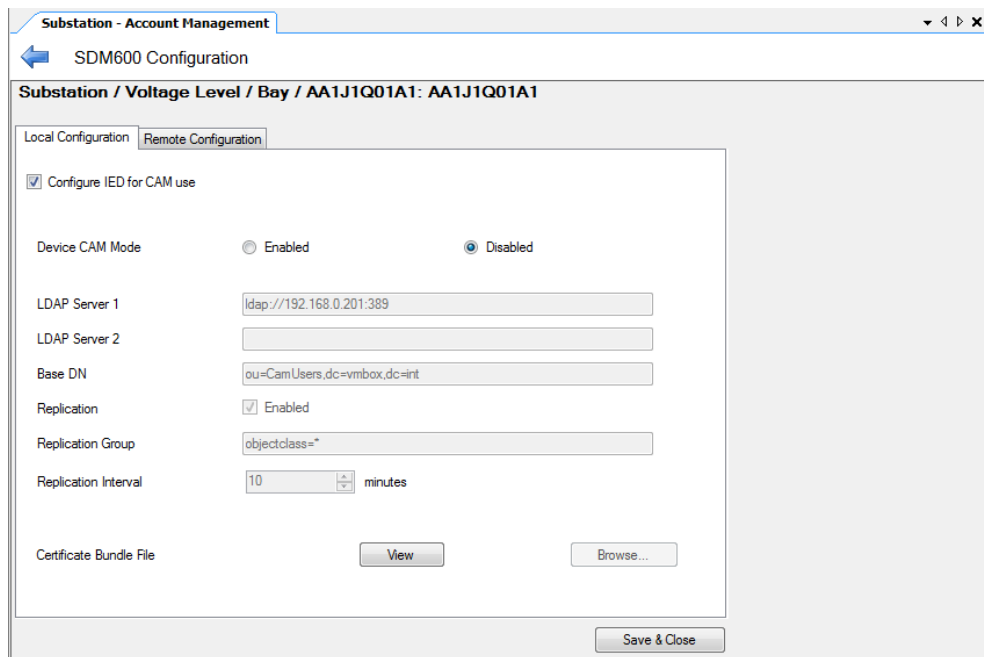


Figure 54: Deactivation of Central Account Management

2. Select **Device CAM Mode** as **Disable** as shown in fig 54
3. Click on **Save & Close** button, to save and close manual configuration screen.
4. Right click on the **Device**, and select **Write to IED** as shown in fig 55

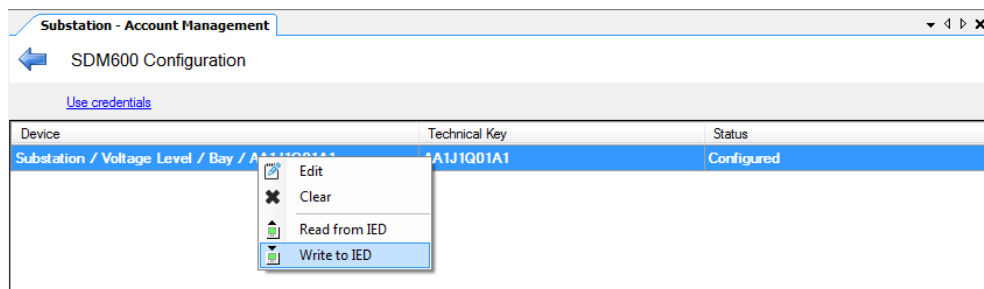


Figure 55: Write configuration to IED





5. PCM600 output window indicates the result of the write operation as shown in fig 56

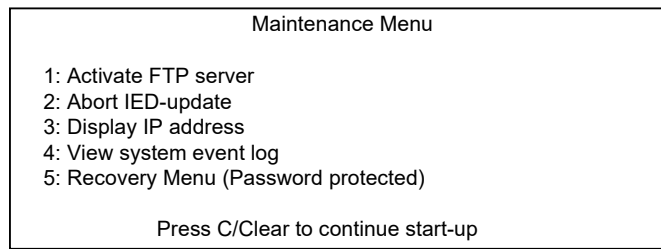
| Output                   |          |                         |        |  |
|--------------------------|----------|-------------------------|--------|--|
| Date and Time            | Category | User                    | Object | Message  |
| 8/19/2015 9:42:44.665 AM | Message  | AA1J1Q01A1              | System | Central Account Management configuration parameters are changed  |
| 8/19/2015 9:42:44.676 AM | Message  | AA1J1Q01A1              | System | Successfully re-activated Central Account Management in IED  |
| 8/19/2015 9:42:44.722 AM | Message  | [local]abb - System ... | System | Timestamp updated after Writing Central Account Management configuration parameters to IED : 08/19/2015 09:42:44 |
| 8/19/2015 9:42:59.506 AM | Message  | AA1J1Q01A1              | System | Successfully activated certificates in IED   |
| 8/19/2015 9:42:59.512 AM | Message  | [local]abb - System ... | System | Timestamp updated after transferring and activating Certificate in IED : 08/19/2015 09:42:59                     |
| 8/19/2015 9:43:00.124 AM | Message  | AA1J1Q01A1              | System | Successfully disabled Central Account Management in IED  |
| 8/19/2015 9:43:08.131 AM | Message  | [local]abb - System ... | System | Timestamp updated after Writing Central Account Management mode to IED : 08/19/2015 09:43:08                     |

Figure 56: PCM600 output window indicating deactivation of Central Account Management in the IED

### 5.3.4 Deactivation of Central Account Management on local HMI


In case of wrong configuration of CAM and Certificates, there is a possibility to disable Central Account Management and delete the loaded certificates in the IED. This can be done from recovery menu option. To enter this menu, the IED must be rebooted and a specific key combination must be pressed on the LHMI during the IED boot sequence.

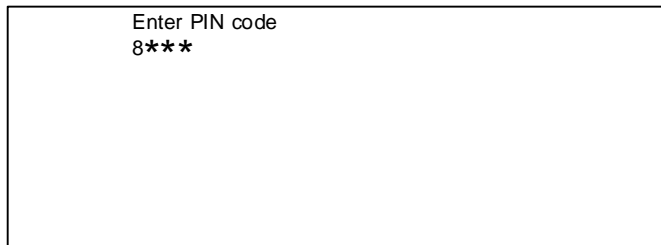
1. Switch off the power supply to the IED and leave it off for one minute.
2. Switch on the power supply to the IED and press and hold down  and  until the Maintenance Menu appears on the LHMI (this takes around 20-60s).
3. Navigate down and select Recovery Menu and press  or .



IEC12000168-3-en.vsd



*Figure 57:*

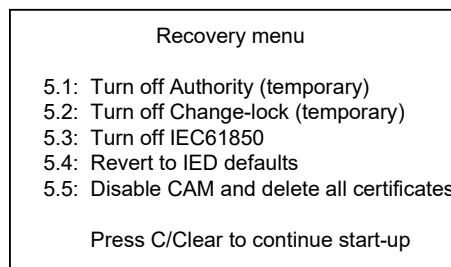
4. Enter PIN code 8282 and press .



IEC13000036-3-en.vsd

*Figure 58:*

5. Select Delete Certificates and Disable CAM and press  or .



IEC12000170-3-en.vsd

*Figure 59: Selection menu*

6. Select OK to Delete Certificates and Disable CAM

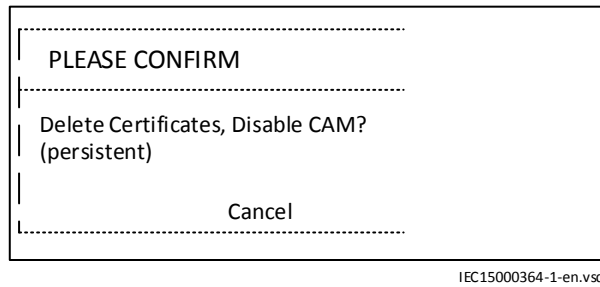


Figure 60: Confirmation

7. Press **Clear** to continue the startup sequence (now all the loaded certificates are deleted in the IED and Central account management is disabled in the IED).

To cancel the operation in any step, press **ESC**.

## 5.4 Authorization with Central Account Management enabled IED

The users, their roles and rights are created, deleted and edited only in the Central Account Management server (SDM600). However, the user rights can be edited in the IED by using the PCM600 user tool.

One user can have one or several user roles. By default, the users in Table 7 are created in the IED, and when creating new users in the SDM600 server, the predefined roles from Table 8 can be used.




At delivery, the IED user has full access as SuperUser when using the LHMI and as Administrator when using FTP or PCM600 until Central Account Management is activated.

