# Protection and Control IED Manager PCM600

## Cyber Security Deployment Guideline

Document ID: 1MRS758440

Issued: 2025-09-11

Revision: H

Product version: 2.14

© Copyright 2025 ABB. All rights reserved

## Copyright

ABB is the owner of the copyright in this document. This document or any parts thereof must not be reproduced or copied without the written permission from ABB and the contents thereof must not be used to any unauthorized purpose.

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

### Trademarks

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

### Open Source Software

This product contains open source software. For license information refer to product documentation at *www.abb.com*.

### Warranty

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

*www.abb.com/mediumvoltage*

## Disclaimer

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.

# Contents

# 1 Introduction

## 1.1 This manual

The cyber security deployment guideline describes the process for handling cyber security when engineering and monitoring protection and control IEDs. The cyber security deployment guideline provides information on how to secure the engineering environment on which the IED is installed. The guideline can be used as a technical reference during the engineering phase, installation and commissioning phase, and during normal service. See also all IED-related cyber security deployment guidelines.

## 1.2 Intended audience

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

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

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

## 1.3 Product documentation

### 1.3.1 Product documentation set

The cyber security deployment guideline describes the process for handling cyber security when engineering and monitoring protection and control IEDs. The cyber security deployment guideline provides information on how to secure the engineering environment on which the IED is installed. The guideline can be used as a technical reference during the engineering phase, installation and commissioning phase, and during normal service. See also all IED-related cyber security deployment guidelines.

The getting started guide provides basic instructions on how to use PCM600. The manual provides instructions for typical use cases in operation and field, as well as for use cases in engineering and commissioning. The purpose of the manual is to describe the PCM600 tool functionality, and it can be seen as a complementary manual to the application-related instructions, such as the relay-specific operation or engineering manuals.

The online help contains instructions on how to use the software.

## 1.3.2 Document revision history

| Document revision/date | Product version | History |
|---|---|---|
| A/2015-11-20 | 2.7 | First release |
| B/2016-09-29 | 2.8 | Content updated to correspond to the product version |
| C/2018-04-18 | 2.9 | Content updated to correspond to the product version |
| D/2020-01-22 | 2.10 | Content updated to correspond to the product version |
| E/2021-11-17 | 2.11 | Content updated to correspond to the product version |
| F/2022-11-30 | 2.12 | Content updated to correspond to the product version |
| G/2024-03-11 | 2.13 | Content updated to correspond to the product version |
| H/2025-09-11 | 2.14 | Content updated to correspond to the product version |

## 1.3.3 Related documentation

Product series- and product-specific manuals can be downloaded from the ABB Web site *go.abb/digitalsubstations*.

## 1.3.4 Symbols and conventions

### 1.3.4.1 Symbols

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

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

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

Operation of damaged equipment could, under certain operational conditions, result in degraded process performance leading to information or property loss. Therefore, comply fully with all notices.

### 1.3.4.2 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**.
- Menu, tab, button, list and box names as well as window or dialog box titles are presented in bold.

  On the **File** menu, click **New Project**.

  Right-click the **MainApp** tab and select **Copy** from the shortcut menu.

  Click **OK** to start the comparing.
- Shortcut keys are presented in uppercase letters.

  A page can also be added pressing the shortcut keys CTRL+SHIFT+P.
- Command prompt commands are shown in Courier font.

  Type `ping <devices_IP_address>/t` and wait for at least one minute to see if there are any communication breaks.
- Parameter names are shown in italics.

  The function can be enabled and disabled with the *Operation* setting.

# 2 Security in substation and distribution automation systems

## 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.

See also all IED-related cyber security deployment guidelines.

# 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 IEDs 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 IEDs are also part of this concept. The following should be taken into consideration when planning the system protection.

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

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 TCP/IP based protocols and used IP ports

PCM600 does not require specific ports to be open if distributed setup is not used. However, Update Manager requires allowing outbound connections to port 443 (https protocol).

To set up an IP firewall, see the IED-specific cyber security deployment guidelines for the ports that are used to communicate and to configure the IEDs. All closed ports can be opened in the configuration. Ports that are open by default are used for configuring or monitoring the protection IED.

## 3.3 Secure communication

Some of the protection IEDs support encrypted communication according to the principles of IEC 62351 in secured communication for WHMI and file transfer protocol. If the *Secure Communication* parameter is activated in the IED, protocols require TLS protocol based encryption method support from the clients. In case of file transfer, the client must use FTPS. PCM600 supports FTPS and is able to download and upload configuration files in encrypted format from IED.

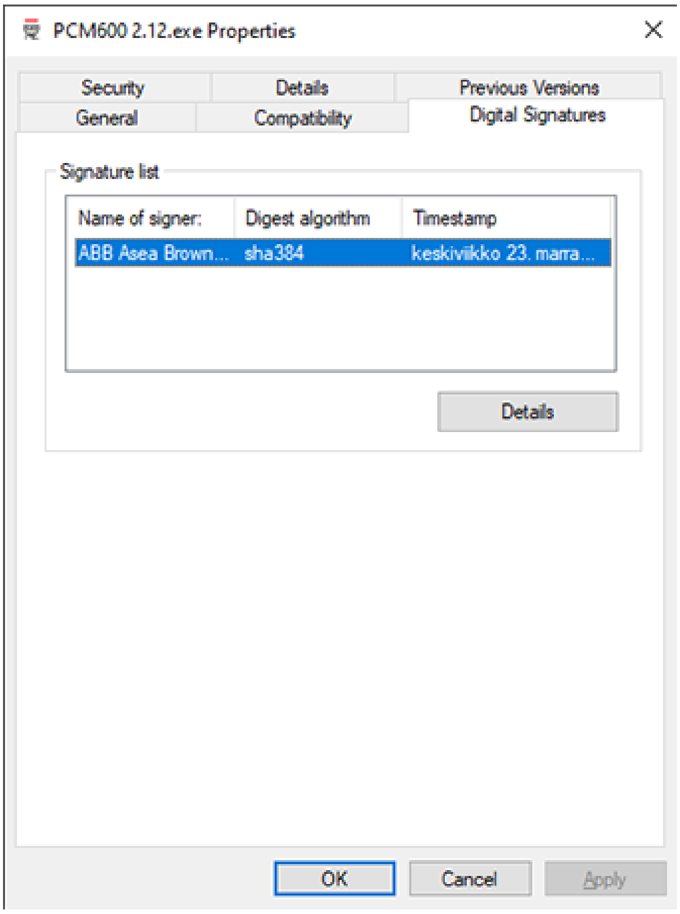
For legacy devices which do not support secure communication, non-encrypted communication is used.

## 3.4 Validating PCM600 installer integrity

Integrity of the PCM600 installation package can be verified with the following procedure.

