

ABB ABILITY™ SMART SUBSTATION CONTROL AND PROTECTION FOR ELECTRICAL SYSTEMS
JANUARY 2019

CYBER SECURITY DEPLOYMENT GUIDELINE

SSC600



Copyright

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

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

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 (eay@cryptsoft.com) and Tim Hudson (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.

Open Source Software

This product contains open source software. For license information refer to product documentation at <http://www.abb.com>.

Warranty

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

<http://www.abb.com/mediumvoltage>

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.

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..... | 8 |
| 1.1 | This manual..... | 8 |
| 1.2 | Intended audience..... | 8 |
| 1.3 | Product documentation..... | 8 |
| 1.3.1 | Product documentation set..... | 8 |
| 1.3.2 | Document revision history..... | 9 |
| 1.3.3 | Related documentation..... | 9 |
| 1.4 | Symbols and conventions..... | 9 |
| 1.4.1 | Symbols..... | 9 |
| 1.4.2 | Document conventions..... | 10 |
| 2 | Security in distribution automation..... | 11 |
| 2.1 | General security in distribution automation..... | 11 |
| 2.2 | Reference documents..... | 11 |
| 3 | Secure system setup..... | 12 |
| 3.1 | Basic system hardening rules..... | 12 |
| 3.2 | Device communication interfaces..... | 12 |
| 3.3 | TCP/IP based protocols and used IP ports..... | 13 |
| 3.4 | Secure communication..... | 14 |
| 3.4.1 | Certificate handling..... | 14 |
| 3.4.2 | Encryption algorithms..... | 14 |
| 3.5 | Web HMI..... | 15 |
| 4 | User management..... | 16 |
| 4.1 | User roles..... | 16 |
| 4.2 | User authorization..... | 17 |
| 4.2.1 | Setting passwords..... | 18 |
| 5 | Security logging..... | 19 |
| 5.1 | Audit trail..... | 19 |
| 6 | Using the Web HMI..... | 21 |
| 6.1 | Logging in..... | 21 |
| 6.2 | Logging out..... | 21 |

| | | |
|----------|---|-----------|
| 7 | Protection of device and system configuration..... | 22 |
| 7.1 | Backup files..... | 22 |
| 7.1.1 | Creating a backup from the device configuration..... | 22 |
| 7.1.2 | Creating a backup from the PCM600 project..... | 22 |
| 7.2 | Restoring factory settings..... | 22 |
| 7.3 | Restoring the administrator password..... | 25 |
| 8 | Glossary..... | 26 |

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. 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

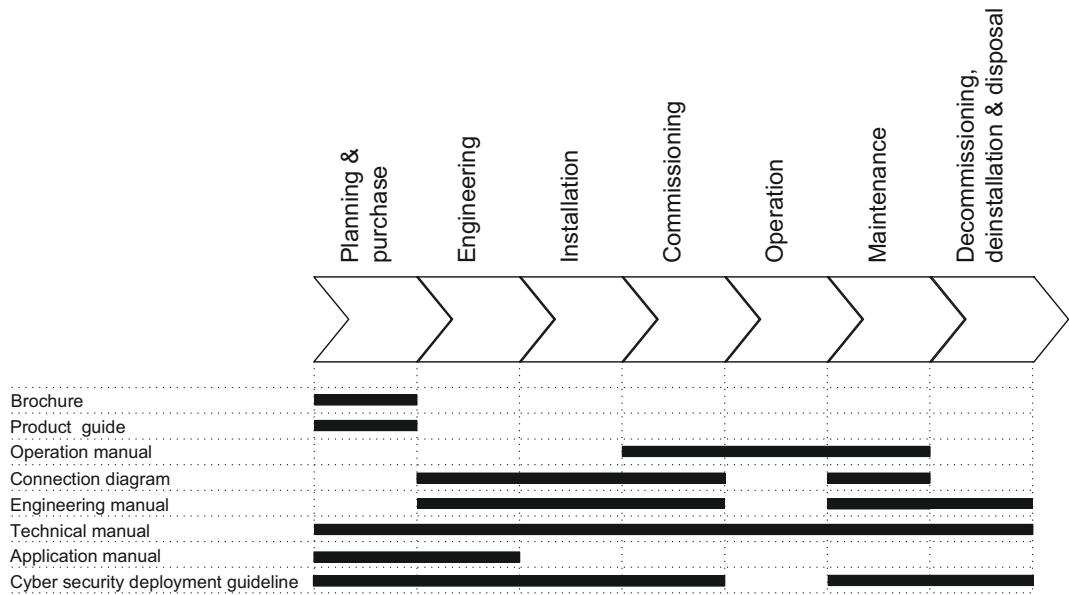


Figure 1. The intended use of documents during the product life cycle



Note: 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/2019-01-11 | 1.0 | First release |



Note: Download the latest documents from the ABB Web site <http://www.abb.com/mediumvoltage>.