Table 7: Default users

| User name     | User rights   |
|---------------|---|
| SuperUser     | Full rights, only presented in LHMI. LHMI is logged on by default until other users are defined                           |
| Guest         | Only read rights, only presented in LHMI. LHMI is logged on by default when other users are defined (same as VIEWER)      |
| Administrator | Full rights. Password: Administrator. This user has to be used when reading out disturbances with third party FTP-client. |

Table 8: Predefined user roles according to IEC 62351-8

| User roles                   | Role explanation | User rights  |
|------------------------------|------------------|--|
| VIEWER                       | Viewer           | Can read parameters and browse the menus from LHMI   |
| OPERATOR                     | Operator         | Can read parameters and browse the menus as well as perform control actions                                      |
| ENGINEER                     | Engineer         | Can create and load configurations and change settings for the IED and also run commands and manage disturbances |
| INSTALLER                    | Installer        | Can load configurations and change settings for the IED  |
| Table continues on next page |                  |  |

| User roles    | Role explanation       | User rights  |
|---------------|------------------------|--|
| SECADM        | Security administrator | Can change role assignments and security settings. Can deploy certificates.  |
| SECAUD        | Security auditor       | Can view audit logs  |
| RBACMNT       | RBAC management        | Can change role assignment   |
| ADMINISTRATOR | Administrator rights   | Sum of all rights for SECADM, SECAUD and RBACMNT<br><br> This User role is vendor specific and not defined in IEC 62351-8 |



Changes in user management settings do **not** cause an IED reboot.



The PCM600 tool caches the login credentials after successful login for 15 minutes. During that time no more login will be necessary.

The successful activation of Central Account Management will disable built-in users or remove all local created users from PCM600.

Management of user credentials and roles is handled on the central Account Management server e.g. SDM600. The IED employs two strategies to ensure availability of the authentication system even if there is a problem with the network or authentication server:

- A substation can be equipped with two redundant authentication servers operating in a hot standby mode.
- If configured by the security administrator, the IED itself maintains a local replica in the database with selected users. This database is periodically updated with data from the server and used as fallback if none of the servers are reachable.

Note that not all users in the SDM600 server are part of the replica. There might be users that are not assigned to any replication group. IED only replicates those users which are part of replication group configured in the IED.

This replication can be disabled using PCM600 by the security administrator, which means that the IED will forward login requests to the SDM600 for authorization and in case of problems with the network users will not be able to log in to the IED.



If user replication has been disabled in a CAM-enabled IED and if communication with SDM600 is lost, access to that IED will be denied until communication is re-established.

All communication between the central management and the IEDs is protected using secure communication. Customers using SDM600 are required to generate and distribute certificates during the engineering process of the substation. These certificates ensure mutual trust between IED and for example SDM600, FTP, PCM600 and other system.

Table 9: Authority-related IED functions

| Function                        | Description   |
|---------------------------------|---|
| Authority status<br>ATHSTAT     | This function is an indication function block for user logon activity. User denied attempt to logon and user successful logon are reported.   |
| Authority check<br>ATHCHCK      | To safeguard the interests of our customers, both the IED and the tools that are accessing the IED are protected, by means of authorization handling. The authorization handling of the IED and the PCM600 is implemented at both access points to the IED: <ul style="list-style-type: none"> <li>local, through the local HMI</li> <li>remote, through the communication ports</li> </ul> <p>The IED users can be created, deleted and edited only in the CAM server.</p> |
| Authority management<br>AUTHMAN | This function enables/disables the maintenance menu. It also controls the maintenance menu logon time out.  |

For more information on the functions Authority Management (AUTHMAN), Authority Status (ATHSTAT), and Authority Check (ATHCHCK) functions, refer to chapter “Basic IED functions” in the Technical Manual.

## 5.5 Predefined user roles

There are different roles of users that can access or operate different areas of the IED and tool functions.

The meaning of the legends used in the table:

- X= Full access rights
- R= Only reading rights
- - = No access rights

Table 10: Predefined user roles according to IEC 62351-8

| Access rights          | VIEWER | OPERATOR | ENGINEER | INSTALLER | SECADM | SECAUD | RBACMNT | ADMINISTRATOR |
|------------------------|--------|----------|----------|-----------|--------|--------|---------|---------------|
| Config – Basic         | -      | -        | X        | X         | -      | -      | -       | -             |
| Config – Advanced      | -      | -        | X        | X         | -      | -      | -       | -             |
| FileTransfer – Tools   | -      | -        | X        | X         | -      | -      | -       | -             |
| UserAdministration     | -      | -        | -        | -         | X      | -      | X       | X             |
| Setting – Basic        | R      | -        | X        | X         | -      | -      | -       | -             |
| Setting – Advanced     | R      | -        | X        | X         | -      | -      | -       | -             |
| Control – Basic        | -      | X        | X        | -         | -      | -      | -       | -             |
| Control – Advanced     | -      | X        | X        | -         | -      | -      | -       | -             |
| IEDCmd – Basic         | -      | X        | X        | -         | -      | -      | -       | -             |
| IEDCmd – Advanced      | -      | -        | X        | -         | -      | -      | -       | -             |
| FileTransfer – Limited | -      | X        | X        | X         | X      | X      | X       | X             |
| DB Access normal       | -      | X        | X        | X         | X      | X      | X       | X             |

Table continues on next page

| Access rights                  | VIEWER | OPERATOR | ENGINEER | INSTALLER | SECADM | SECAUD | RBACMNT | ADMINISTRATOR |
|--------------------------------|--------|----------|----------|-----------|--------|--------|---------|---------------|
| Audit log read                 | -      | -        | -        | -         | -      | X      | -       | X             |
| Setting – Change Setting Group | -      | X        | X        | X         | -      | -      | -       | -             |
| Security Advanced              | -      | -        | -        | -         | -      | X      | -       | X             |



ADMINISTRATOR is a vendor specific user role and not specified in IEC 62351-8

Table 11: Access rights explanation

| Access rights                  | Explanation  |
|--------------------------------|--|
| Config – Basic                 | Configuration – Basic is intended for engineers that only adapt an existing configuration e.g. the I/O-Configuration using SMT                   |
| Config – Advanced              | Configuration – Advanced is intended for engineers that do the whole application engineering and using e.g. ACT                                  |
| FileTransfer – Tools           | FileTransfer – Tools is used for some configuration files for the configuration and shall have the same value as Config – Advanced               |
| UserAdministration             | UserAdministration is used to handle user management e.g. adding new user  |
| Setting – Basic                | Setting – Basic is used for basic settings e.g. control settings and limit supervision   |
| Setting – Advanced             | Setting – Advanced is used for the relay engineer to set settings e.g. for the protection functions  |
| Control – Basic                | Control – Basic is used for a normal operator without possibility to bypass safety functions e.g. interlock or synchro-check bypass              |
| Control – Advanced             | Control – Advanced is used for an operator that is trusted to do process commands that can be dangerous  |
| IEDCmd – Basic                 | IEDCmd – Basic is used for commands to the IED that are not critical e.g. Clear LEDs, manual triggering of disturbances                          |
| IEDCmd – Advanced              | IEDCmd – Advanced is used for commands to the IED that can hide information e.g. Clear disturbance record  |
| FileTransfer – Limited         | FileTransfer - Limited is used for access to disturbance files e.g. through FTP  |
| DB Access normal               | Database access for normal user. This is needed for all users that access data from PCM  |
| Audit log read                 | Audit log read allows reading the audit log from the IED   |
| Setting – Change Setting Group | Setting – Change Setting Group is separated to be able to include the possibility to change the setting group without changing any other setting |
| Security Advanced              | Security Advanced is the privilege required to do some of the more advanced security-related settings  |

IED users can be created, deleted and edited only in the SDM600 server. From the LHMI or PCM600, no users can be created nor changed when Central Account Management has been enabled in the IED. However, user rights are edited using the PCM600 user tool (IEDUM) and password can be changed from PCM600 or LHMI.

At delivery, the IED has a default Administrator defined with full access rights. PCM600 uses this default user to access the IED. This user is automatically removed in IED when users are defined in the SDM600 server and replicated to the IED.



Only characters A - Z, a - z and 0 - 9 shall be used in user names. User names are not case sensitive. For passwords see the Password policies.



In order to allow the IED to communicate with PCM600 when users are defined in the SDM600 server, the access rights "UserAdministration" and "FileTransfer — Limited" must be applied to at least one user. User rights are assigned using the PCM600 user tool (IEDUM).



"DB Access normal" and "FileTransfer – Limited" are required for PCM600 access to the IED.

## 5.6 Password policy settings for Central Account Management enabled IED

The password policy is set in the Central Account Management server (SDM600). Refer to SDM600 user manual.

## 5.7 PCM600 access to Central Account Management enabled IED

During normal access, e.g. parameter writing, of the IED from PCM600, the user interaction will be very similar as to a non Central Account Management enabled IED. The following steps are included in the process:

- When a login is needed the login dialog is presented to the user
- When the user name and password is entered the user credentials are sent to the IED
- The IED forwards these credentials to the Central Account Management server to authenticate the user and get the user roles back. If a user has multiple roles, then the privilege he gets is the union of all the roles.
  - If the IED fails in accessing the Central Account Management server, the local replica of the users are used to authenticate the user and get the user roles back
- The IED check the Rights for the Roles and secure that only authorized things according to the Rights are allowed



If communication with the Central Account Management server is lost, the current password will not expire until the communication with the server is reestablished.