1. Locate the downloaded installer package.
2. Right-click on the installer and select **Properties**.

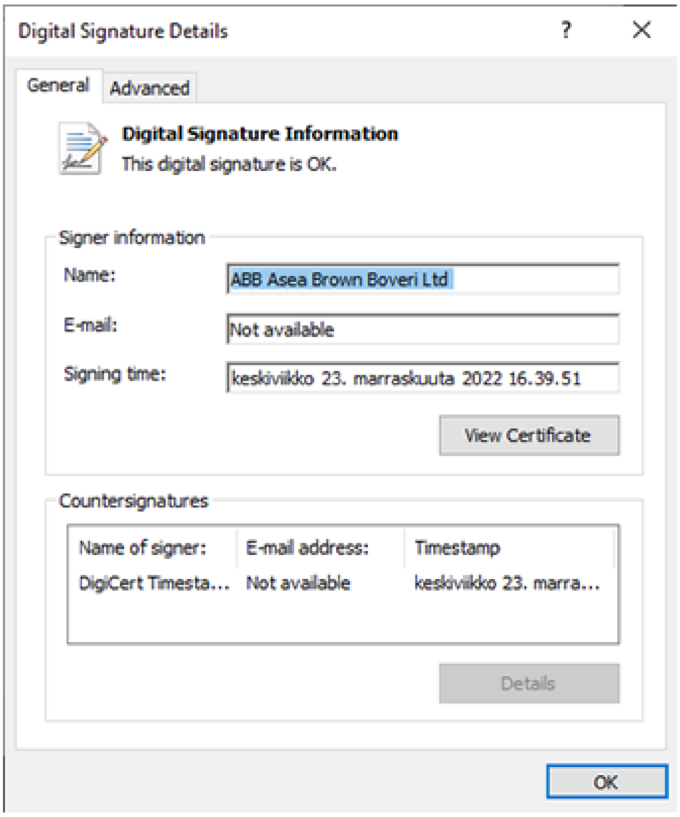
3. Go to **Digital Signatures**.
4. Select the ABB Signature from the list and click **Details**.



| Name of signer: | Digest algorithm | Timestamp |
|---|---|---|
| ABB Asea Brown... | sha384 | keskiviikko 23. marra... |

*Figure 1: Selcting digital signature*

Dialog opens for **Digital Signature Details**. The dialog shows that the digital signature is OK.



Digital Signature Details

**Digital Signature Information**

This digital signature is OK.

Signer information

Name: ABB Asea Brown Boveri Ltd

E-mail: Not available

Signing time: keskiviikko 23. marraskuuta 2022 16.39.51

Countersignatures

| Name of signer: | E-mail address: | Timestamp |
|---|---|---|
| DigiCert Timesta... | Not available | keskiviikko 23. marra... |

*Figure 2: Digital Signature Information*

## 3.5 Validation of application libraries

PCM600 includes a functionality for validating application binary files. In other words, PCM600 validates its own application files and the activated connectivity package application files. Default security level is "High".

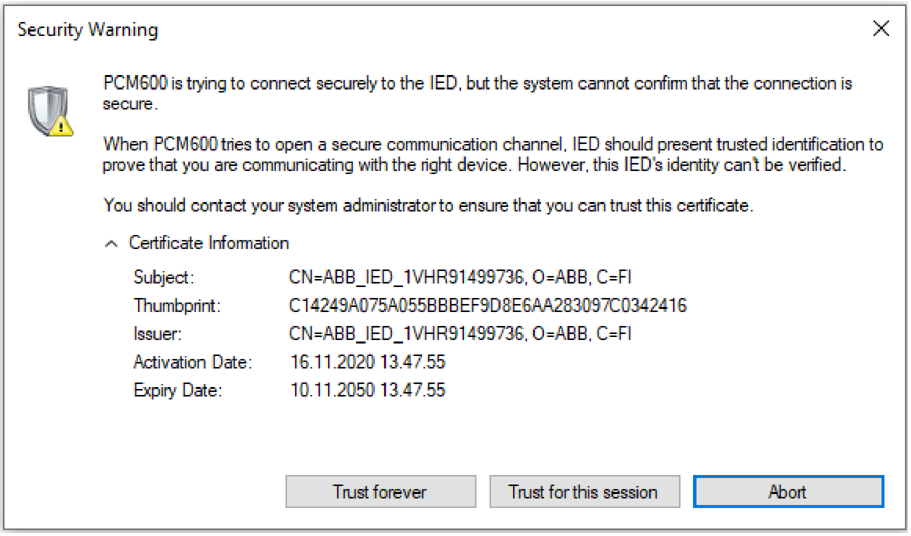
**Table 1: Available security levels**

| Security level | Description |
|---|---|
| Low | Application files are not validated by PCM600. Use this option when it is certain that both PCM600 and connectivity packages are loaded from a trusted secure location. |
| Medium | Application files are validated by PCM600. Exceptions can be added to load an activated connectivity package that failed the application file validation.<br>Use this option when it is certain that the connectivity packages are loaded from a trusted secure location. |
| High | Application files are validated by PCM600. Activated connectivity packages that fail the application file validation are blocked from PCM600. |

The recommended security level is “High”.

## 3.6 IED certificates

When PCM600 connects securely to an IED, the IED security certificate is shown. The user can select to trust that IED forever or for the current PCM600 session.



Security Warning

PCM600 is trying to connect securely to the IED, but the system cannot confirm that the connection is secure.

When PCM600 tries to open a secure communication channel, IED should present trusted identification to prove that you are communicating with the right device. However, this IED's identity can't be verified.

You should contact your system administrator to ensure that you can trust this certificate.

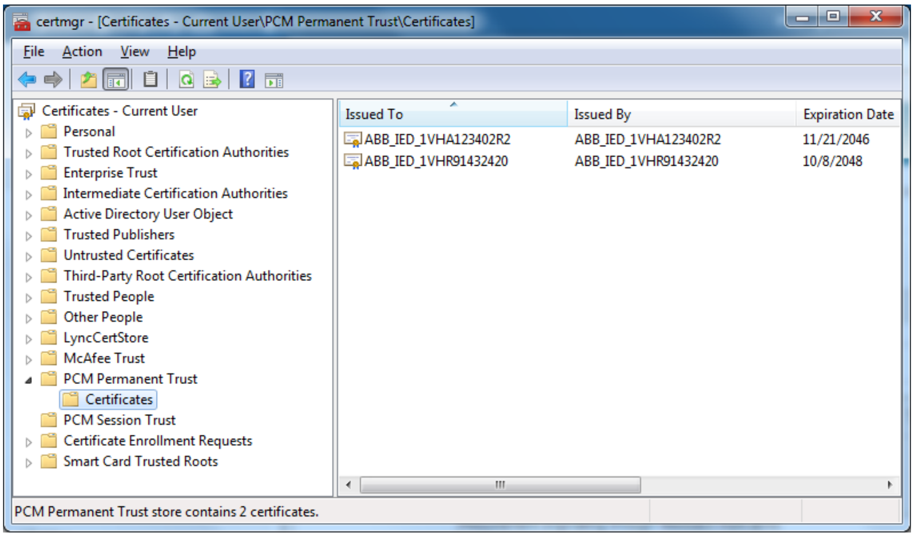
Certificate Information

| | |
|---|---|
| Subject: | CN=ABB_IED_1VHR91499736, O=ABB, C=FI |
| Thumbprint: | C14249A075A055BBBEF9D8E6AA283097C0342416 |
| Issuer: | CN=ABB_IED_1VHR91499736, O=ABB, C=FI |
| Activation Date: | 16.11.2020 13.47.55 |
| Expiry Date: | 10.11.2050 13.47.55 |

*Figure 3: Security warning*

These certificates are added to Windows Certificate Storage and can be viewed using the certmgr.msc management snippet in Windows.

