ABB ABILITY™ SMART SUBSTATION CONTROL AND PROTECTION FOR ELECTRICAL SYSTEMS

SSC600
Cyber Security Deployment Guideline

Document ID: 1MRS759013
Issued: 2022-11-30
Revision: E
Product version: 1.0 FP4

Copyright

Disclaimer

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

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

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

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

Conformity

This product complies with the directive of the Council of the European Communities on the approximation of the laws of the Member States relating to electromagnetic compatibility (EMC Directive 2014/30/EU) and concerning electrical equipment for use within specified voltage limits (Low Voltage Directive 2014/35/EU). This conformity is the result of tests conducted by 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 and IEC 61805-3:2013.

Contents

1   Introduction

1.1   This manual

The cyber security deployment guideline describes the process for handling cyber security when communicating with the ABB Ability™ Smart Substation Control and Protection for electrical systems SSC600 and SSC600 SW. The cyber security deployment guideline provides information on how to secure the system on which the protection device is installed. The guideline can be used as a technical reference during the engineering phase, installation and commissioning phase, and during normal service.

1.2   Intended audience

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

- Protection and control relays, gateways and Windows workstations
- Networking, including Ethernet and TCP/IP with its concept of ports and services
- Security policies
- Firewalls
- Antivirus protection
- Application whitelisting
- Secure remote communication

1.3 Product documentation

1.3.1 Product documentation set
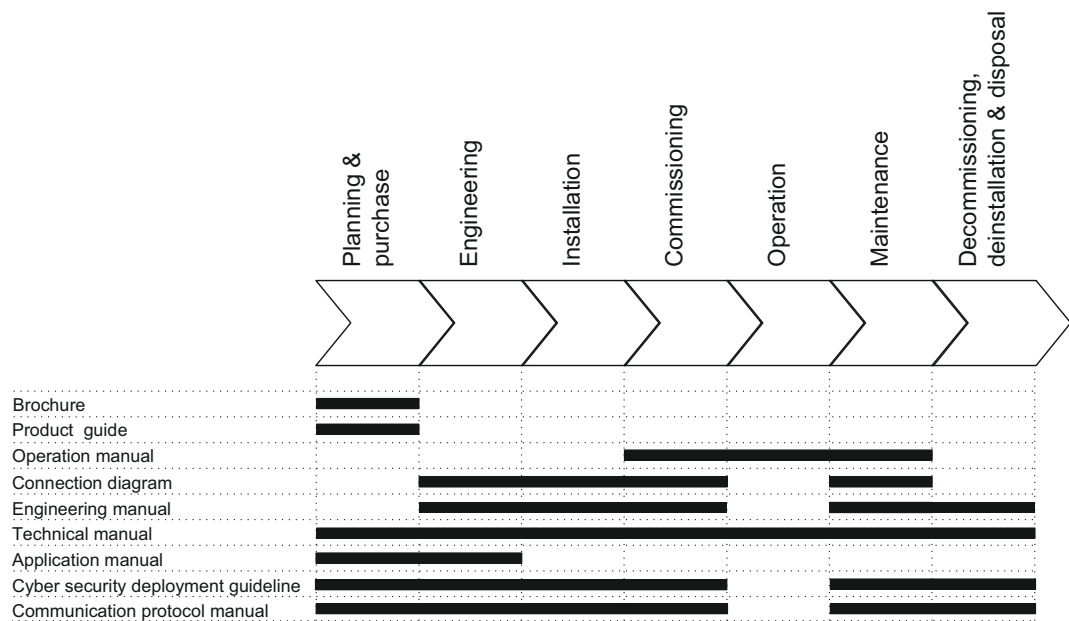
Figure 1: The intended use of documents during the product life cycle

> Product series- and product-specific manuals can be downloaded from the ABB Web site.

1.3.2 Document revision history

Document revision/date	Product series version	History
A/2019-05-13	1.0	First release
B/2020-03-10	1.0 FP1	Content updated
C/2020-09-11	1.0 FP2	Content updated
D/2021-11-08	1.0 FP3	Content updated
E/2022-11-30	1.0 FP4	Content updated to correspond to the product connectivity level

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

1.3.3 Related documentation

Product series- and product-specific manuals can be downloaded from the ABB Web site *www.abb.com/mediumvoltage*.

1.4 Symbols and conventions

1.4.1 Symbols

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

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

1.4.2 Document conventions

A particular convention may not be used in this manual.

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

  Select **Main menu** > **Settings**.
- Parameter names are shown in italics

  The function can be enabled and disabled with the *Operation* setting.
- Parameter values are indicated with quotation marks.