When the user tries to communicate with an IED using PCM600, then PCM600 will validate the "Certificate" presented by the IED and if there are new warnings/errors found during certificate validation, PCM600 will display a Security Warning to the user. In this situation, user needs to take appropriate action on the security warning to continue communicating with the IED.





If the user tries to authenticate towards a Central Account Management enabled IED using PCM600, with credentials that will expire in the near future, a new warning will be shown to the user and an option to change the password will be provided.

## 5.7.1 Changing password

The user can also change the own password from PCM600 or LHMI. The following process is used:

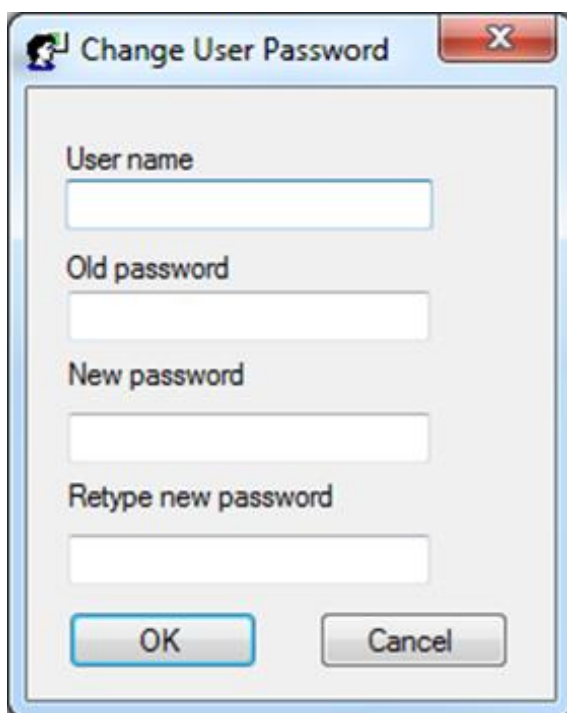
- A change password dialog is presented for the user in PCM600 or LHMI
- The IED will forward this to the Central Account Management server
  - Password can only be changed if the IED has contact with Central Account Management server
- The Central Account Management server verifies the password towards the password policies
  - If it fails an error code will be sent back to the user
- An acknowledgement is sent back to the IED and forwarded to PCM600 or LHMI
- The user gets an acknowledge that the password has changed

As soon as the IED get feedback from the Central Account Management server that the password is about to expire or that the password need to be changed, the user will be forced to change the password. The actual change will be according to above. The SDM600 server will issue a warning message that the password is going to expire (for instance in 5 days) if this feature is configured in SDM600. If the password has expired or is not valid for other reasons, a new password must be set in the Central Account Management server.

A change of password for any user, via PCM600 or LHMI, will force a replication of the users to the IED. Otherwise, if the communication to the Central Account Management server is lost shortly after the passwords is changed, the old password must be used until the connection to Central Account Management server is restored. All other IEDs in the system need to wait until next cyclic replication.

### Changing password

1. Right click on the IED in plant structure and select IED users tool.
2. Go to General Tab.
3. Click on Change Own Password, then following dialog will appear



IEC15000295-1-en.vsd x

*Figure 61: Change own password*

4. User can enter details and click on OK button. Password will be changed and the result of the operation will be indicated in the PCM600 output window.

## 5.7.2 Error messages

When a user wants to access the IED or change the password, it might fail. In such cases the user will be presented that it failed and also a reason.

The tables below list the possible error messages. The UAL column marks if the error is logged as a security event. The User feedback column marks the message to the user. In some cases another error is listed and will be presented for the user.

Table 12: Error indications from failed login

| Description  | EVENT NUMBER | User feedback   |
|--|--------------|---|
| Login successful.<br>An additional password expiry time can be sent by the CAM server. This information contains the number of seconds for which the password is still valid at the time the authentication was executed.* | 1110         | *: Your password will expire in x days. Do you want to change it? |
| Login successful.<br>When in Central Account Management: Password has expired and the user had grace logins left. (Of which one was used for this login).*<br>When in PCM600 users: Password expired login OK.**           | 1115         | *: Password must be changed.<br>**: Login OK, password expired.   |
| Login failed   | 1120         | Access denied   |
| Login failed.<br>Password has expired. User should contact the system administrator to reset the password.   | 1150         | Password expired  |
| Login failed 3 times (in case of PCM600 users only)  | 1170         | Login blocked for this ID!  |
| An error occurred during authentication. (E.g. No server connection and replica.)  |              | Error in the Central Account Server!                              |
| User authentication has failed due to wrong username and/or password.  | 1130         | Access denied   |

Table 13: Error indications from failed change password

| Description   | EVENT NUMBER | User feedback                           |
|---|--------------|---|
| Password of <User name> has been successfully changed to <new password>   | 2210         | Password change successful              |
| Provided credentials <old password> could not be used to login.<br>Password is not changed.   | 1130 + 2220  | Old password invalid.                   |
| Provided credentials <old password> already expired.<br>Password is not changed.  | 1150 + 2220  | Password expired                        |
| Password <new password> did not fulfill the password policy of the CAM server.<br>Password is not changed.  | 2235         | Password do not meet policy requirement |
| CAM server failed to write password to the provider.<br>Password is not changed.  | 2220         | Error in the Central Account Server!    |
| Connection to CAM server could not be established or connection has been terminated unexpectedly. Verify status and connectivity of the CAM server.<br>Password is not changed. | 2220         | Error in the Central Account Server!    |
| Generic error.<br>Password is not changed.  | 2220         | Error in the Central Account Server!    |

## 5.8 Trouble shooting Central Account Management.

To know the status of the Central Account Management, the diagnostics information is provided on Local HMI. This is available under **Diagnostics/Communication/CAM status/CAMStatus**

1. When IED is not configured with any users the default status of the **CAMStatus** diagnostics will be:

|  |                |             |
|--|----------------|-------------|
| ...menu/Diagnostics/Communication/CAM status/CAMStatus:1 |                |             |
| UAMMode  |                |             |
| Builtin  |                |             |
| CAMServer1Status   | Not configured |             |
| CAMServer2Status   | Not configured |             |
| Replication  | Not replicated |             |
| ReplicaLastUpdate  | Never          |             |
|  |                |             |
| 2015-09-28 15:38:26                                      | \$SuperUser    | Object name |

IEC15000369-1-en.vsd.x

Figure 62: CAM default status

2. When IED is not configured with Central Account Management the default status of the **CAMStatus** diagnostics will be:

|  |                |             |
|--|----------------|-------------|
| ...menu/Diagnostics/Communication/CAM status/CAMStatus:1 |                |             |
| UAMMode  | Local          |             |
| CAMServer1Status   | Not configured |             |
| CAMServer2Status   | Not configured |             |
| Replication  | Not replicated |             |
| ReplicaLastUpdate  | Never          |             |
|  |                |             |
| 2015-09-28 16:38:10                                      | \$Guest        | Object name |

IEC15000354-1-en.vsd.x

Figure 63: CAM diagnostics default status

3. When the IED is Central Account Management configured with One server, the status of CAMStatus will be:

|  |                     |             |
|--|---------------------|-------------|
| ...menu/Diagnostics/Communication/CAM status/CAMStatus:1 |                     |             |
| UAMMode  | Central             |             |
| CAMServer1Status   | Online              |             |
| CAMServer2Status   | Not configured      |             |
| Replication  | Good                |             |
| ReplicaLastUpdate  | 2015-09-28 16:36:58 |             |
|  |                     |             |
| 2015-09-28 16:37:11                                      | \$Guest             | Object name |

IEC15000355-1-en.vsd/x

Figure 64: IED CAM configured status

Table 14:

| Label            | Rational   | Values         | Remarks                                      |
|------------------|--|----------------|--|
| UAMMode          | User account management mode                               | Builtin        | When IED is configured with PCM users        |
|                  |  | Local          | When IED is configured with default users    |
|                  |  | Central        | When Central Account Management is active    |
| CAMServerXStatus | Indicates the connectivity status of the server X.         | Not configured | When there is no server URL specified        |
|                  |  | Online         | When specified server is online              |
|                  |  | Offline        | When specified server is offline             |
| Replication      | Indicates the status of the last replication               | Not replicated | When replication is not configured           |
|                  |  | Good           | When last replication was successful         |
|                  |  | Failed         | When last replication cycle has failed       |
| Last Update      | Indicates the last update of the status information above. | Never          | When replication was not configured          |
|                  |  | Timestamp      | Time when successful replication took place. |

4. Errors during activation or redeployment of Certificates:

Table 15: Errors

| Symptoms   | Probable causes   | Solution  |
|--|---|---|
| PCM error <b>CAM enabling failed.</b><br>or<br>Security event 3810 <b>CAM server communication failed.</b><br>or<br>Security event 3820 <b>Replication performed. No users replicated!.</b><br>or<br>Security event 3830 <b>Replication attempted but failed. No capacity.</b> | Wrong configuration parameters (e.g. LDAP address...).  | Check IED.2.1 CAM configuration parameters  |
|  | Server(s) not reachable during activation, Invalid or wrong certificate is deployed.                                    | In case of security event 3810 <b>CAM server communication failed:</b> Check if servers are reachable and the IED is connected. Also, check if the deployed certificates are valid.   |
|  | In case of replication is enabled, the replica is not valid (no users or more than 100 users in the replication group). | In case of 3820 <b>Replication performed. No users replicated!</b> or 3830 <b>Replication attempted but failed. No capacity.</b> Check if there are sufficient users in the replication group and there are not more than 100 users in the replication group.           |
|  |   | If the Central Account Management is activated without replication to a non existent Central Account Management server or in case of invalid certificate being redeployed. The only way to disable Central Account Management is through maintenance menu on Local HMI. |



If the initial activation of CAM failed, the IED reverts to local UAM or default users. Access to the device is possible using the local default credentials. If syslog is not configured then security events can be read from Event Viewer tool in PCM600.