In Certificate Manager, all IED certificates are stored under PCM Permanent Trust and PCM Session Trust. PCM Session Trust is cleared when PCM600 is closed. Permanently trusted IED certificates can be manually removed by deleting them from PCM Permanent Trust.


certmgr - [Certificates - Current User\PCM Permanent Trust\Certificates]
File
Action
View
Help

Certificates - Current User
- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers
- Untrusted Certificates
- Third-Party Root Certification Authorities
- Trusted People
- Other People
- LyncCertStore
- McAfee Trust
- PCM Permanent Trust
  - Certificates
- PCM Session Trust
- Certificate Enrollment Requests
- Smart Card Trusted Roots

| Issued To | Issued By | Expiration Date |
|---|---|---|
| ABB_IED_1VHA123402R2 | ABB_IED_1VHA123402R2 | 11/21/2046 |
| ABB_IED_1VHR91432420 | ABB_IED_1VHR91432420 | 10/8/2048 |

PCM Permanent Trust store contains 2 certificates.

*Figure 4: PCM Permanent Trust certificates*

All IED certificates are trusted in the current user scope. Every PCM600 user must trust IED certificates individually.

# 4 PCM600 user management

## 4.1 PCM600 SQL Server authorization

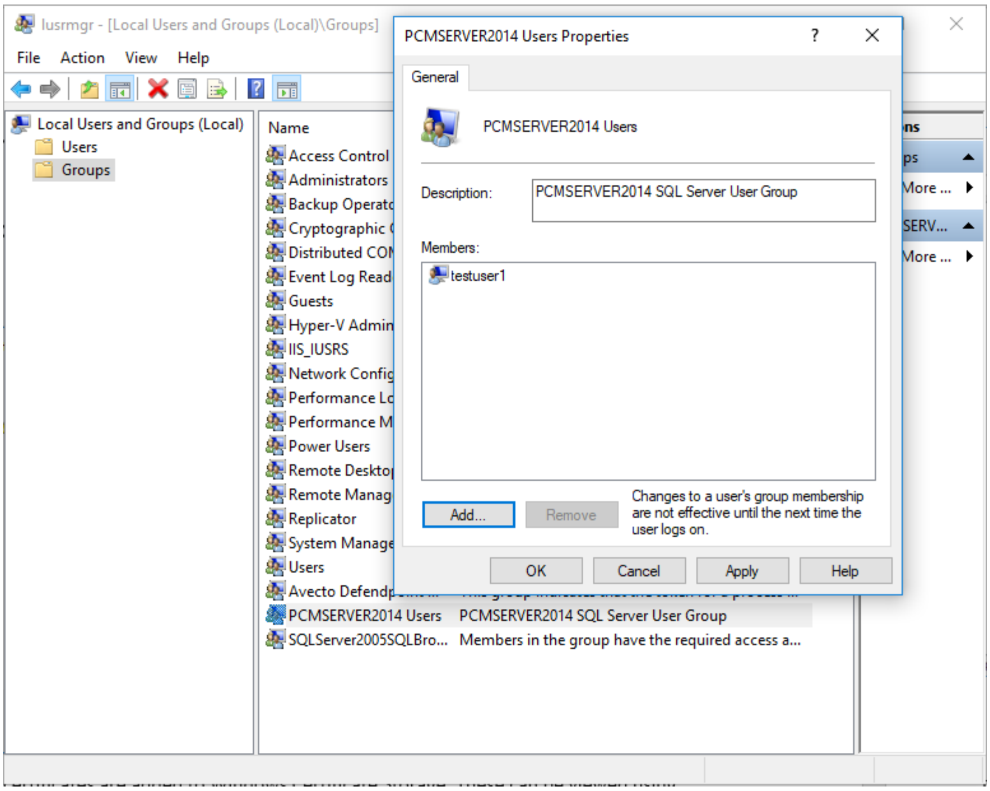
PCM600 works with two specific SQL Server instances: PCMSRV22ABB for normal project data and PCMSECSRV22ABB for security settings. Authorization for PCM600 databases is handled by two specific Windows user groups: PCMSERVER2014 Users and PCM Security Administrators.

Every Windows user using PCM600 must belong to PCMSERVER2014 Users.

Windows users acting as PCM600 Security Administrators must belong to PCM Security Administrators.

Adding users to PCM600 user groups:

1. Open lusrmgr.msc.
2. Add the required PCM600 users to the **PCMSERVER2014 Users** group.



lusrmgr - [Local Users and Groups (Local)\Groups]

Local Users and Groups (Local)
- Users
- Groups

| Name | |
|---|---|
| Access Control | |
| Administrators | |
| Backup Operato | |
| Cryptographic ( | |
| Distributed COM | |
| Event Log Read | |
| Guests | |
| Hyper-V Admin | |
| IIS_IUSRS | |
| Network Config | |
| Performance Lo | |
| Performance M | |
| Power Users | |
| Remote Desktop | |
| Remote Manag | |
| Replicator | |
| System Manage | |
| Users | |
| Avecto Defendp... | This group indicates that the token for a process ... |
| PCMSERVER2014 Users | PCMSERVER2014 SQL Server User Group |
| SQLServer2005SQLBro... | Members in the group have the required access a... |

PCMSERVER2014 Users Properties

PCMSERVER2014 Users

Description: PCMSERVER2014 SQL Server User Group

Members:
testuser1

Changes to a user's group membership are not effective until the next time the user logs on.

*Figure 5: PCMSERVER2014 Users group*

3. Add all PCM600 security administrators to the **PCM600 Security Administrators** group.

## 4.2 PCM600 user authentication

This section describes the user authentication for PCM600. For IED user authentication, see the IED-specific cyber security deployment guidelines.

PCM600 supports working with Windows authentication or without authentication. Windows authentication method is enabled by default.

It is not recommended to use PCM600 without authentication.