  The corresponding parameter values are "On" and "Off".
- Input/output messages and monitored data names are shown in Courier font.

  When the function starts, the `START` output is set to TRUE.
- This document assumes that the parameter setting visibility is "Advanced".

2 Security in distribution automation

2.1 General security in distribution automation

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

The new generation of automation systems uses open standards such as IEC 60870-5-104, DNP3 and IEC 61850 and commercial technologies, in particular Ethernet and TCP/IP based communication protocols. They also enable connectivity to external networks, such as office intranet systems and the Internet. These changes in technology, including the adoption of open IT standards, have brought huge benefits from an operational perspective, but they have also introduced cyber security concerns previously known only to office or enterprise IT systems.

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

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

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

2.2   Reference documents

Information security in critical infrastructure like electrical distribution and transmission networks has been in high focus for both vendors and utilities. This together with developing technology, for example, appliance of Ethernet and IP based communication networks in substations, power plants and network control centers creates a need of specifying systems with cyber security.

ABB is involved in the standardization and definition of several cyber standards, the most applicable and referred ones are ISO 2700x, IEC 62443, IEEE P1686 and IEC 62351. Besides standardization efforts there are also several governments initiated requirements and practices like NERC CIP and BDEW. ABB fully understands the importance of cyber security for substation automation systems and is committed to support users in efforts to achieve or maintain compliance to these.

3 Secure system setup

3.1 Basic system hardening rules

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

- Recognizing and familiarizing all parts of the system and the system's communication links
- Removing all unnecessary communication links in the system
- Rating the security level of remaining connections and improving with applicable methods
- Consider the physical security of the assets, e.g. protection devices, removable media and communication cables
- Hardening the system by removing or deactivating all unused processes, communication ports and services
- Checking that the whole system has backups available from all applicable parts
- Collecting and storing backups of the system components and keeping those up-to-date
- Removing all unnecessary user accounts
- Changing default passwords and using strong enough passwords
- Checking that the link from substation to upper level system uses strong enough encryption and authentication
- Separating public network from automation network
- Segmenting traffic and networks including virtualization environment when using SSC600 SW
- Using firewalls and demilitarized zones
- Assessing the system periodically
- Using antivirus software in workstations and keeping those up-to-date
- Keeping software components up-to-date. Including SSC600 and related environment, e.g. hypervisors.

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

When using SSC600 SW, hypervisor hardening should be considered. Best practices related to the chosen hypervisor should be followed. SSC600 SW hardening follows the same practices as SSC600.

3.2 Device communication interfaces

All physical ports dedicated for station bus and process bus communication except local port can be opened and closed in device configuration. Local port is used for engineering and it can be used only for point-to-point configuration access with PCM600 or WHMI. Local port should not be connected to any Ethernet network.

Table 1: Physical ports on device's communication cards

Port ID	Type	Default state	Description
LAN1	RJ-45	Enabled	Local port
LAN2	RJ-45	Disabled	Remote port (for engineering)
LAN3	RJ-45 or fiber optic	Disabled	Process bus A
LAN4	RJ-45 or fiber optic	Disabled	Process bus B
LAN5	RJ-45	Enabled	Rear port
LAN6	RJ-45	Disabled	not in use
LAN7	RJ-45	Disabled	Service port
LAN8	RJ-45	Disabled	not in use

IEC 61850 protocol and LAN1 and LAN5 ports are by default activated as those are used for engineering of the protection device.

3.3 TCP/IP based protocols and used IP ports

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

The device supports an option with multiple station communication Ethernet ports. In this case, all ports use the same IP address regardless of what redundancy option is activated in the device configuration.

To set up an IP firewall the following table summarizes the IP ports used by the device. Ports which are by default open are used for configuring the protection device.

Table 2: IP ports used by the device

Port number	Type	Default state	Description
20, 21	TCP	Open	File Transfer protocol (FTPS)
102	TCP	Open	IEC 61850
80, 443	TCP	Open	Web Server HTTPS
5001	TCP	Open	Firmware upgrade using HTTPS, user account management and certificate updates.
2404	TCP	Closed	IEC 60870-5-104 TCP
67	UDP	Open	DHCP server at LAN1 and LAN2

FTPS and IEC 61850 are primary services needed for device configuration and those cannot be disabled. Additionally, the protection device uses R-GOOSE (IP/UDP multicast) and layer 2 communications in GOOSE, SMV, IEEE 1588 (PTP) and PRP supervision services, which needs to be considered when designing the network.

In addition to the HTTPS and FTPS protocols, the device supports the IEC 61850 Ethernet-based substation automation communication protocol. IEC 61850 is always enabled.