##### 5. Server not reachable during runtime:

Table 16:

| Symptoms   | Probable causes         | Solution  |
|--|-------------------------|---|
| Diagnostics on Local HMI:<br>Central Account Manager Server<br>status will be indicated as<br><b>Offline</b> .<br><br>Security Event: 3810 <b>CAM Server<br/>           communication failed</b> . | Server(s) not reachable | Check if LDAP server is up and<br>running<br><br>Check IED connection |



Authentication will continue to work based on the latest local LDAP Replica if replication is enabled. After reconnection with the server(s), authentication will again run via the LDAP server and the local replica will be updated.

|  |                     |             |
|--|---------------------|-------------|
| ...menu/Diagnostics/Communication/CAM status/CAMStatus:1 |                     |             |
| UAMMode  | Central             |             |
| CAMServer1Status   | Offline             |             |
| CAMServer2Status   | Not configured      |             |
| Replication  | Failed              |             |
| ReplicaLastUpdate  | 2015-09-28 16:33:55 |             |
| 2015-09-28 16:36:10                                      | \$Guest             | Object name |

IEC 15000356-1-en.vsd.x

Figure 65: Replication status

##### 6. Local replication failed

Table 17:

| Symptoms  | Probable causes  | Solution   |
|---|--|--|
| <p>Diagnostics: <b>Replication Failed.</b><br/><i>ReplicaLastUpdate</i> shows the time when last successful replication.</p> <p>Security Event: 3810 <b>CAM Server communication failed</b></p> | <p>Server(s) not reachable</p> <p>Server configuration has changed</p> | <p>Check if LDAP server is up and running</p> <p>Verify with system administrator that LDAP settings are still valid</p> <p>Check the IED connection</p> |



Authentication will continue to work based on the latest local LDAP replica. After reconnection with the server(s), authentication will again run via the LDAP server and the local replica will be updated.



## Section 6 User activity logging

### 6.1 Activity logging protocol

Activity Logging can be reported from the IED through two different protocols; either IEC 61850 or Syslog. Syslog is a standard for computer message logging (RFC 5424). For IEC 61850, configuration is as for buffered reporting. Syslog is configured through a number of parameters where the Syslog server is defined. The IED is the Syslog client and it sends the events to the Syslog server.

Both IEC 61850 and Syslog are to be seen as online protocols when it comes to activity logging. If an event has occurred while 61850 or Syslog communication has been down, the events will not be retransmitted. In this case, use PCM600 to read out the activity logging from the IED.

### 6.2 Activity logging ACTIVLOG

ACTIVLOG contains all settings for activity logging.

There can be 6 external log servers to send syslog events to. Each server can be configured with IP address; IP port number and protocol format. The format can be either syslog (RFC 5424) or Common Event Format (CEF) from ArcSight.

### 6.3 Settings

Table 18: ACTIVLOG Non group settings (basic)

| Name           | Values (Range)                                      | Unit          | Step | Default   | Description                       |
|----------------|---|---------------|------|-----------|-----------------------------------|
| ExtLogSrv1Type | Off<br>SYSLOG UDP/IP<br>SYSLOG TCP/IP<br>CEF TCP/IP | -             | -    | Off       | External log server 1 type        |
| ExtLogSrv1Port | 1 - 65535   | -             | 1    | 514       | External log server 1 port number |
| ExtLogSrv1IP   | 0 - 18  | IP<br>Address | 1    | 127.0.0.1 | External log server 1 IP-address  |
| ExtLogSrv2Type | Off<br>SYSLOG UDP/IP<br>SYSLOG TCP/IP<br>CEF TCP/IP | -             | -    | Off       | External log server 2 type        |
| ExtLogSrv2Port | 1 - 65535   | -             | 1    | 514       | External log server 2 port number |
| ExtLogSrv2IP   | 0 - 18  | IP<br>Address | 1    | 127.0.0.1 | External log server 2 IP-address  |
| ExtLogSrv3Type | Off<br>SYSLOG UDP/IP<br>SYSLOG TCP/IP<br>CEF TCP/IP | -             | -    | Off       | External log server 3 type        |
| ExtLogSrv3Port | 1 - 65535   | -             | 1    | 514       | External log server 3 port number |
| ExtLogSrv3IP   | 0 - 18  | IP<br>Address | 1    | 127.0.0.1 | External log server 3 IP-address  |

Table continues on next page

| Name           | Values (Range)                                      | Unit          | Step | Default   | Description                       |
|----------------|---|---------------|------|-----------|-----------------------------------|
| ExtLogSrv4Type | Off<br>SYSLOG UDP/IP<br>SYSLOG TCP/IP<br>CEF TCP/IP | -             | -    | Off       | External log server 4 type        |
| ExtLogSrv4Port | 1 - 65535   | -             | 1    | 514       | External log server 4 port number |
| ExtLogSrv4IP   | 0 - 18  | IP<br>Address | 1    | 127.0.0.1 | External log server 4 IP-address  |
| ExtLogSrv5Type | Off<br>SYSLOG UDP/IP<br>SYSLOG TCP/IP<br>CEF TCP/IP | -             | -    | Off       | External log server 5 type        |
| ExtLogSrv5Port | 1 - 65535   | -             | 1    | 514       | External log server 5 port number |
| ExtLogSrv5IP   | 0 - 18  | IP<br>Address | 1    | 127.0.0.1 | External log server 5 IP-address  |
| ExtLogSrv6Type | Off<br>SYSLOG UDP/IP<br>SYSLOG TCP/IP<br>CEF TCP/IP | -             | -    | Off       | External log server 6 type        |
| ExtLogSrv6Port | 1 - 65535   | -             | 1    | 514       | External log server 6 port number |
| ExtLogSrv6IP   | 0 - 18  | IP<br>Address | 1    | 127.0.0.1 | External log server 6 IP-address  |

## 6.4 Generic security application GSAL

As a logical node GSAL is used for monitoring security violation regarding authorization, access control and inactive association including authorization failure. Therefore, all the information in GSAL can be configured to report to 61850 client. For more information about GSAL, see IEC 61850 Edition 2 Communication Protocol Manual.

## 6.5 Security alarm SECALARM

The function creates and distributes security events for mapping the security events on protocols such as DNP3.

It is possible to map respective protocol to the signals of interest and configure them for monitoring with the Communication Management tool (CMT) in PCM600. No events are mapped by default.

Parameter names:

- EVENTID: Event ID of the generated security event
- SEQNUMBER: Sequence number of the generated security event

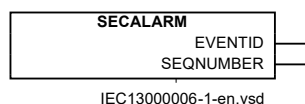


Figure 66: Function block, Security alarm SECALARM

## 6.5.1 Signals

Table 19: SECALARM Output signals

| Name      | Type    | Description                                     |
|-----------|---------|---|
| EVENTID   | INTEGER | EventId of the generated security event         |
| SEQNUMBER | INTEGER | Sequence number of the generated security event |

## 6.5.2 Settings

Table 20: SECALARM Non group settings (basic)

| Name      | Values (Range) | Unit | Step | Default | Description      |
|-----------|----------------|------|------|---------|------------------|
| Operation | Off<br>On      | -    | -    | On      | Operation On/Off |

## 6.6 About Security events

Relevant user operations are logged as security events. A security event contains an event ID, a time stamp, a sequence number, the user name, the severity of the action and the name of the source. These events can be sent to external security log servers using Syslog. The log servers are configured from PCM600. Syslog is a standard protocol for event logging.



To be able to access the security logs the user need the role SECAUD (security auditor) or the access right “Audit log read”.