1.3.3 Related documentation

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

1.4 Symbols and conventions

1.4.1 Symbols



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



Caution: 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.



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



Tip: 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
- 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
- Using firewalls and demilitarized zones
- Assessing the system periodically
- Using antivirus software in workstations and keeping those up-to-date

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

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 |

FTPS and IEC 61850 are primary services needed for device configuration and those cannot be disabled. Additionally, the protection device uses layer 2 communications in GOOSE, SMV, IEEE 1588 (PTP) and PRP supervision services, which needs to be taken into account 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.

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.



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

3.4.2 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 that certain technical features must be supported and enabled by the used Web client.

- HTTP 1.1
- HTML 4 and HTML 5
- XSLT 2.0
- CSS1 and CSS2.1
- AJAX
- JavaScript 1.2
- DOM 1.0
- HTTP Digest Access Authentication
- HTTP session cookies
- HTTP compression

In case of HTTPS access the Web client must support HTTPS via TLS 1.0 or TLS 1.1/1.2. The WHMI is verified with Internet Explorer 11.0.

The access to the device's WHMI is protected by the HTTP Digest Access Authentication (DAA) that requires a user name and password. DAA ensures that the user credentials are encrypted secure before sending over the network. See RFC2617 "HTTP Authentication: Basic and Digest Access Authentication" for detailed information about DAA.

User authentication is always required in WHMI.

4 User management

4.1 User roles

Four user categories have been predefined for the WHMI.

The default passwords in the protection device delivered from the factory can be changed with Administrator user rights. Device user passwords can be changed using WHMI or the IED User Management tool in PCM600 and the user information is stored to the protection device's internal memory.



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

Table 3: Predefined user categories

| Username | User rights |
|---------------|--|
| VIEWER | Read only access |
| OPERATOR | <ul style="list-style-type: none"> • Selecting remote or local state (only via Local port) • Changing setting groups • Controlling • Clearing indications |
| ENGINEER | <ul style="list-style-type: none"> • Changing settings • Clearing event list • Clearing disturbance records • Changing system settings such as IP ADDRESS or disturbance recorder settings • Setting the protection device to test mode • Selecting language |
| ADMINISTRATOR | <ul style="list-style-type: none"> • All listed above • Changing password • Factory default activation |

If the Remote override parameter from the **Main menu > Configuration > Authorization > Passwords** menu has been disabled, changes have to be made in the IED's object properties in PCM600. When the protection device uses remote authentication, the activated user level and its password are required when the protection device is configured using PCM600.

Table 4: Object properties to change

| Object Properties field | Value |
|----------------------------|----------------------------|
| Is Authentication Disabled | False |
| Is Password used | True |
| Password | Write the correct password |

When communicating with the protection device with PCM600 tools and with the device authentication enabled, the device username and password must be given when prompted. When setting the technical key, the username and password must be given twice.



Tip: If the PCM600 authentication has been enabled in PCM600 System Settings, a device 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 device.



Note: When Remote override is disabled, also MMS clients need authentication using correct password.



Note: FTP always requires authentication.

4.2 User authorization

The user categories have been predefined for WHMI, each with different rights and default passwords. For all user categories there are two different passwords, which are needed for different purposes. For local connection there is a separate 'WHMI local password' and for remote connection 'WHMI remote password'. Local connection is allowed only from the Ethernet port called 'Local port'. Via the local connection user is allowed to perform local control operations such as opening or closing circuit breaker. From all other Ethernet ports only remote connections are allowed.

Passwords are settable for all predefined user categories. The password must contain at least nine characters. The maximum number of characters is 20. Only the following characters are accepted.

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



Note: User authorization is disabled by default and can be enabled via the WHMI Main Menu > Configuration > Authorization > Passwords.

Table 5: Predefined user categories and default passwords

| Username | WHMI remote password | WHMI local password | User rights |
|---------------|----------------------|---------------------|---|
| VIEWER | remote0001 | 0001 | Only view access |
| OPERATOR | remote0002 | 0002 | Authorized to make operations |
| ENGINEER | remote0003 | 0003 | Allowed to change IED parameters, but no operation rights |
| ADMINISTRATOR | remote0004 | 0004 | Full access |



Note: For user authorization for PCM600, see PCM600 documentation.

4.2.1

Setting passwords

If user authorization is off or the user is logged in as an administrator, user passwords can be set via the WHMI or with PCM600.



Note: There are two separate WHMI connections - Local WHMI connection via Local port (one dedicated ethernet port), and all other ports are 'remote connections'. Local passwords can be changed only via the Local WHMI. Remote passwords can be changed via the WHMI 'remote connections' or with PCM600.

Select **Main menu > Configuration > Authorization > Passwords**.



Note: If the administrator 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.