3.4   Secure communication

The protection device supports encrypted communication according to the principles of IEC 62351 in secured communication for WHMI and file transfer. *Secure Communication* is enabled by default and protocols therefore require TLS protocol based encryption method support from the clients. In this case WHMI must be connected from a Web browser using the HTTPS protocol. In case of file transfer, the client must use FTPS. PCM600 supports FTPS and is able to download and upload configuration files in encrypted communication channel from device. Some industry related protocols such as IEC 60870-5-104 and MMS are implemented according to the respective standards without secure communication. It's essential to consider hardening as described in *Chapter 3.1 Basic system hardening rules*.

3.4.1   Certificate handling

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

Certificates use encryption to provide secure communication over the network. A self-signed X.509 certificate and an RSA key-pair with key-length of 2048 bits is generated by the protection device. The RSA key stored in the certificate is used to establish secure communication.

The certificate is used to verify that a public key belongs to an identity. In case of HTTPS, the WHMI server in the protection device presents the certificate to the Web client giving the client the public key and the identity of the server. The

public key is one part of an asymmetric key algorithm in which one key is used to encrypt a message and another key is used to decrypt it. The public private key pair (asymmetric key) is used to exchange the symmetric key, which is used to encrypt and decrypt the data that is exchanged between server and client.

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

Once the protection device certificate has been manually trusted in a separate dialog box, the certificate is trusted in communication between the device and PCM600. For WHMI use, the certificate signed by the protection device must be accepted in the Web browser when opening the connection to WHMI.

> Web browser displays a warning because WHMI uses self-signed certificates.

3.4.2 Uploading a Certificate

- External Certificate:

  By default, SSC600 supports self-signed certificate-based communication security feature. For enhanced security it also supports certificate signed by a trusted certificate authority. External certificate update supports manual import of third-party trusted certificates.

- Methodology:

  SSC600 can use any certificate in .p12 format. Certificates are taken in use with SSC600. Detailed information about writing the certificates to SSC600 is documented in "PCM600 User Guide".
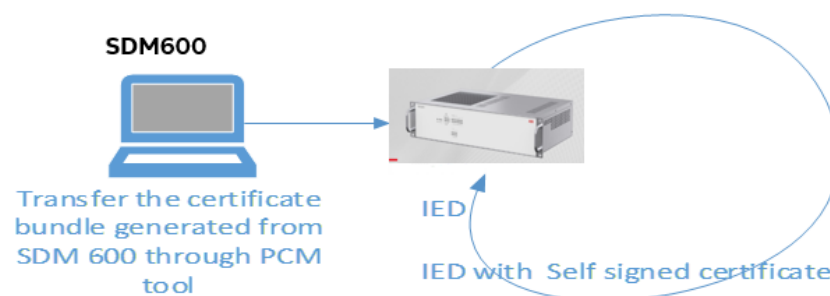
> Initially SSC600 device works with a self-signed certificate. Once it receives trusted certificate, it authorizes the device with the external certificate.

- Certificate Extraction:

  Certificate bundle (.p12) imported to SSC600 and Certificates are Extracted and then uploaded to SSC600.
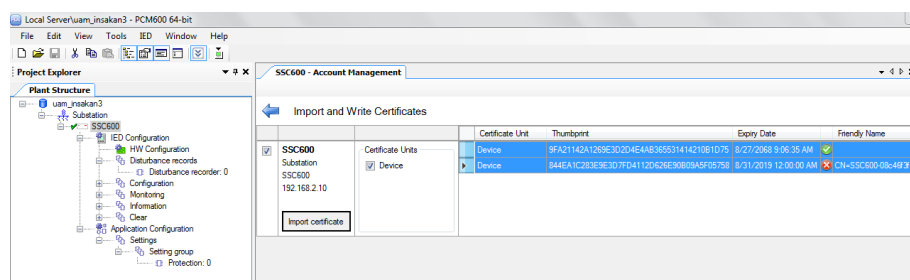
- Certificate update can be verified on WHMI of the device, by clicking the lock icon on the left side of the address bar (though there are small differences between browsers).

3.4.3 Encryption algorithms

TLS connections are encrypted with either AES 256 or AES 128 ciphers. At start-up 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 512 is stored in the IED. These are not accessible from outside via any ports.

3.5 Web HMI

The WHMI is the only user access service in the protection device. To provide encryption and secure identification in the communication to the WHMI, the device supports HTTPS protocol. In this case plain HTTP connection request is automatically changed to HTTPS.