## 6.7 Event types

The following table contains the event types that can be logged, including their 61850 mapping on the logical node GSAL

Table 21: Event type codes

| Event number                 | Acronyms                | GSAL mapping  | English                                 |
|------------------------------|-------------------------|---------------|---|
| 1110                         | LOGIN_OK                | GSAL.Ina      | Login successful                        |
| 1115                         | LOGIN_OK_PW_EXPIRED     | GSAL.Ina      | Password expired, login successful      |
| 1120                         | LOGIN_FAIL_UNKNOWN_USER | GSAL.AuthFail | Login failed - Unknown user             |
| 1130                         | LOGIN_FAIL_WRONG_CR     | GSAL.AuthFail | Login failed - Wrong credentials        |
| 1150                         | LOGIN_FAIL_PW_EXPIRED   | GSAL.AuthFail | Login failed - Password expired         |
| 1170                         | LOGIN_FAIL_3_TIMES      | GSAL.AuthFail | Login failed 3 times                    |
| 1210                         | LOGOUT_USER             | GSAL.Ina      | Logout (user logged out)                |
| 1370                         | VIEW_SEC_EV_LIST_OK     | GSAL.Ina      | Viewed security event logs successfully |
| 1380                         | PARAM_CHANGE_OK         | GSAL.Ina      | Parameter changed successfully          |
| Table continues on next page |                         |               |   |

| Event number                 | Acronyms                    | GSAL mapping    | English   |
|------------------------------|-----------------------------|-----------------|---|
| 1460                         | PARAM_CHANGE_FAIL_RIGHTS    | GSAL.AcsCtlFail | Parameter changes failed — no rights                  |
| 1470                         | PARAM_CHANGE_FAIL_RANGE     | GSAL.SvcViol    | Parameter change failed - out of range                |
| 1710                         | CONFIG_RESET_FACTORY_DEF    | GSAL.Ina        | Device reset to factory default                       |
| 2110                         | USER_ACCNT_CREATE_OK        | GSAL.Ina        | User account created successfully                     |
| 2120                         | USER_ACCNT_DEL_OK           | GSAL.Ina        | User account deleted successfully                     |
| 2130                         | USER_ACCNT_CREATE_FAIL      | GSAL.SvcViol    | User account creation failed                          |
| 2140                         | USER_ACCNT_DEL_FAIL         | GSAL.SvcViol    | User account deletion failed                          |
| 2160                         | USER_NEW_ROLE_OK            | GSAL.Ina        | New role assigned to user successfully                |
| 2170                         | USER_ROLE_REMOVED_OK        | GSAL.Ina        | User role assignment removed successfully             |
| 2210                         | USER_PW_CHANGE_OK           | GSAL.SvcViol    | User password changed successfully                    |
| 2220                         | USER_PW_CHANGE_FAIL         | GSAL.SvcViol    | Change of user password failed                        |
| 2233                         | USER_PW_CHANGE_FAIL_SHORT   | GSAL.SvcViol    | User password change failed — too short               |
| 2235                         | USER_PW_CHANGE_FAIL_POLICY  | GSAL.SvcViol    | User Password change failed - policy check failed     |
| 3710                         | CAM_SRV_COMM_OK             | GSAL.Ina        | CAM Server communication successful                   |
| 3810                         | CAM_SRV_COMM_FAIL           | GSAL.Ina        | CAM Server communication failed                       |
| 3820                         | CAM_REPLICATION_NO_USERS    | GSAL.Ina        | Replication performed. No users replicated!           |
| 3830                         | CAM_REPLICATION_NO_CAPACITY | GSAL.Ina        | Replication attempted but failed. No capacity.        |
| 4210                         | SSL_CONN_FAIL_CERT          | GSAL.AuthFail   | SSL Connection failed - Certificate validation failed |
| 5110                         | MANUAL_RESET                | GSAL.Ina        | Manual reset  |
| 5270                         | SYS_STARTUP                 | GSAL.Ina        | System startup  |
| 5280                         | SYS_SHUTTING_DOWN           | GSAL.Ina        | System shutting down                                  |
| 6110                         | TEST_MODE_START_OK          | GSAL.Ina        | Test Mode started successfully                        |
| 6120                         | TEST_MODE_END               | GSAL.Ina        | Test mode ended successfully                          |
| 6130                         | CONTRL_OP_PERF_OK           | GSAL.Ina        | Control operation performed successfully              |
| 6132                         | CONTRL_OP_PERF_FAIL         | GSAL.Ina        | Failed to perform a control operation                 |
| 6140                         | SIGN_FORCED_VALUE           | GSAL.Ina        | Signal forced - value changed successfully            |
| 7310                         | HW_CHANGE_DETECTED          | GSAL.Ina        | Hardware change detected                              |
| 8020                         | DATE_TIME_SET_OK            | GSAL.Ina        | Date and time set successfully                        |
| 8030                         | NEW_CERT_GEN_OK             | GSAL.Ina        | New certificate generated successfully                |
| 8230                         | NEW_CERT_GEN_FAIL           | GSAL.Ina        | New certificate generation failed                     |
| 9010                         | ATT_DET_FLOODING            | GSAL.Ina        | Flooding attack detected                              |
| 9530                         | PKI_CERT_EXP_NEAR           | GSAL.Ina        | Certificate about to expire                           |
| Table continues on next page |                             |                 |   |

| Event number | Acronyms                    | GSAL mapping | English  |
|--------------|-----------------------------|--------------|--|
| 9620         | X509_CERT_EXPIRED           | GSAL.Ina     | Certificate validation failed - Certificate expired                |
| 9640         | X509_CERT_UNTRUSTED         | GSAL.Ina     | Certificate validation failed - Certificate signature check failed |
| 10010        | MAINT_ENTER_MENU_OK         | GSAL.Ina     | Device successfully entered maintenance menu due to user action    |
| 10020        | MAINT_FORCED_MENU_OK        | GSAL.Ina     | Device successfully forced into maintenance menu due to new state  |
| 10030        | MAINT_FTP_ACTIV_OK          | GSAL.Ina     | FTP server successfully activated from maintenance menu            |
| 10032        | MAINT_FTP_ACTIV_FAIL        | GSAL.Ina     | Activation of FTP server from maintenance menu failed              |
| 10040        | MAINT_UPDATE_ABORT_OK       | GSAL.Ina     | Firmware update procedure aborted successfully                     |
| 10050        | MAINT_RECOVERY_ENTER_OK     | GSAL.Ina     | Recovery menu entered successfully                                 |
| 10052        | MAINT_RECOVERY_ENTER_FAIL   | GSAL.Ina     | Failed to enter Recovery menu                                      |
| 10060        | MAINT_AUTH_DIS_OK           | GSAL.Ina     | Authentication disabled from maintenance menu successfully         |
| 10070        | MAINT_CHANGE_LOCK_DIS_OK    | GSAL.Ina     | Change lock disabled successfully from Maintenance menu            |
| 10080        | MAINT_61850_DIS_OK          | GSAL.Ina     | IEC 61850 disabled successfully from Maintenance menu              |
| 13200        | TRANSFER_CONFIG_OK          | GSAL.Ina     | Configuration transferred to the device successfully               |
| 13250        | CONFIG_MODE_ENTER_OK        | GSAL.Ina     | Entered configuration mode successfully                            |
| 13260        | CONFIG_MODE_EXIT_OK         | GSAL.Ina     | Exited configuration mode successfully                             |
| 13400        | TRANSFER_FIRMW_OK           | GSAL.Ina     | Firmware transferred to the device successfully                    |
| 13500        | READ_FIRMW_OK               | GSAL.Ina     | Firmware files read/exported from the device successfully          |
| 13520        | TRANSFER_CERTS_OK           | GSAL.Ina     | Certificates transferred to the device successfully                |
| 13580        | READ_CERTS_OK               | GSAL.Ina     | Exported/read certificates from device successfully                |
| 13610        | ADD_ENTITY_CERT_OK          | GSAL.Ina     | Installed entity certificate successfully                          |
| 13620        | REMOVE_ENTITY_CERT_OK       | GSAL.Ina     | Removed entity certificate successfully                            |
| 13630        | ADD_TRUST_ANCHOR_CERT_OK    | GSAL.Ina     | Installed trust anchor certificate successfully                    |
| 13640        | REMOVE_TRUST_ANCHOR_CERT_OK | GSAL.Ina     | Removed entity certificate successfully                            |
| 14200        | TRANSFER_CONFIG_FAIL        | GSAL.SvcViol | Failed to transfer configuration to the device                     |
| 14250        | CONFIG_MODE_ENTER_FAIL      | GSAL.Ina     | Failed to enter configuration mode                                 |
| 14260        | CONFIG_MODE_EXIT_FAIL       | GSAL.Ina     | Failed to exit configuration mode                                  |

Table continues on next page

| Event number | Acronyms            | GSAL mapping | English                                       |
|--------------|---------------------|--------------|---|
| 14400        | TRANSFER_FIRMW_FAIL | GSAL.SvcViol | Failed to transfer firmware to the device     |
| 14500        | READ_FIRMW_FAIL     | GSAL.Ina     | Failed to read firmware files from the device |
| 14520        | TRANSFER_CERTS_FAIL | GSAL.Ina     | Failed to transfer certificates to the device |
| 14580        | READ_CERTS_FAIL     | GSAL.Ina     | Failed to read certificates from the device   |

## Section 7 Local HMI use

At delivery, login is not required and the user has full access until users and passwords are created with PCM600 and written into the IED. The LHMI is logged on as SuperUser by default until other users are defined.

Commands, changing parameter values and resetting indications, for example, are actions requiring password when the password protection is activated. Reading information on the LHMI is always allowed without password. The LHMI is logged on as Guest by default when other users are defined.