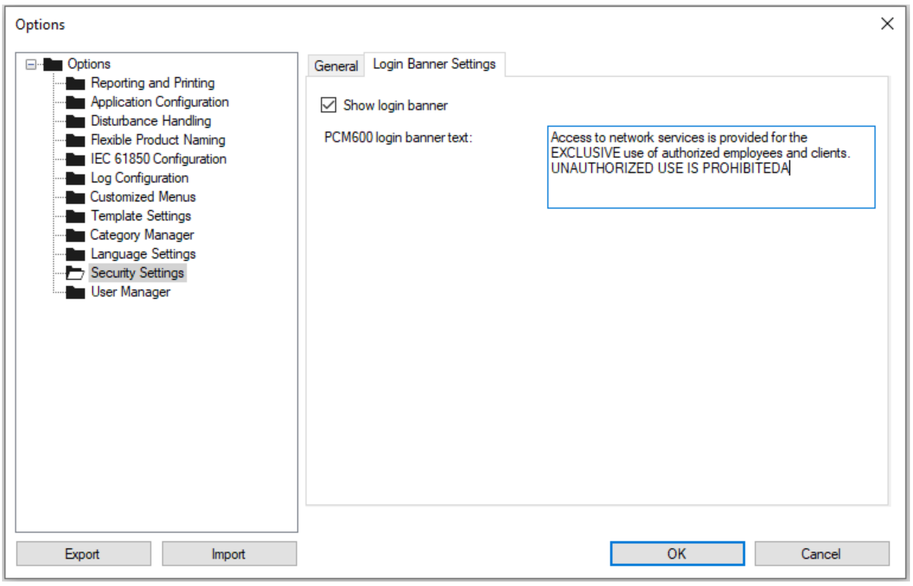
When PCM600 is started for the first time, a PCM600 system engineer account will be created and launching Windows user will be associated with created system engineer account. The user starting PCM600 for the first time must belong to PCM Security Administrators user group in Windows.

It is not recommended to use the administrator accounts by default. It is recommended to create limited user accounts that have privileges only for performing the necessary tasks related to the user role.

### 4.2.1 Configuring login banner

In some countries, a legal statement banner should be displayed when accessing a device. Login banner configuration is enabled only if the logged in PCM600 user has function and rights set to User Management - Administration allowed.

1. On the menu bar, click **Tools** and select **Options**.
2. Click **Security Settings** and select the **Login Banner Settings** tab.
3. Select the **Show login banner** check box.



☑ Show login banner

PCM600 login banner text: Access to network services is provided for the EXCLUSIVE use of authorized employees and clients. UNAUTHORIZED USE IS PROHIBITEDA

*Figure 6: Configuring the login banner*

PCM600 authentication must be enabled to show and configure the login banner functionality.

## 4.3 Activating user authentication

The system engineer can enable or disable the user authentication. When the user authentication is disabled, all the users get full rights to operate. The login function also works according to this function. For more information on the login functions, see the getting started guide.

1. On the menu bar, click **Tools** and select **Options**.
2. Click **Security Settings** and select the **General** tab.
3. Under **Authentication**, select the appropriate option.
   - **Disabled** means that user authentication is disabled.
   - **Windows** authentication compares the account name of the current Windows user to the Windows account name specified for users in PCM600 User Manager. If Windows authentication is enabled and the current Windows user account has not been linked to any PCM600 user account, PCM600 can’t be started.

When entering Windows account names in PCM600 User Manager, the account name must contain both a domain and a user name. The account names are entered in the Windows Account field, for example, mydomain\john.

The recommended authentication method is the Windows authentication. This also enables indirect password recovery. Windows user passwords can be recovered on Windows if forgotten.

## 4.4 User categories

## 4.4.1 Creating user categories

The user management is based on the users and the user categories. The users have a user account for PCM600. Each user account is mapped to one user category, which defines the permission to access certain functions. There are four default user categories.

- System Engineer acts as an administrator for the system and has full rights to perform any function and can define the user accounts.
- Security Administrator has access to security related functionality of PCM600 and IEDs
- Operator can perform certain simple tasks and has read-only access to certain functionality of PCM600.
- Application Engineer can access most of the functions and has read and write access to the IED engineering functionality.

Check the actual settings of the user categories from **Tools** > **Options** > **Category Manager** in PCM600.

The users belonging to a category with user management administration rights can create new user categories. The name of the user category must be unique.

1. On the menu bar, click **Tools** and select **Options** to start the user management.
2. Select the **Category Manager** folder.
3. Click **Add New Category** to open the **Add New Category** dialog.
4. Type the name for the new user category.
5. Specify the rights to perform different functions under the **Functions And Rights** field.
6. Select **OK** to save the definition.

## 4.4.2 Deleting user categories

A user with the System Engineer rights can delete the user categories. System Engineer and Security Administrator categories cannot be deleted. If there are members in the deleted category, a confirmation for removing the category appears. If the category is removed, the user accounts remain, but they are no longer mapped to any user category. The category changes are saved to the system configuration data.

1. On the menu bar, click **Tools** and select **Options** to start the user management.
2. Select the **Category Manager** folder.
3. Select the right user category from the drop-down list.
4. Click **Delete Category** to remove the user category.
5. Click **Yes** to confirm the delete operation.

### 4.4.3 Modifying existing user categories

Users belonging to a category with user management administration rights can change access rights of user categories. Access rights of System Engineer and Security Administrator user categories cannot be changed. The System Engineer user category has always full privileges.

1. On the menu bar, click **Tools** and select **Options** to start the user management.
2. Select **Category Manager** folder.
3. Select the right user category from the **User Category** drop-down list to activate the **Functions And Rights** field.
4. Change the user rights by selecting one of the user levels in the drop-down menu of the function.

The Functions And Rights field is divided into different sections for you to specify the user rights by a specific tool component or function.

## 4.5 User management

This chapter describes the user management for PCM600. For IED user management, see the IED-specific cyber security deployment guidelines.

### 4.5.1 Creating users

Create a new user to PCM600 and define the user information.

- User name (mandatory)
- Real name of the user
- User category

The Windows account can be used to log in automatically. Single Windows account can be mapped to a single PCM600 account. These Windows account names are only used for login, if the administrator has enabled the Windows authentication.

1. On the menu bar, click **Tools** and select **Options** to start the user management.
2. Select the **User Manager** folder.
3. Click **Add New User** in the **User Profile** field.

   The **Add New User** dialog is displayed.
4. Type **User Name** and select **User Category** from the drop-down list.

   The user name must be at least three characters long.
5. Click **OK** to confirm.

   The new user is created.

### 4.5.2 Deleting users

1. On the menu bar, click **Tools** and select **Options** to start the user management.
2. Select **User Manager** folder.

3. Select the right user name from the **User Name** drop-down list.
4. Click **Delete User** under the User Profile field.

Users belonging to a category with user management administration rights can delete users.

ℹ The System Engineer account cannot be deleted.

# 5 PCM600 Scheduler setup

To use the Scheduler service on PCM600, the logon account for the service must be the same as the intended Windows account for running PCM600. The service logon account can be configured in Services.msc. Search for appropriate ABBPCMSchedulerService version depending on your PCM600 version and change the service logon account on the Log On tab.

If authentication is enabled for the IED, use the Scheduler tool in PCM600 using the same Windows account as the account defined as logon account for the Scheduler service.

If ABBPCMSchedulerService fails to start for the standard user, ensure that the user has the "Log on as a service" user rights defined using the Local Security Policy tool.