The WHMI requires a modern web browser, with support for HTML5 and ECMAScript 6. Note that Internet Explorer is not supported. Secure communication is required, with TLS v1.2 or v1.3.

The WHMI is verified with latest versions of Microsoft Edge, Firefox and Google Chrome.

User authentication is always required in WHMI. After successful login, user needs to select the role with which they want to proceed.

4   User management

4.1   Local user account management

The user account management and role-based access control in the protection relay have been handled as specified in IEC 62351-8.

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

Table 3: Showing Four Factory Default Users, respective roles and respective default passwords

Four Factory Default Users	Role	Default Password
VIEWER	VIEWER	remote0001
OPERATOR	OPERATOR	remote0002
ENGINEER	ENGINEER	remote0003
ADMINISTRATOR	ADMINISTRATOR	remote0004

The default passwords in the protection relay delivered from the factory can be changed by user with User Management Right or the users themselves.

Relay user passwords can be changed using the WHMI or IED Users tool in PCM600.

Figure 2: Showing Change password option in WHMI (the users themselves can change from here)
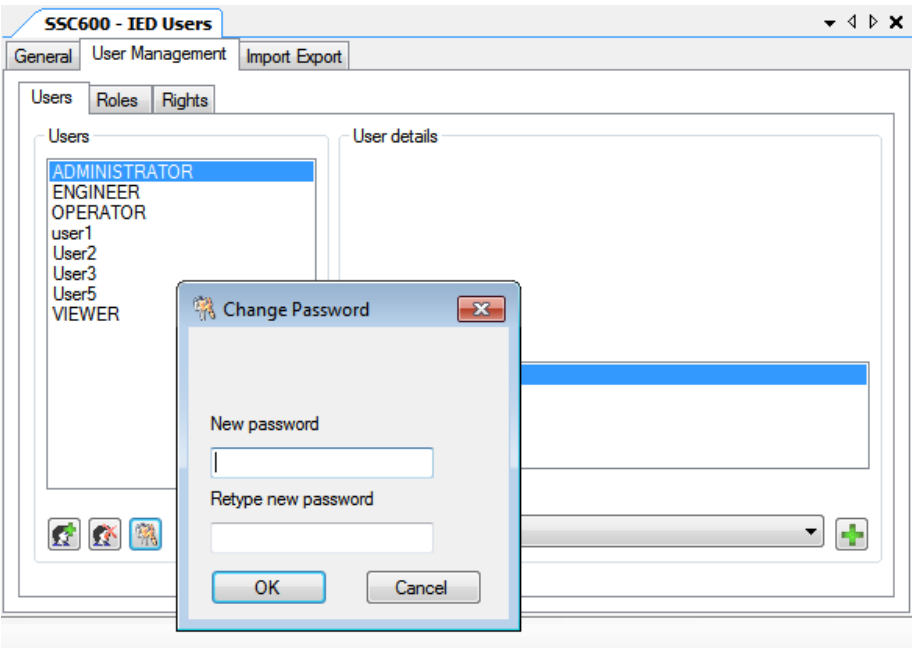
Figure 3: Showing Change password option in PCM600. (user with User Management Right can change from here)

In addition to the default user accounts, additional user accounts under eight predefined roles, can be added for the protection relay from IED Users in PCM600.
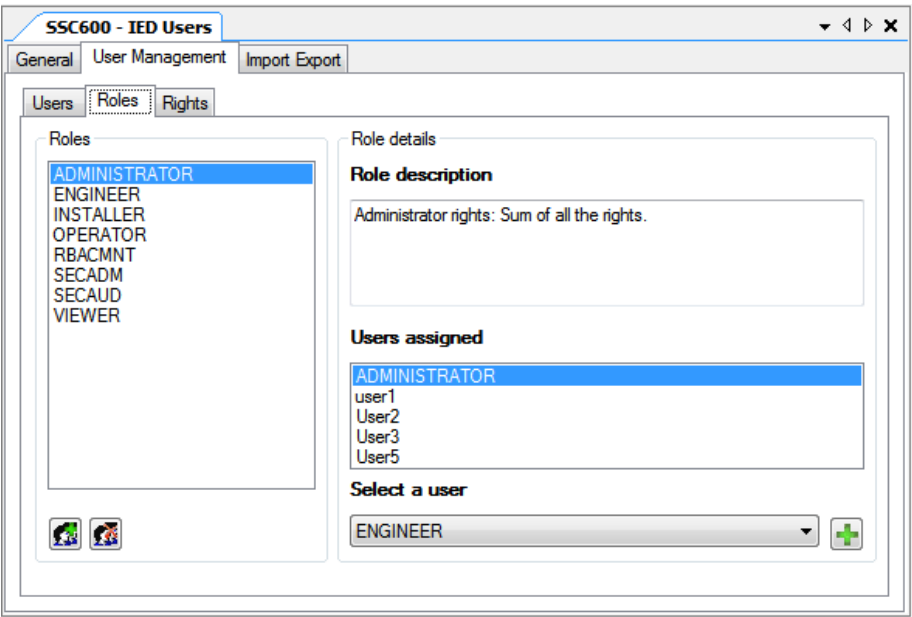