Utility security policies and practical consideration should always be taken on the feasibility of using passwords. In emergency situations, the use of passwords could delay urgent actions. When security issues must be met, the two factors must be seriously considered.



The auxiliary power supply to the IED must not be switched off before changes such as passwords, setting parameter or local/remote control state changes are saved.




### 7.1 Logging on


1. Press  to activate the login procedure.  
The login is also activated when attempting a password-protected operation.
2. Press  to activate the User field.  
If CAM is activated an on-screen keyboard is shown.
3. Type in the user name using the on-screen keyboard.  
You can end user name editing at any time by pressing  while the user field is focused (or navigate to the OK button and press ) , or press  (or navigate to the Cancel button and press ) to abort the login attempt.  
If CAM is not activated select the user by scrolling with  and  , and press  to confirm.






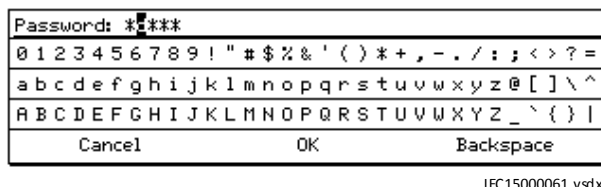
IEC12000161-3-en.vsd

Figure 67: Selecting the user name

4. Select **OK** on the on-screen keyboard and press  to stop editing the user name.
5. Press  to select the Password field and press  to activate it.  
An on-screen keyboard is shown.

Each added character is shown for a short time, then hidden with an asterisk character '\*' to enhance security. You can end password editing at any time by pressing  while the

password field is focused (or navigate to the OK button and press ) to attempt to login, or press  (or navigate to the Cancel button and press ) to abort the login attempt.  
When the cursor is moved, the newly selected character is shown for a short time.



6. Type in the password using the on-screen keyboard.






*Figure 68: Entering the password*

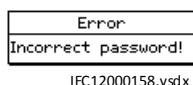


Passwords are case sensitive.



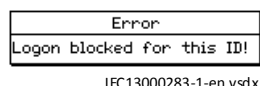
Only characters A - Z, a - z and 0 - 9 shall be used in user names. User names are not case sensitive. For passwords see the Password policies in PCM600.

7. Select **OK** on the on-screen keyboard and press  to stop editing the password.
8. Select **OK** in the **Log on** dialog and press  to confirm the login, or press  or Cancel to cancel the procedure.  
If the login fails, a message is displayed on the display.



*Figure 69: Error message indicating an incorrect password*

If a false password is entered three times, the login is blocked for that ID and the following message is displayed:



*Figure 70: Error message indicating blocked ID*





The logon dialog appears if the attempted operation requires another level of user rights.



Once a user is created and written into the IED, login is possible with the password assigned in the tool. If there is no user created, an attempt to login causes the display to show a corresponding message.

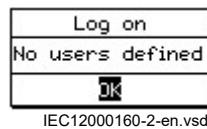


Figure 71: No user defined

## 7.2 Logging off

The user is automatically logged off after the display timeout. The IED returns to a state where only reading is enabled. Manual logoff is also possible.

1. Press .
2. To confirm logoff, select **Yes** and press .

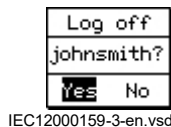


Figure 72: Logging off

- To cancel logoff, press .

## 7.3 Saving settings

Editable values are stored in the nonvolatile flash memory. Most of the parameter changes take effect immediately after storing, but some parameter changes require application restart. Values stored in the flash memory remain in effect also after reboot.

1. Press to confirm any changes.
2. Press to move upwards in the menu tree or to enter the Main Menu.
3. To save the changes in nonvolatile memory, select **Yes** and press .
  - To exit without saving changes, select **No** and press .
  - To cancel saving settings, select **Cancel** and press .



Pressing **Cancel** in the Save changes dialog closes only the Save changes dialog box, but the IED remains in the editing mode. All the changes applied to any setting are not lost, and changing settings can continue. To leave the change setting mode, select **No** or **Yes** in the Save changes dialog.



After changing the parameters marked with the exclamation mark “!”, the IED restarts automatically for the changes to take effect.

## 7.4 Recovering password



This section is only valid for PCM600 users. For Central Account Management users, the administrator should reset the password in the Central Account Management server (SDM600).

In case of password loss or any other file system error that prevents the IED from working properly, the whole file system can be restored to IED default state. All the default settings and configuration files stored in the IED at the factory are restored. One important usage of this menu is to disable the authority system. This can be used to recover an IED where the user-defined passwords are lost

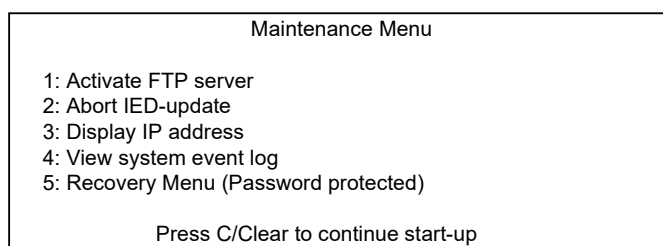
It is possible to disable the Maintenance menu. This is done by setting the parameter *MaintMenuEnable* to *No* in the Group *AUTHMAN: 1* using the **Parameter settings** in PCM600.



If the Maintenance menu is disabled, there is no way to bypass authority if passwords are forgotten. To be able to do field updating; the maintenance menu have to be re-enabled.

To enter this menu, the IED must be rebooted and a specific key combination must be pressed on the LHMI during the IED boot sequence.

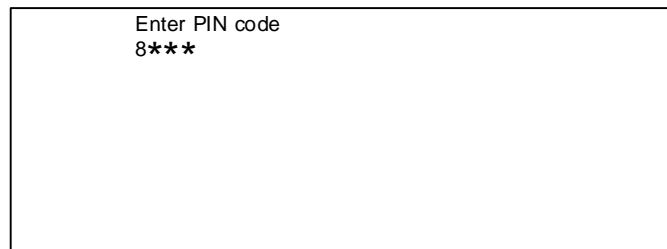
1. Switch off the power supply to the IED and leave it off for one minute.
2. Switch on the power supply to the IED and press and hold down and until the Maintenance Menu appears on the LHMI (this takes around 20-60s).
3. Navigate down and select **Recovery Menu** and press or .



IEC12000168-3-en.vsd

Figure 73: Select Recovery menu

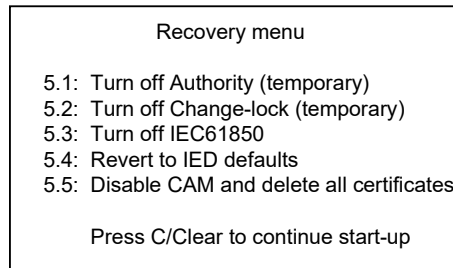
4. Enter PIN code 8282 and press .



IEC13000036-3-en.vsd


*Figure 74: Enter PIN code*

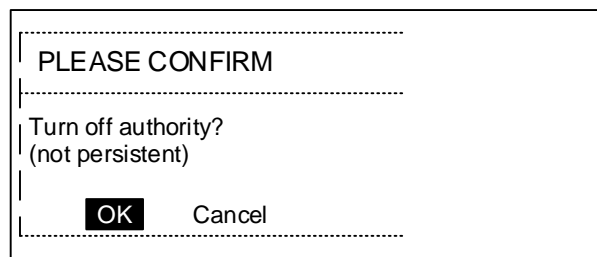
5. Select **Turn off authority** and press  or .



IEC12000170-3-en.vsd

*Figure 75: Turn off Authority*


6. Select **OK** to turn off the authority and press .



IEC12000169-3-en.vsd

*Figure 76: Confirm selection*

In a Central Account Management enabled IED, the IED will be set to default after "Turn off authority". For an IED with local account management, the below sequence is applicable.

7. Press  to continue the startup sequence, (now the authority is temporarily disabled until next reboot of the IED).

To cancel the operation in any step, press .

Open PCM600 and start the IED Users tool.

- Remove the faulty user
- Create a new user with the same access rights
- Write the user management settings to the IED

The IED perform a reboot, new settings are activated and the authority system is enabled again.



The Maintenance Menu is only available on the Local HMI. The purpose of this menu is to have a way to recover in the field at different situations. The recovery menu is also protected with a 4–digit PIN code, fixed for all IEDs.



Avoid unnecessary restoring of factory IED default setting (*Revert to IED defaults*), since all parameter settings earlier written to the IED are overwritten with factory default values.



When *Revert to IED defaults* is selected the IED restores the factory IED default settings and restarts. Restoring can take several minutes. Confirmation of the restored factory IED default settings is shown on the display for a few seconds, after which the IED restarts.

## 7.5 Fallback access

There exist a fallback solution, to access the IED via Maintenance menu. Since the Maintenance menu requires direct access to the IED and a restart of the device, this will be reported in the system.

In the Maintenance menu there are two options:

- Temporarily disable authentication until next reboot of the device. This is also applicable for local account management IEDs.
- Delete Certificates, Disable CAM? according to above. This will delete all certificates in the IED and disables Central Account Management. It is persistent and Central Account Management deployment has to be done again in the IED.