To use PCM600 Scheduler with IEDs with security certificates, the PCM600 option Always trust IED security certificates in Security Settings must be enabled. This setting should be enabled only in a secure environment where the communication between PCM600 and the IED is secure.

# 6 Configuration of computer settings for PCM600

## 6.1 General security actions

In general, the Windows operating system can be protected from the malicious attacks with the latest service packs and security updates, firewalls, security policies, application whitelisting, and virus scanners. In computers where PCM600 is installed, programs and services that are not used can be uninstalled or disabled to reduce the attack surface.

This section gives an overview of different ways to secure the operating systems on which PCM600 is installed.

If PCM600 is run on virtual computer, these recommendations still apply.

## 6.2 Operating systems

**Table 2: Supported operating systems for PCM600 installation**

| Edition | Operating system |
|---|---|
| Desktop | Windows 11 64 bit |
| Server | Windows Server 2022 64 bit<br>Windows Server 2025 64 bit |

Only 64-bit OS is supported.

See the operating system related documentation and best practices to further reduce the attack surface in the operating system.

## 6.3 BIOS settings

Passwords must be enabled and remote wake up/wake on LAN disabled manually.

## 6.4 Windows updates and patch management

There are nine update classifications defined by Microsoft. These include, for example, critical updates, drivers, security updates and service packs. The compatibility of PCM600 with the latest Microsoft security updates and service packs is tested and verified monthly by ABB. The report does not cover computers from which PCM600 is accessed remotely. In general, it is recommended to install all the Windows updates.

**Windows Update vs. Microsoft Update**

Windows Update receives updates only for the Windows operating system. Microsoft Update must be used for other installed Microsoft products. The updates must be configured manually.

After PCM600 installation, it is recommended to update the system to the latest ABB verified patch level of all installed ABB software products. For other vendors' software products, see the respective documentation.

## 6.5 Virus scanner

PCM600 does not create specific requirements for anti-virus software. It is recommended to use organization specific de facto anti-virus software, which has to be configured manually.

## 6.6 Malware protection

PCM600 does not create specific requirements for malware protection software. It is recommended to use organization specific de facto malware protection software, which has to be configured manually.

## 6.7 Firewall, ports and services

PCM600 does not have specific firewall requirements if distributed setup is not used. PCM600 is a client system from the communication point of view. However, sometimes when reading disturbance records using FTPS, for example, communication fails after some amount of successful communication. This is caused by the Windows Firewall’s Stateful Package Inspection feature. The feature can be disabled by running the following PowerShell command with administrator privileges:

```
Set-NetFirewallSetting -EnableStatefulFtp false -PolicyStore PersistentStore
```

When PCM600 is used in a distributed setup, see *Chapter 6.8 Distributed installation of PCM600* for actions needed on the SQL Server computer.

The firewall has to be configured manually.

## 6.8 Distributed installation of PCM600

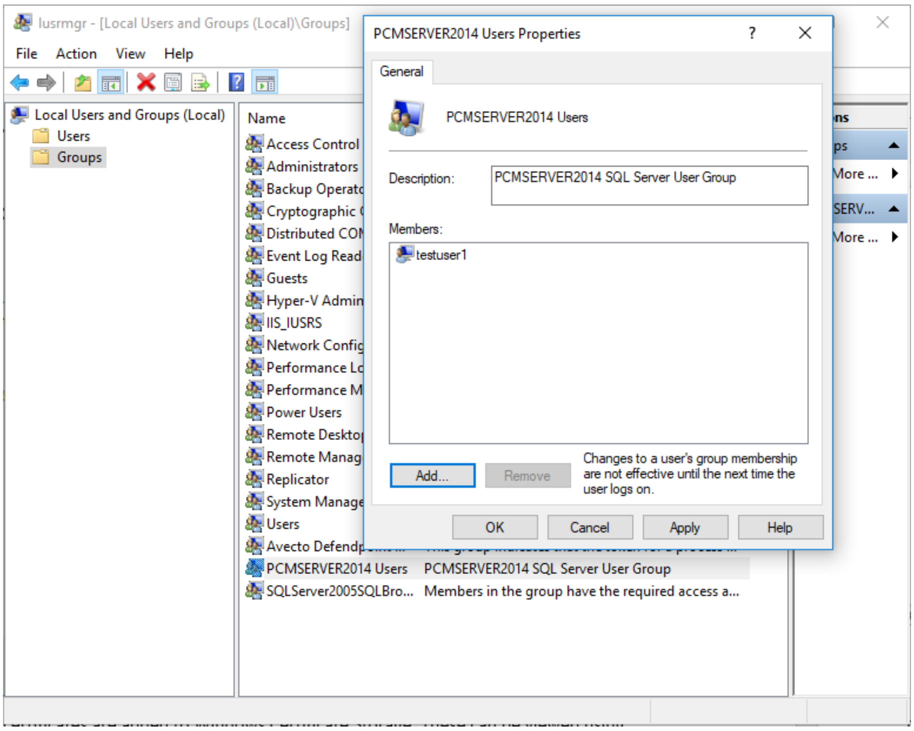
SQL Server and PCM600 can be installed on different computers. The server computer contains SQL Server and a shared location where PCM600 stores internal files. The client PC contains PCM600, Update Manager and connectivity packages. PCM600 installer can perform client or server installation. For installation instructions, see PCM600 Installation Guide.

When using the distributed setup, each user using PCM600 must have access to SQL Server. This is done by adding the user to the PCMSERVER2014 Users user group. The user group is automatically created after installing PCM600 on the server computer. User administrating PCM600 must be also added to PCM Security Administrators group.

The users must be added to the abovementioned groups on both server and client computers.

Distributed installation can’t be used without using Windows domain accounts. It means that setting up a distributed system with local Windows user accounts is not possible as it was with earlier product versions (2.13 and earlier).

A certificate is required to secure the communication between PCM600 and SQL Server.



PCMSERVER2014 Users — PCMSERVER2014 SQL Server User Group

SQLServer2005SQLBro... — Members in the group have the required access a...

Description: PCMSERVER2014 SQL Server User Group

Members:
testuser1

Changes to a user's group membership are not effective until the next time the user logs on.

*Figure 7: PCMSERVER2014 Users group*

The server machine must share the directory defined by the %PCMDATADIRABB% system environment variable and the PCMSERVER2014 Users user group must be given full privileges to that directory. If the name “PCMDataBasesABB” is given to the share, the client automatically has the correct path in PCMDATADIRABB system environment variable after the client installation.