Table 6: Audit trail events

| Audit trail event | Description |
|----------------------|--|
| Configuration change | Configuration files changed |
| Firmware change | Firmware changed |
| Firmware change fail | Firmware change failed |
| Setting group remote | User changed setting group remotely |
| Setting group local | User changed setting group locally |
| Control remote | DPC object control remote |
| Control local | DPC object control local |
| Test on | Test mode on |
| Test off | Test mode off |
| Reset trips | Reset latched trips (TRPPTRC*) |
| Setting commit | Settings have been changed |
| Time change | Time changed directly by the user. Note that this is not used when the protection device is synchronised properly by the appropriate protocol. |
| View audit log | Administrator accessed audit trail |
| Login | Successful login from IEC 61850-8-1 (MMS), WHMI or FTP. |
| Logout | Successful logout from IEC 61850-8-1 (MMS), WHMI or FTP. |
| Password change | Password changed |

| Audit trail event | Description |
|-------------------|---|
| Firmware reset | Reset issued by user or tool |
| Audit overflow | Too many audit events in the time period |
| Violation remote | Unsuccessful login attempt from IEC 61850-8-1 (MMS), WHMI. |
| Violation local | Unsuccessful login attempt from IEC 61850-8-1 (MMS), WHMI or FTP. |

PCM600 Event Viewer can be used to view the audit trail events and process related events. Audit trail events are visible through dedicated Security events view. Since only the administrator has the right to read audit trail, authorization must be used in PCM600. 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.



Note: To expose the audit trail events through Event list, define the Authority logging level parameter via **Configuration > Authorization > Security**. This exposes audit trail events to all users.

Table 7: Comparison of authority logging levels

| Audit trail event | Authority logging level | | | | | |
|---------------------------|-------------------------|------------------------------|------------------|--------------------------------|---------------|-----|
| | None | Configura- tion change | Setting group | Setting group, con- trol | Settings edit | All |
| Configuration change | | • | • | • | • | • |
| Firmware change | | • | • | • | • | • |
| Firmware change fail | | • | • | • | • | • |
| Setting group re- mote | | | • | • | • | • |
| Setting group local | | | • | • | • | • |
| Control remote | | | | • | • | • |
| Control local | | | | • | • | • |
| Test on | | | | • | • | • |
| Test off | | | | • | • | • |
| Reset trips | | | | • | • | • |
| Setting commit | | | | | • | • |
| Time change | | | | | | • |
| View audit log | | | | | | • |
| Login | | | | | | • |
| Logout | | | | | | • |
| Password change | | | | | | • |
| Firmware reset | | | | | | • |
| Violation local | | | | | | • |
| Violation remote | | | | | | • |

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.



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



Note: 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 Internet Explorer.
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.

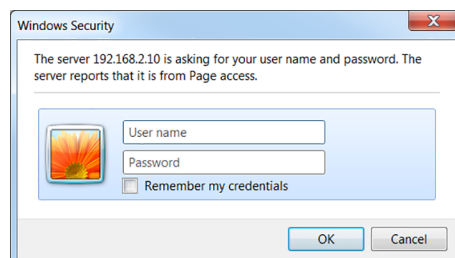


Figure 2. Entering username and password to use the WHMI

5. Click **OK**.
The language file starts loading and the progress bar is displayed.

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.



Note: User authorization is needed before using the tool.

2. Enter the user credentials if the default administrator password has been changed. Administrator or engineer credentials are needed for authorization.

7.1.2 Creating a backup from the PCM600 project

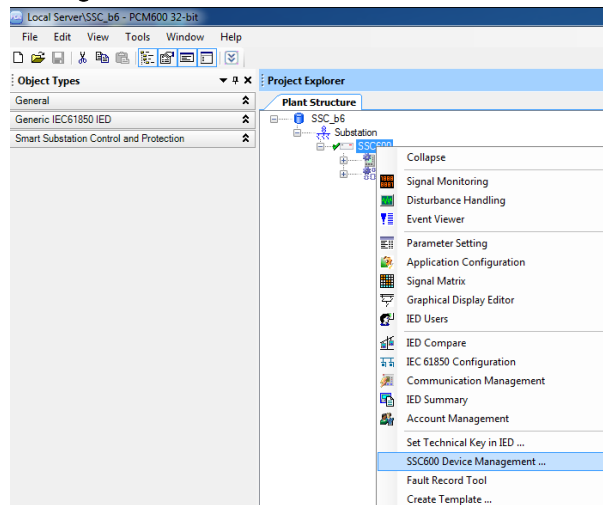
Backup from the PCM600 project is made by exporting the project.

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.