For customers that do not allow any fallback, this fallback functionality can be disabled by setting parameter *MaintMenuDisAuth* in: **Main Menu/Configuration/Communication/Cyber security/AuthMan:1**



When the IED is reverted to IED defaults through Maintenance menu, the certificates will be deleted.

## Section 8 Standard compliance statement

### 8.1 Applicable standards

Cyber security issues have been the subject of standardization initiatives by ISA, IEEE, or IEC for some time and ABB plays an active role in all these organizations, helping to define and implement cyber security standards for power and industrial control systems.

Some of the cyber security standards which are most important for substation automation are still under active development such as IEC62351 and IEC62443 (former ISA S99). ABB is participating in the development by delegating subject matter experts to the committee working on the respective standard. Since these standards are still under development ABB strongly recommends to use existing common security measures as available on the market, for example, VPN for secure Ethernet Communication.

An overview of applicable security standards and their status is shown in Table 22:

Table 22: Overview of cyber security standards

| 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                |

\* Ongoing: major changes will affect the final solution.

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, IEEE1686, as well as local activities like the German BDEW white paper.

The two standards IEC 62351 and IEC 62443 are still under revision. Due to interoperability reasons ABB recommend not to implement these standards yet. Nevertheless, ABB considers these standards already today as a guideline to implement product features or system architectures.

## 8.2 IEEE1686 compliance

Table 23: IEEE1686 compliance

| Clause                       | Title  | Status      | Comment   |
|------------------------------|--|-------------|---|
| 5                            | IED cyber security features                          | Acknowledge |   |
| 5.1                          | Electronic access control                            | Acknowledge |   |
| 5.1.1                        | IED access control overview                          | Comply      | Access is protected for local access through control panel. Access is protected for local access through communication / diagnostic ports. Access is protected for remote access through a communication media  |
| 5.1.2                        | Password defeat mechanisms                           | Comply      |   |
| 5.1.3                        | Number of individual users                           | Exceed      | 20 unique ID/password combinations are supported (only applicable in Local User Account Management)   |
| 5.1.4                        | Password construction                                | Comply      | The minimum enforced password length is configurable. If password policy is enforced, minimum is 6. Use of mix of lower and UPPERCASE characters is enforced, configurable in password policies Use of numerical values is enforced, configurable in password policies. Use of non-alphanumeric character (e.g. @, #, %, &, *) is enforced, configurable in password policies. When Central Account Management is active the password policy is not defined in the IED. |
| 5.1.5                        | IED access control                                   | Acknowledge |   |
| 5.1.5.1                      | Authorization levels by password                     | Comply      |   |
| 5.1.5.2                      | Authorization using role-based access control (RBAC) | Exceed      | IED provides 8 user-defined roles.  |
| 5.1.6                        | IED main security functions                          | Acknowledge |   |
| 5.1.6 a)                     | View data  | Comply      | Feature is accessible through individual user accounts.   |
| 5.1.6 b)                     | View configuration settings                          | Comply      | Feature is accessible through individual user accounts.   |
| 5.1.6 c)                     | Force values   | Comply      | Feature is accessible through individual user accounts.   |
| 5.1.6 d)                     | Configuration change                                 | Comply      | Feature is accessible through individual user accounts.   |
| 5.1.6 e)                     | Firmware change                                      | Comply      | Feature is accessible through individual user accounts.   |
| 5.1.6 f)                     | ID/password or RBAC management                       | Comply      | Feature is accessible through individual user accounts.   |
| Table continues on next page |  |             |   |

| Clause   | Title  | Status      | Comment  |
|----------|--|-------------|--|
| 5.1.6 g) | Audit log  | Comply      | Feature is accessible through individual user accounts.                      |
| 5.1.7    | Password display                                     | Comply      |  |
| 5.1.8    | Access time-out                                      | Comply      | A time-out feature exists. The time period is configurable by the user.      |
| 5.2      | Audit trail  | Acknowledge |  |
| 5.2.1    | Audit trail background                               | Comply      | The Audit log can be viewed through PCM 600                                  |
| 5.2.2    | Storage capability                                   | Comply      |  |
| 5.2.3    | Storage record                                       | Comply      |  |
| 5.2.3 a) | Event record number                                  | Comply      |  |
| 5.2.3 b) | Time and date  | Comply      |  |
| 5.2.3 c) | User identification                                  | Comply      |  |
| 5.2.3 d) | Event type   | Comply      |  |
| 5.2.4    | Audit trail event types                              | Acknowledge |  |
| 5.2.4 a) | Login  | Comply      |  |
| 5.2.4 b) | Manual logout  | Comply      |  |
| 5.2.4 c) | Timed logout   | Comply      |  |
| 5.2.4 d) | Value forcing  | Comply      |  |
| 5.2.4 e) | Configuration access                                 | Exception   |  |
| 5.2.4 f) | Configuration change                                 | Comply      |  |
| 5.2.4 g) | Firmware change                                      | Comply      |  |
| 5.2.4 h) | ID/password creation or modification                 | Comply      |  |
| 5.2.4 i) | ID/password deletion                                 | Comply      |  |
| 5.2.4 j) | Audit-log access                                     | Comply      |  |
| 5.2.4 k) | Time/date change                                     | Comply      |  |
| 5.2.4 l) | Alarm incident                                       | Comply      |  |
| 5.3      | Supervisory monitoring and control                   | Acknowledge |  |
| 5.3.1    | Overview of supervisory monitoring and control       | Comply      | Made available through IEC 61850 and syslog                                  |
| 5.3.2    | Events   | Exception   | Time/date change and configuration access not reported; Otherwise compliance |
| 5.3.3    | Alarms   | Acknowledge |  |
| 5.3.3 a) | Unsuccessful login attempt                           | Comply      |  |
| 5.3.3 b) | Reboot   | Comply      | A start-up event is created every boot                                       |
| 5.3.3 c) | Attempted use of unauthorized configuration software | Exception   | Client certificates are not in use   |
| 5.3.3 d) | Invalid configuration or firmware download           | Comply      |  |
| 5.3.3 e) | Unauthorized configuration or firmware file          | Exception   | Not supported  |

Table continues on next page

| Clause                       | Title                               | Status      | Comment   |
|------------------------------|-------------------------------------|-------------|---|
| 5.3.3 f)                     | Time signal out of tolerance        | Exception   | IED validates the time synchronization messages but it does not alarm if message is not within the tolerances of the IED's clock            |
| 5.3.3 g)                     | Invalid field hardware changes      | Comply      | IED send a hardware changed detected alarm.   |
| 5.3.4                        | Alarm point change detect           | Comply      |   |
| 5.3.5                        | Event and alarm grouping            | Exception   | Not supported   |
| 5.3.6                        | Supervisory permissive control      | Exception   | Not supported   |
| 5.4                          | IED cyber security features         | Acknowledge |   |
| 5.4.1                        | IED functionality compromise        | Comply      | Services and ports used for real-time protocols are listed in the user documentation.   |
| 5.4.2                        | Specific cryptographic features     | Exception   | File transfer functionality provided by the IED user File transfer protocol over TLS.   |
| 5.4.2 a)                     | Webserver functionality             | Comply      | Feature not supported   |
| 5.4.2 b)                     | File transfer functionality         | Exception   | File transfer protocol over TLS   |
| 5.4.2 c)                     | Text-oriented terminal connections  | Comply      | Feature not supported   |
| 5.4.2 d)                     | SNMP network management             | Comply      | Feature not supported   |
| 5.4.2 e)                     | Network time synchronization        | Comply      |   |
| 5.4.2 f)                     | Secure tunnel functionality         | Comply      | Feature not supported   |
| 5.4.3                        | Cryptographic techniques            | Comply      | Recommendation from the NIST Computer Security Division are taken into account in the cryptographic techniques implemented by the IED       |
| 5.4.4                        | Encrypting serial communications    | Comply      | Feature not supported   |
| 5.4.5                        | Protocol-specific security features | Comply      |   |
| 5.5                          | IED configuration software          | Acknowledge |   |
| 5.5.1                        | Authentication                      | Exception   | IED can be configured using unauthorized copies of the configuration software. However configuration download is handled by authentication. |
| 5.5.2                        | Digital signature                   | Exception   | Feature not supported   |
| 5.5.3                        | ID/password control                 | Comply      | Stored in the IED.  |
| 5.5.4                        | ID/password controlled features     | Comply      |   |
| 5.5.4.1                      | View configuration data             | Comply      |   |
| Table continues on next page |                                     |             |   |



| Clause  | Title                      | Status    | Comment   |
|---------|----------------------------|-----------|---|
| 5.5.4.2 | Change configuration data  | Comply    |   |
| 5.6     | Communications port access | Comply    |   |
| 5.7     | Firmware quality assurance | Exception | Quality control is handled according to ISO9001 and CMMI. |