Figure 4: Showing Eight Pre-Defined Roles in PCM600

These roles are then mapped to user rights.
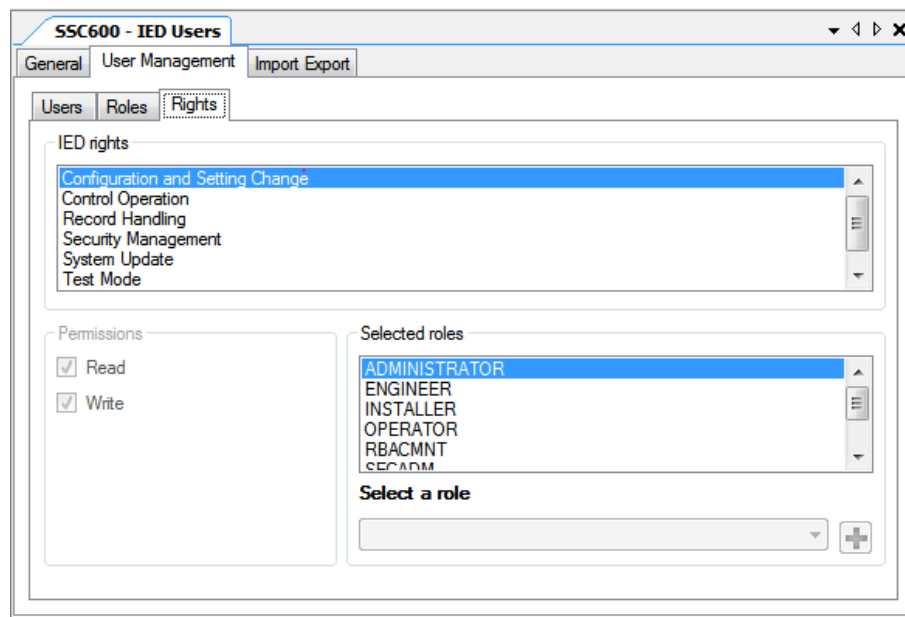
Figure 5: Showing roles to rights mapping

It is required to login as a user with role which is having User Management Right in PCM600 to be able to add additional pre-defined roles and map them to user rights. User defined roles can be added to protection relay.

Each protection relay supports eight fixed roles and 50 user accounts belonging to any one of these roles. Each user account can be mapped to a maximum of eight roles.

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

- User accounts can be created and assigned with any default roles (VIEWER, OPERATOR, ENGINEER and ADMINISTRATOR) or additional roles (INSTALLER, SECADM, SECAUD and RBACMNT)
- User with role (Role Mapped to User Management Right) can create user accounts and update the roles-to-rights mapping.
- User with role (Role Mapped to User Management Right) needs to share the default password generated for the user account by the tool with the users and recommend the user to change the password.
- The password of the user accounts can be changed by the users themselves from PCM600 or from WHMI.
- User with role (Role Mapped to User Management Right) can reset the passwords of the users.

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

Any user logging into the protection relay from WHMI (HTTPS) or PCM600 (FTPS) is authenticated based on the user account information in the relay.

Table 4: Pre-defined user roles

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

Table 5 describes the default mapping of all the user rights associated with all the roles in the protection relay. This mapping can be modified according to the user requirements.

Table 5: Default roles-to-rights mapping

Possible user actions / Rights	VIEWER	SECAUD	OPERATOR	INSTALLER	ENGINEER	RBACMNT	SECADM	ADMINISTRATOR
Configuration and Setting Change	No	No	No	No	Yes	No	No	Yes
Control Operations	No	No	Yes	No	No	No	No	Yes
User Management	No	No	No	No	No	Yes	Yes	Yes
Security Management	No	Yes	No	No	No	No	Yes	Yes
Test Mode	No	No	No	No	Yes	No	No	Yes

Table continues on the next page

Possible user actions / Rights	VIEWER	SECAUD	OPERATOR	INSTALLER	ENGINEER	RBACMNT	SECADM	ADMINISTRATOR
Record Handing	No	Yes	No	No	No	No	No	Yes
System up-date	No	No	No	No	No	No	Yes	Yes

The permissions and rights mentioned in the IEC 62351-8 standard are covered directly or by a combination of the rights mentioned in *Table 5*. In PCM600 the rights are managed as Read/Write/None instead of Yes/No. If None right is not applicable for an action (for example Test Mode), it will default to Read right.