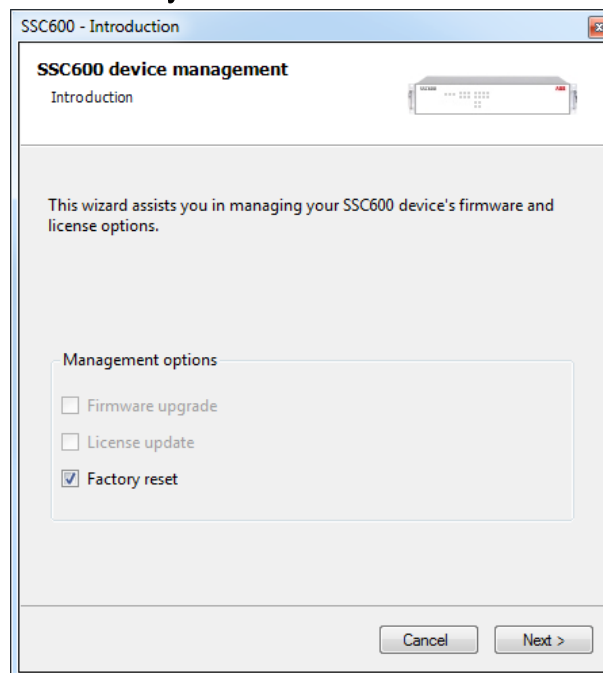
7.2 Restoring factory settings

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 the administrator can restore the factory settings.

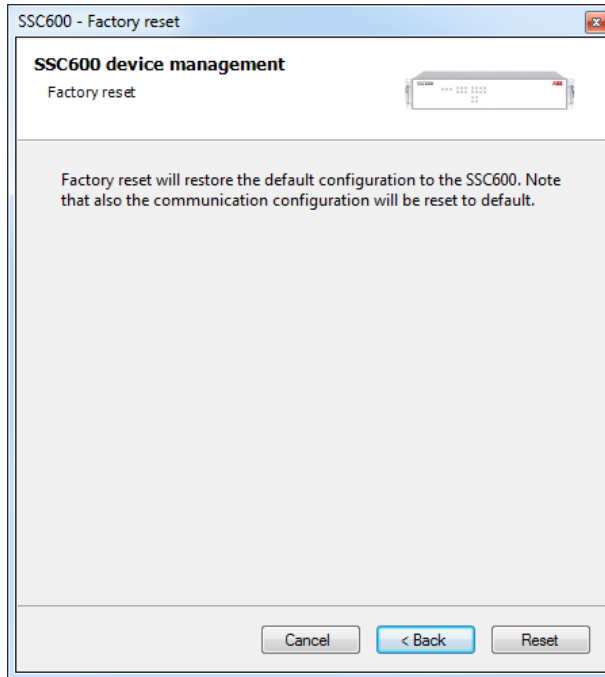
1. In the **Plant Structure** view, right-click the device and select **SSC600 Device Management**.



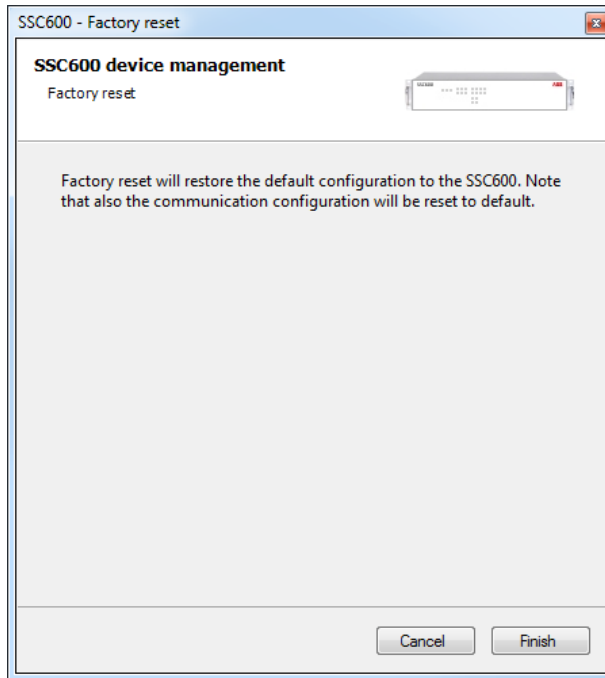
2. Select **Factory reset** and click **Next**.



3. Click **Reset**.



4. Click **Finish**.



Results

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.



Note:

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 the administrator password

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

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

8 Glossary

| | |
|-----------------|--|
| BDEW | Bundesverband der Energie- und Wasserwirtschaft |
| CA | Certification authority |
| 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 60870-5-101 |
| 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. |
| IRIG-B | Inter-Range Instrumentation Group's time code format B |
| ISO | International Standard Organization |
| 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 |
| RJ-45 | Galvanic connector type |
| 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 Distribution Solutions
Distribution Automation
P.O. Box 699
FI-65101 VAASA, Finland
Phone +358 10 22 11
Fax +358 10 22 41094
www.abb.com/mediumvoltage