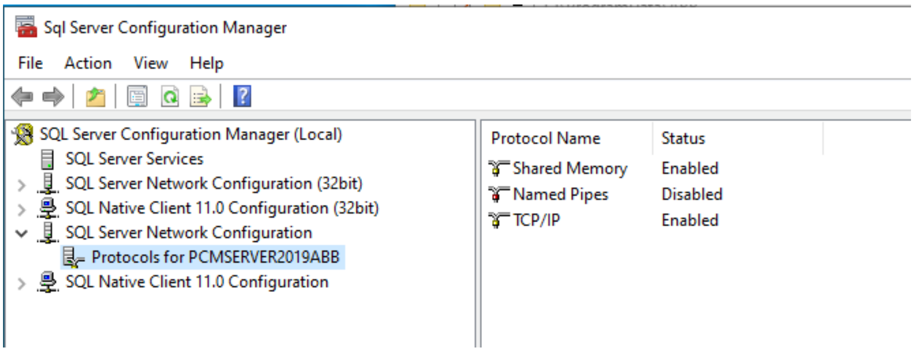
If the server machine has firewall, it needs to allow communication to two ports.

**Table 3: Ports for SQL Browser service and SQL Server**

| Port | Description |
|---|---|
| 1434/UDP | SQL Browser service |
| 1435/TCP by default | SQL Server |

If multiple PCM600 versions of Distributed PCM600 Servers are installed, unique available ports must be assigned for both SQL Browser service and SQL Server. The first installed Distributed PCM600 Server installation gets the default ports. If this is noticed after the installation, the ports can be changed and the repair action on PCM600 installer can be run for both server and client side.

The server uses the SQL Browser service to tell the client which port the server is listening to. The SQL Server port can be changed using SQL Server Configuration Manager.



Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 11.0 Configuration (32bit)
SQL Server Network Configuration
Protocols for PCMSERVER2019ABB
SQL Native Client 11.0 Configuration

| Protocol Name | Status |
|---|---|
| Shared Memory | Enabled |
| Named Pipes | Disabled |
| TCP/IP | Enabled |

*Figure 8: SQL Server Configuration Manager*

## 6.8.1 Installing PCM600 on client computer

1. Install PCM600 with option **Install only PCM600**.
2. Ensure that all users using PCM600 have domain user accounts. Both server and client machine must also have joined that domain.
   The PCMDATADIRABB system environment variable is automatically set to point to the shared folder of the server (PCMDataBasesABB, by default). If the server share name is not PCMDataBasesABB, the PCMDATADIRABB system environment variable must be set to point to the correct path. A UNC path must be used (for example, \\server\share).

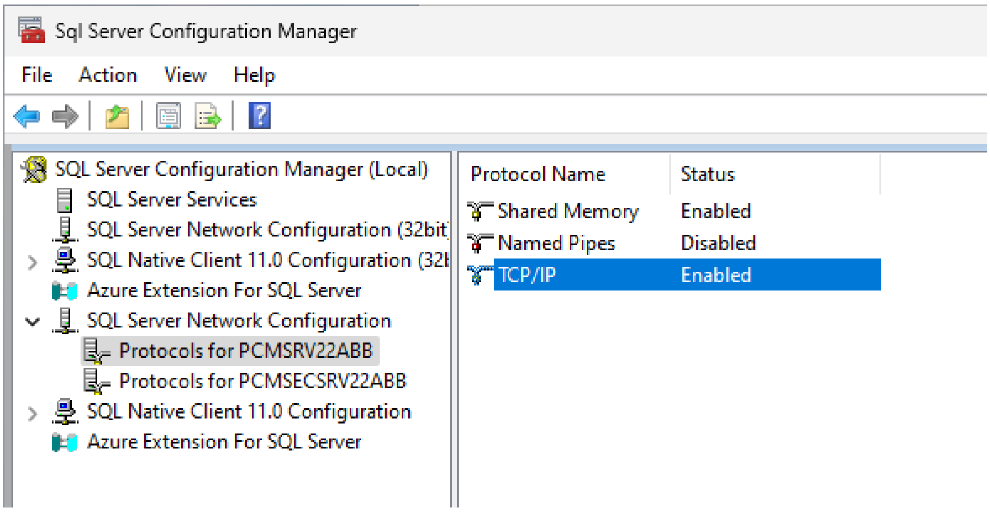
## 6.8.2 Installing PCM600 on SQL Server computer

1. Install PCM600 with option **Install only SQL Server**.
2. Ensure that all users using PCM600 have a domain user account.
3. Using lusrmgr.msc, add all regular PCM600 users to the **PCMSERVER2014 Users** group. In addition, add PCM600 security administrators to **PCM Security Administrators** group.
4. Share the **PCMDataBasesABB** folder (with full control) with all PCM600 users.

5. Configure the SQL Server Browser service to start up automatically and start it if it is not running.
6. Ensure that the firewall allows communication with SQL Server Browser (port UDP 1434).
7. Start **Sql Server Configuration Manager** (SQLServerManager16.msc).
8. Enable TCP/IP for PCMSRV22ABB by right-clicking selecting **Enable**.

   Restart the server instance in **SQL Server Services** tree node.

   Repeat same for PCMSECSRV22ABB.


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit
SQL Native Client 11.0 Configuration (32l
Azure Extension For SQL Server
SQL Server Network Configuration
Protocols for PCMSRV22ABB
Protocols for PCMSECSRV22ABB
SQL Native Client 11.0 Configuration
Azure Extension For SQL Server

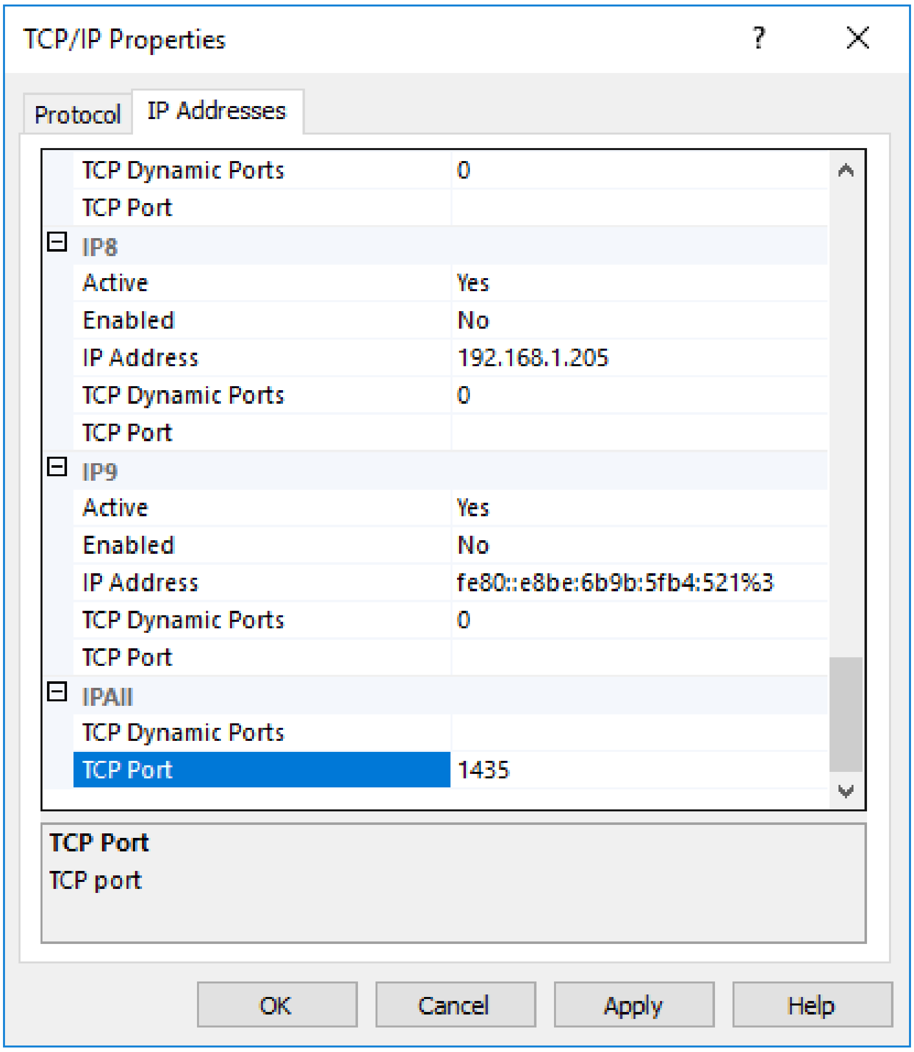
| Protocol Name | Status |
|---|---|
| Shared Memory | Enabled |
| Named Pipes | Disabled |
| TCP/IP | Enabled |