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

WHMI always requires authentication. Changes in *User management* settings do not cause the protection relay to reboot. The changes are taken into use immediately after committing the changed settings on the menu root level.

Username and password are always required for communication with the relay over FTP/FTPS and HTTPS protocols.

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

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

4.1.1   Password policies

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

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

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

- Minimum password length: 9
- Maximum password length: 20
- Minimum uppercase characters: 0
- Minimum numeric: 0
- Minimum special characters: 0

The protection relays are delivered from the factory with default passwords. It is required to change the default passwords.

Table 6: Predefined roles and default passwords

Username	Password (remote clients/WHMI)
VIEWER	remote0001
OPERATOR	remote0002
ENGINEER	remote0003
ADMINISTRATOR	remote0004

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

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

It is required to login as a User (who has User Management Right) in PCM600 in order to change the password policies.

Each user can change their own password, but only User with User Management Right can reset the passwords of other users.

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

> ℹ️ For user authorization for PCM600, see the PCM600 documentation.

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

> ℹ️ If the last User with User Management Right password is lost, contact ABB's technical customer support.

5   Security logging

5.1   Audit trail

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

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

The protection device stores 2048 audit trail events to the nonvolatile audit trail. Additionally, 8192 process events are stored in a nonvolatile event list. Both the audit trail and event list work according to the FIFO principle. Nonvolatile memory is based on a memory type which does not need battery backup nor regular component change to maintain the memory storage.

Audit trail events related to user authorization (login, logout, violation remote and violation local) are defined according to the selected set of requirements from IEEE 1686. The logging is based on predefined user names or user categories. The user audit trail events are accessible with IEC 61850-8-1, PCM600 and WHMI.

> **i** Events which happen without authenticated user will be recorded with a generic username.

Table 7: Audit trail events

Event Id	Description	Severity
1110	Log-in successful	Event
1130	Log-in failed - Wrong credentials	Event
1210	Log-out (user logged out)	Event
1320	Downloaded / wrote configuration successfully	Event
1370	Viewed Security Event logs successfully	Alarm
1380	Parameter changed successfully	Event
1420	Download / writing configuration failed	Event
1520	Software updated successfully	Event
1610	Firmware change fail	Event
1710	Device reset to factory default	Event
2110	User account created successfully	Alarm
2120	User account deleted successfully	Alarm
2180	New role created successfully	Alarm

Table continues on the next page

Event Id	Description	Severity
2190	Role deleted successfully	Alarm
2210	User password changed successfully	Event
2220	Change of user password failed	Event
5110	Firmware Reset	Alarm
5140	Software reset	Alarm
5270	System startup	Alarm
6110	Test Mode started successfully	Alarm
6120	Test Mode ended successfully	Alarm
6130	Control operation performed successfully	Alarm
6220	Time Synchronized successfully	Event
6320	Time Synchronization failed	Event
8020	Date and time set successfully	Event
9020	Flooding attack detected	Alarm
13520	Certificates transferred to the device successfully	Event
14520	Failed to transfer certificates to the device	Event

PCM600 Event Viewer tool can be used to view the audit trail events and process related events. Audit trail events are visible through dedicated Security events view. Since, user with Security Management Right can read audit trail. The audit trail cannot be reset, but PCM600 Event Viewer can filter data. Audit trail events can be configured to be visible also in WHMI Event list together with process related events.

In WHMI, Audit trail events are displayed based on user rights. A user having Security Management right can view audit trail logs.

5.2 Central Activity Logging

The audit trail events can be reported from the relay to a Central Activity Logging (CAL) server in Syslog format. The relay is the CAL client and it sends the events to a CAL server which can be SDM600 or any other tool capable of handling the Syslog format.

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

Table 8: Configuring Central Activity Logging

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

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

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

> For the overall system security, it's important to ensure secure communication between SSC600 and CAL server. More information about system hardening can be found in *Chapter 3.1 Basic system hardening rules*.

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

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

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

> The protection relay supports Syslog version 1.

6   Using the Web HMI

As secure communication is enabled by default, the WHMI must be accessed from a Web browser using the HTTPS protocol. Log in with the proper user rights to use the WHMI.

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

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

6.1   Logging in

1. Open a supported web browser.
2. Type the IED's IP address in the Address bar and press ENTER.
3. Type the username with capital letters.
4. Type the password.