## Section 9

## Glossary

|                    |  |
|--------------------|--|
| <b>AES</b>         | Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of cycles of repetition are as follows: 10 cycles of repetition for 128-bit keys. 12 cycles of repetition for 192-bit keys. 14 cycles of repetition for 256-bit keys. |
| <b>AGSAL</b>       | Generic security application   |
| <b>ANSI</b>        | American National Standards Institute  |
| <b>ASCII</b>       | American Standard Code for Information Interchange (ASCII) is a character-encoding scheme originally based on the English alphabet. ASCII codes represent text in computers, communications equipment, and other devices that use text.  |
| <b>CA</b>          | In cryptography, certificate authority, or certification authority, (CA) is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate  |
| <b>CAM</b>         | Central Account Management. User, roles and rights are handled in a Central Account Management server.   |
| <b>CMT</b>         | Communication Management tool in PCM600  |
| <b>CPU</b>         | Central processor unit   |
| <b>CRC</b>         | Cyclic redundancy check  |
| <b>DARPA</b>       | Defense Advanced Research Projects Agency (The US developer of the TCP/IP protocol etc.)   |
| <b>DHCP</b>        | Dynamic Host Configuration Protocol  |
| <b>DNP3</b>        | DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies. It plays a crucial role in SCADA systems, where it is used by SCADA Master Stations (aka Control Centers), Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs). It is primarily used for communications between a master station and RTUs or IEDs'. |
| <b>EMC</b>         | Electromagnetic compatibility  |
| <b>EN 50263</b>    | Electromagnetic compatibility (EMC) - Product standard for measuring relays and protection equipment.  |
| <b>EN 60255-26</b> | Electromagnetic compatibility (EMC) - Product standard for measuring relays and protection equipment.  |
| <b>EN 60255-27</b> | Electromagnetic compatibility (EMC) - Product standard for measuring relays and protection equipment.  |
| <b>ESD</b>         | Electrostatic discharge  |
| <b>FTP</b>         | File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host or to another host over a TCP-based network, such as the Internet.  |
| <b>FTPS</b>        | FTPS (also known as FTP-ES, FTP-SSL and FTP Secure) is an extension to the commonly used File Transfer Protocol (FTP) that adds support for the  |

|                            |   |
|----------------------------|---|
|                            | Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols.  |
| <b>GDE</b>                 | Graphical display editor within PCM600  |
| <b>GOOSE</b>               | Generic object-oriented substation event  |
| <b>GPS</b>                 | Global positioning system   |
| <b>GSM</b>                 | GPS time synchronization module   |
| <b>GTM</b>                 | GPS Time Module   |
| <b>HMI</b>                 | Human-machine interface   |
| <b>ID</b>                  | IDentification  |
| <b>IEC</b>                 | International Electrical Committee  |
| <b>IEC 60255</b>           | This standard specifies the general performance requirements of all electrical measuring relays and protection equipment used in the electrotechnical fields covered by the IEC.  |
| <b>IEC 60870-5-103</b>     | Communication standard for protective equipment. A serial master/slave protocol for point-to-point communication  |
| <b>IEC 61850</b>           | Substation automation communication standard  |
| <b>IEC 61850-8-1</b>       | Communication protocol standard   |
| <b>IED</b>                 | Intelligent electronic device   |
| <b>IEDUM</b>               | IED User Management   |
| <b>IEEE</b>                | Institute of Electrical and Electronics Engineers   |
| <b>IEEE 1344</b>           | A standard that defines parameters for synchrophasors for power systems. The standard also added extension to the IRIG-B time code to cover year, time quality, daylight saving time, local time offset and leap second information. IEEE 1344 was published in 1994 and was superseded by IEEE C37.118 in 2005 and the time extensions were adopted as part of the IRIG timing standard in the 2004 edition. |
| <b>IEEE 1686</b>           | Standard for Substation Intelligent Electronic Devices (IEDs') Cyber Security Capabilities  |
| <b>IEEE C37.118-2005</b>   | IEEE standard for synchrophasors for power systems. The standard was published in 2006 and a new version of the standard was published in December 2011 which split the IEEE C37.118-2005 into IEEE C37.118.1-2011 and IEEE C37.118.2-2011.   |
| <b>IEEE C37.118.1-2011</b> | IEEE standard for synchrophasor measurements for power systems. IEEE C37.118.1-2011 is superseded by IEEE C37.118.1a-2014.  |
| <b>IEEE C37.118.2-2011</b> | IEEE standard for synchrophasor data transfer for power systems.  |
| <b>IP</b>                  | 1. Internet protocol. The network layer for the TCP/IP protocol suite widely used on Ethernet networks. IP is a connectionless, best-effort packet-switching protocol. It provides packet routing, fragmentation and reassembly through the data link layer.<br>2. Ingression protection, according to IEC standard   |
| <b>IP 20</b>               | Ingression protection, according to IEC standard, level 20  |
| <b>ISO 9001</b>            | Set of standards for quality management.  |
| <b>IT</b>                  | Information technology  |
| <b>KEK</b>                 | key encryption key. Key used to protect other keys (e.g. TEK, TSK).   |
| <b>LAN</b>                 | Local area network  |
| <b>LED</b>                 | Light-emitting diode  |

|                   |  |
|-------------------|--|
| <b>LHMI</b>       | Local Human Machine Interface, also Local HMI.   |
| <b>MicroSCADA</b> | System for supervision, control and data acquisition   |
| <b>NCC</b>        | National Control Centre  |
| <b>ODBC</b>       | Open Database Connectivity is a standard for accessing database management systems (DBMS).   |
| <b>PC</b>         | Personal Computer  |
| <b>PCI</b>        | Peripheral component interconnect, a local data bus  |
| <b>PCM600</b>     | Protection and control IED manager   |
| <b>PIN</b>        | Personal Identification Number   |
| <b>PKCS#12</b>    | Archive file format of the Public-Key Cryptography Standards for bundle all the member of a chain of trust   |
| <b>PST</b>        | Parameter setting tool within PCM600   |
| <b>RTU</b>        | Remote terminal unit   |
| <b>SA</b>         | Substation Automation  |
| <b>SCADA</b>      | Supervision, control and data acquisition, see also MicroSCADA   |
| <b>SCT</b>        | System configuration tool according to standard IEC 61850  |
| <b>SHA</b>        | The Secure Hash Algorithm is a family of cryptographic hash functions. The SHA 2 family comprise two similar hash functions, with different block sizes, known as SHA-256 and SHA-512.   |
| <b>SMT</b>        | Signal matrix tool within PCM600   |
| <b>SNTP</b>       | Simple network time protocol – is used to synchronize computer clocks on local area networks. This reduces the requirement to have accurate hardware clocks in every embedded system in a network. Each embedded node can instead synchronize with a remote clock, providing the required accuracy.  |
| <b>SPA</b>        | Strömberg protection acquisition, a serial master/slave protocol for point-to-point communication  |
| <b>TLS</b>        | Transport Layer Security (TLS) is a cryptographic protocol that provides communication security over the Internet. TLS encrypt the segments of network connections at the Application Layer for the Transport Layer, using asymmetric cryptography for key exchange, symmetric encryption for confidentiality, and message authentication codes for message integrity.   |
| <b>Syslog</b>     | Syslog is a standard for computer data logging. Syslog can be used for computer system management and security auditing as well as generalized informational, analysis, and debugging messages   |
| <b>TCP</b>        | Transmission control protocol. The most common transport layer protocol used on Ethernet and the Internet.   |
| <b>TCP/IP</b>     | Transmission control protocol over Internet Protocol. The de facto standard Ethernet protocols incorporated into 4.2BSD Unix. TCP/IP was developed by DARPA for Internet working and encompasses both network layer and transport layer protocols. While TCP and IP specify two protocols at specific protocol layers, TCP/IP is often used to refer to the entire US Department of Defense protocol suite based upon these, including Telnet, FTP, UDP and RDP. |
| <b>UDP</b>        | The User Datagram Protocol (UDP) is one of the core members of the Internet protocol suite. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an   |

Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths.

**UMT**

User management tool

**UTC**

Coordinated Universal Time. A coordinated time scale, maintained by the Bureau International des Poids et Mesures (BIPM), which forms the basis of a coordinated dissemination of standard frequencies and time signals. UTC is derived from International Atomic Time (TAI) by the addition of a whole number of "leap seconds" to synchronize it with Universal Time 1 (UT1), thus allowing for the eccentricity of the Earth's orbit, the rotational axis tilt (23.5 degrees), but still showing the Earth's irregular rotation, on which UT1 is based. The Coordinated Universal Time is expressed using a 24-hour clock, and uses the Gregorian calendar. It is used for aeroplane and ship navigation, where it is also sometimes known by the military name, "Zulu time." "Zulu" in the phonetic alphabet stands for "Z", which stands for longitude zero.

**VPN**

A Virtual Private Network (VPN) extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if it were a private network with all the functionality, security and management policies of the private network.



---

**ABB AB**

**Substation Automation Products**

SE-721 59 Västerås, Sweden

Phone +46 (0) 21 32 50 00

[www.abb.com/substationautomation](http://www.abb.com/substationautomation)



Scan this QR code to visit our website