*Figure 9: Enabling TCP/IP for PCMSRV22ABB in Sql Server Configuration Manager*

9. Configure a port for both SQL Server instances PCMSRV22ABB.

a) Right-click **TCP/IP** and select **Properties**.

b) On the **IP Addresses** tab, scroll down to the **IPAll** section, leave TCP Dynamic Ports empty and specify a port number (for example, 1435, but use different port for each server instance) in the **TCP Port** field.



TCP/IP Properties

| | |
|---|---|
| TCP Dynamic Ports | 0 |
| TCP Port | |
| IP8 | |
| Active | Yes |
| Enabled | No |
| IP Address | 192.168.1.205 |
| TCP Dynamic Ports | 0 |
| TCP Port | |
| IP9 | |
| Active | Yes |
| Enabled | No |
| IP Address | fe80::e8be:6b9b:5fb4:521%3 |
| TCP Dynamic Ports | 0 |
| TCP Port | |
| IPAll | |
| TCP Dynamic Ports | |
| TCP Port | 1435 |

**TCP Port**

TCP port

*Figure 10: Defining a port number for SQL Server*

10. Click **OK** and restart the server instance.
11. Configure the computer firewall to allow traffic to port specified in step 9.
12. Repeat the port configuration (steps 8-11) also for PCMSECSRV22ABB.
13. Allow inbound TCP communication to the selected port in the Windows firewall for both SQL Server instances.

    The executable files are typically

    - `C:\Program Files\Microsoft SQL Server\MSSQL16.PCMSRV22ABB\MSSQL\Binn\sqlservr.exe`
    - `C:\Program Files\Microsoft SQL Server\MSSQL16.PCMSECSRV22ABB\MSSQL\Binn\sqlservr.exe`

### 6.8.3 Uninstalling PCM600

PCM600 can be uninstalled from Apps and Features (Programs and Features). The program name is “ABB Protection and Control IED Manager PCM600”. Some included programs and runtimes, for example ABB IED Connectivity Packages, Wavewin ABB and SQL Server instances used by PCM600, can only be uninstalled separately as they could be used by other programs.

### 6.8.4 Securing the communication between PCM600 and SQL Server

PCM600 and SQL Server uses TCP/IP for communication when distributed installation is used. That communication is not encrypted by default and is vulnerable for network-based attacks especially if the network is not private.

PCM600 forces encryption of the TCP/IP communication to make it secure. Securing the communication requires using a suitable certificate and configuring the SQL Server to use encryption.

#### 6.8.4.1 Getting a certificate

The certificate used for communication encryption must contain both public and private keys. The best way to get a certificate is to purchase it from a well-known certificate authority. It guarantees that the certificate can be verified and trusted. It makes certificate maintenance (like renewing and revoking) also easier.

Ensure that the host name set in the certificate matches the host name given when installing PCM600 to client computers.

A self-signed certificate can also be used if

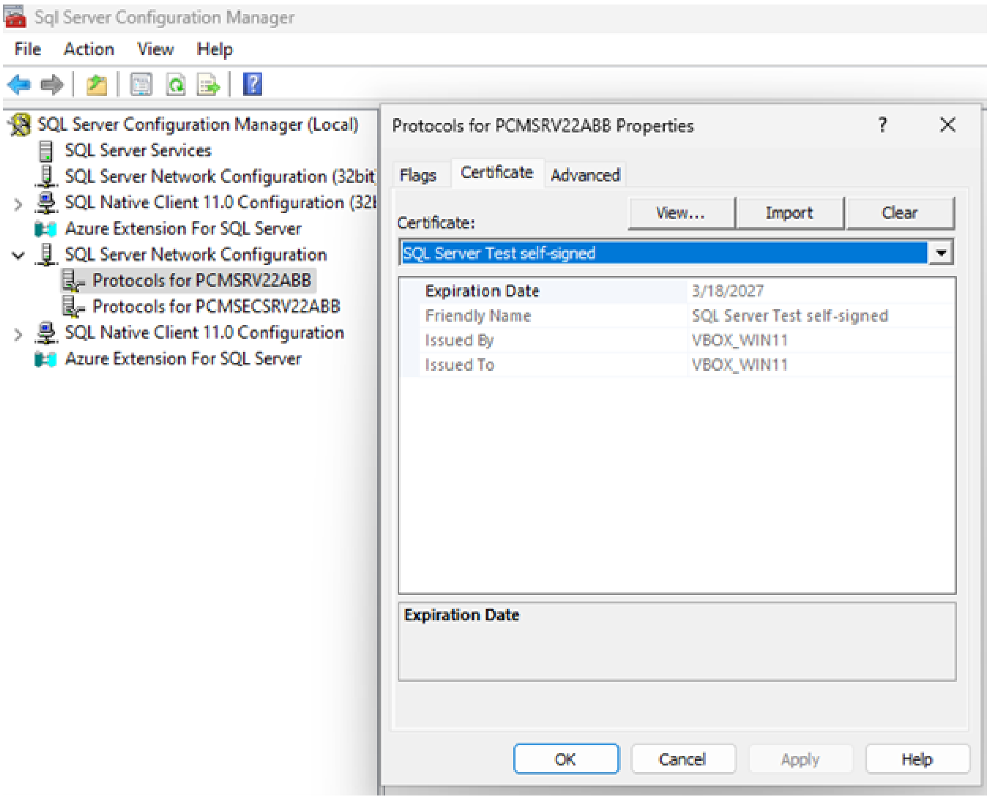
- Risks related to self-signed certificates are accepted
- The self-signed certificate is installed in Trusted Root Certification Authorities folder on all client computers

#### 6.8.4.2 Configuring SQL Server

The encryption is enabled in Sql Server Configuration Manager using the following steps

1. Follow instructions in *Chapter 6.8 Distributed installation of PCM600* to enable TCP/IP communication and configure the server computer.
2. Start **Sql Server Configuration Manager** (SQLServerManager16.msc) .
3. Select **SQL Server Network Configuration**.
4. Open properties for “Protocols for PCMSRV22ABB”.
5. Select **Certificate** tab.
6. Select **Import** and proceed with importing your certificate.
7. Click **OK** and re-open the properties window.