Figure 6: Entering username and password to use the WHMI

5. Click **OK**.
6. Select role to be used from the list of available users. In case there is only one role available, it will be automatically selected.

6.2   Logging out

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

*   To log out manually, select **Logout** in the View bar.

7 Protection of device and system configuration

7.1 Backup files

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

7.1.1 Creating a backup from the device configuration

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

      User authorization is needed before using the tool.

2. Enter the user credentials if the default administrator password has been changed.
    Credentials of a user with "Configuration Settings" right are required for authorization.

### 7.1.2 Creating a backup from the PCM600 project

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

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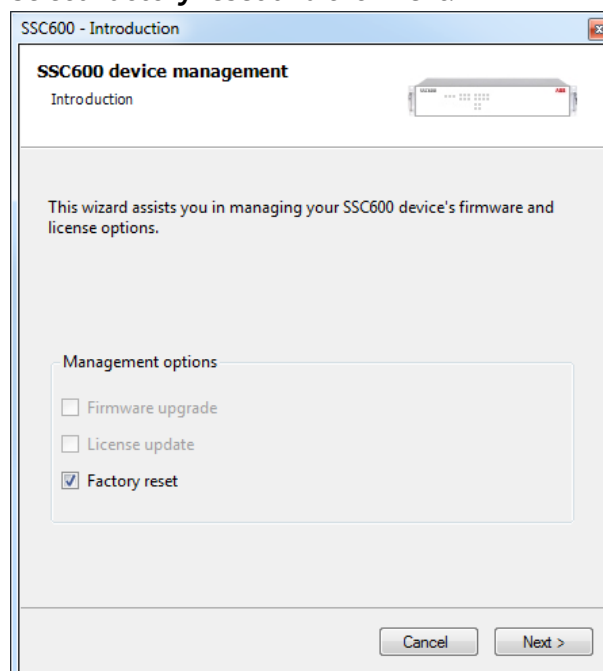
7.2 Restoring factory settings

In case of configuration data loss or any other file system error that prevents the protection device from working properly, the whole file system can be restored to the original factory state. All default settings and configuration files stored in the factory are restored. Only a user with System Update right (refer to table Default roles-to-rights in the Cyber Security Deployment Guideline) (e.g. ADMINISTRATOR) can restore the *factory* settings.
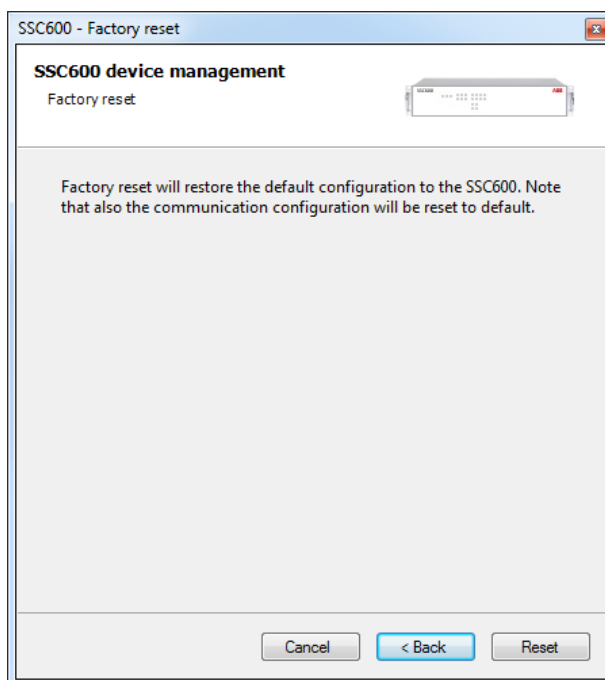
1. In the **Plant Structure** view, right-click the device and select **SSC600 Device Management**.
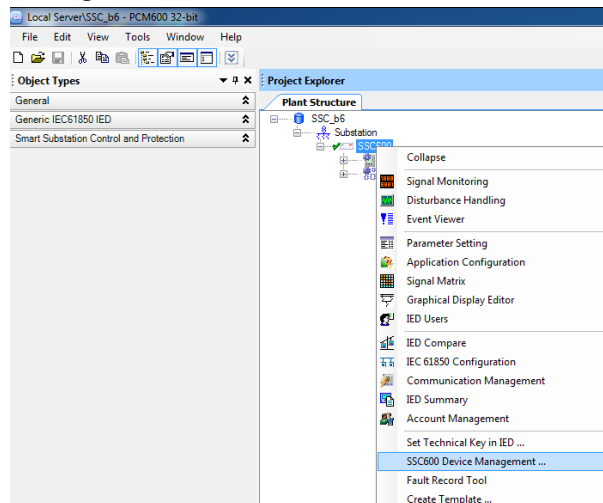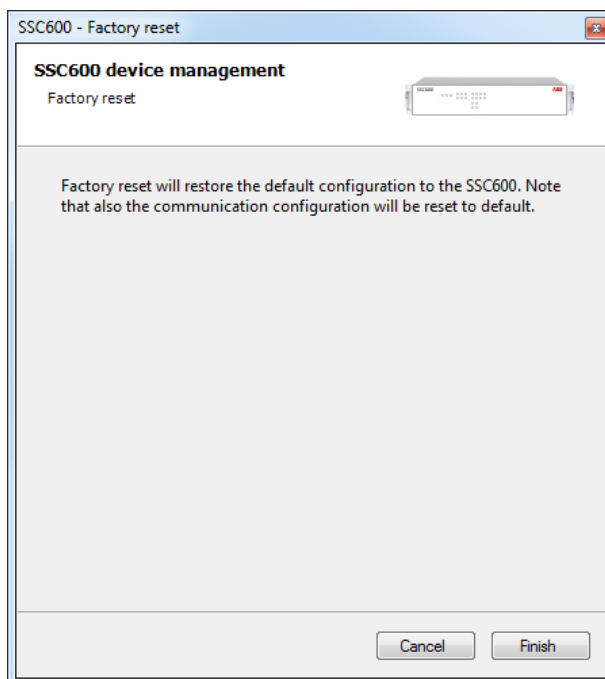

2. Select **Factory reset** and click **Next**.

3. Click **Reset**.

4. Click **Finish**.

The protection device restores the factory settings and restarts. Restoring takes 1...3 minutes. Confirmation of restoring the factory settings is shown on the display a few seconds, after which the device restarts.

Avoid the unnecessary restoring of factory settings, because all the parameter settings that are written earlier to the device will be

overwritten with the default values. During normal use, a sudden change of the settings can cause a protection function to trip.

7.3 Restoring lost password

If authentication is enabled in the protection device and last user with User Management Right password is lost, it is no longer possible to change passwords.

- Contact ABB technical customer support to retrieve back the User Management level access to the protection device.

8   Glossary

AD	Active Directory
BDEW	Bundesverband der Energie- und Wasserwirtschaft
CA	Certification Authority
CAL	Central Activity Logging
CAM	Centralized Account Management
DAA	HTTP Digest Access Authentication
DNP3	A distributed network protocol originally developed by Westronic. The DNP3 Users Group has the ownership of the protocol and assumes responsibility for its evolution.
DOM	Binary output module, four channels
DPC	Double-Point Control
EMC	Electromagnetic Compatibility
Ethernet	A standard for connecting a family of frame-based computer networking technologies into a LAN
FIFO	First In, First Out
FTP	File Transfer Protocol
FTPS	FTP Secure
GOOSE	Generic Object Oriented Substation Event
HMI	Human-Machine Interface
HTML	Hypertext Markup Language
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IEC 60870-5-104	Network access for IEC 60870-5-104 (IEC 104)
IEC 61850	International standard for substation communication and modeling
IEC 61850-8-1	A communication protocol based on the IEC 61850 standard series
IED	Intelligent Electronic Device (protection and control device)
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IEEE 1588 v2	Standard for a Precision Clock Synchronization Protocol for networked measurement and control systems
IEEE 1686	Standard for Substation Intelligent Electronic Devices' (IEDs') Cyber Security Capabilities
IP	Internet Protocol
IP address	A set of four numbers between 0 and 255, separated by periods. Each server connected to the Internet is assigned a unique IP address that specifies the location for the TCP/ IP protocol.
ISO	International Standard Organization
LHMI	Local Human-Machine Interface
MMS	1. Manufacturing message specification 2. Metering management system

	NERC CIP	North American Electric Reliability Corporation - Critical Infrastructure Protection
	PCM600	Protection and Control IED Manager
	PRP	Parallel Redundancy Protocol
	PTP	Precision Time Protocol
	R-GOOSE	Routable GOOSE
	RJ-45	Galvanic connector type
	SDM600	A software solution for automatic management of service and cyber security relevant data across substations
	SMV	Sampled Measured Values
	SNTP	Simple Network Time Protocol
	TCP	Transmission Control Protocol
	TCP/IP	Transmission Control Protocol/Internet Protocol
	UDP	User Datagram Protocol
	VPN	Virtual Private Network
	WHMI	Web Human-Machine interface

ABB

1MRS759013 E