8. Select the imported certificate from drop down list on **Certificate** tab.


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit
SQL Native Client 11.0 Configuration (32I
Azure Extension For SQL Server
SQL Server Network Configuration
Protocols for PCMSRV22ABB
Protocols for PCMSECSRV22ABB
SQL Native Client 11.0 Configuration
Azure Extension For SQL Server
Protocols for PCMSRV22ABB Properties
Flags
Certificate
Advanced
View...
Import
Clear
OK
Cancel
Apply
Help

Certificate: SQL Server Test self-signed

| | |
|---|---|
| Expiration Date | 3/18/2027 |
| Friendly Name | SQL Server Test self-signed |
| Issued By | VBOX_WIN11 |
| Issued To | VBOX_WIN11 |

Expiration Date

*Figure 11: Selecting the imported certificate*

9. Select **Flags** tab.
10. Set Force Encryption to “Yes”.
11. Click **OK**.
12. Select **SQL Server Services** from the left.
13. Right-click SQL Server (PCMSRV22ABB) and select **Restart**.
14. Repeat the steps 4-13 for PCMSECSRV22ABB.
15. Give SQL Server instances permission to access the certificate private key.

a) Open MMC (Microsoft Management Console).
MMC can be found by typing “MMC” in Windows search field in task bar.

b) Add a new “Certificates” snap-in for “computer account”.

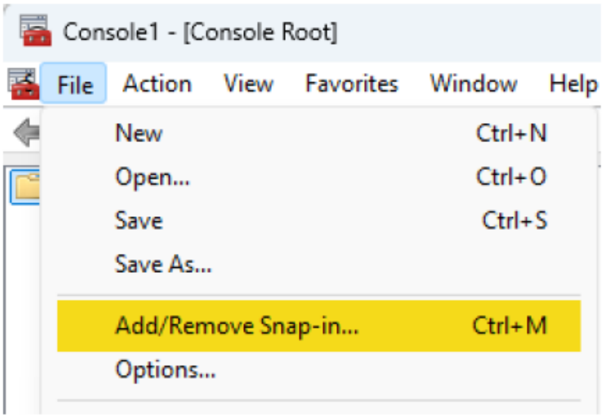
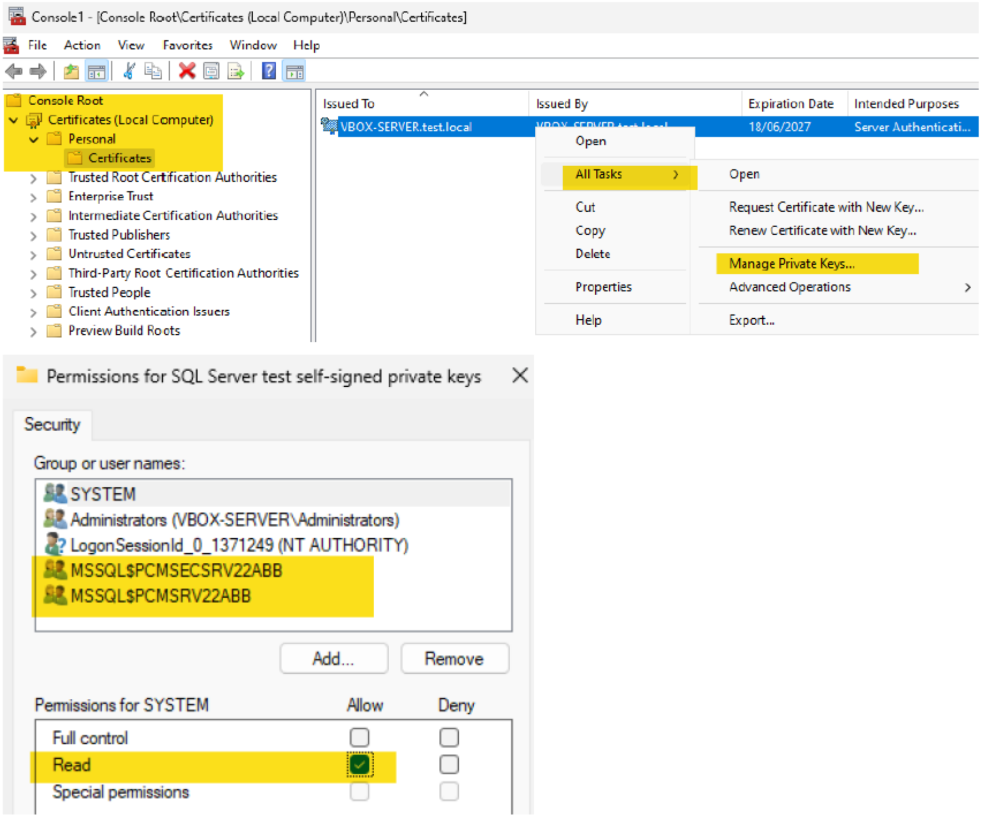


*Figure 12: Adding a new snap-in*

c) Manage private keys for the imported certificate.


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Preview Build Roots
Issued To
Issued By
Expiration Date
Intended Purposes
VBOX-SERVER.test.local
18/06/2027
Server Authenticati...
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Manage Private Keys...
Advanced Operations
Export...
Permissions for SQL Server test self-signed private keys
Security
Group or user names:
SYSTEM
Administrators (VBOX-SERVER\Administrators)
LogonSessionId_0_1371249 (NT AUTHORITY)
MSSQL$PCMSECSRV22ABB
MSSQL$PCMSRV22ABB
Add...
Remove

| Permissions for SYSTEM | Allow | Deny |
|---|---|---|
| Full control | □ | □ |
| Read | ☑ | □ |
| Special permissions | □ | □ |

*Figure 13: Managing private keys*

16. Restart both SQL Server instances.

## 6.9 Disabling of devices

It is recommended to disable any unused devices in the system, such as USB ports, CD/DVD drives, communication ports, or floppy disc controllers. Devices are disabled manually in devmgmt.msc (Device Manager).

**Disabling of autorun functionality**

If it is not possible to disable a device, disable the autorun functionality of the device. The autorun functionality is disabled to prevent the automatic start of the malicious code contained in a removable device. For more information, search how to disable the Autorun functionality in Windows.

## 6.10 Secure boot

PCM600 does not create specific requirements for secure boot. Secure boot should be implemented with organization specific de facto procedures, if needed. Secure boot has to be configured manually.

## 6.11 Isolation techniques

PCM600 Update Manager connects to Internet and it is a separate process from PCM600. It is recommended that there is more than one network interface and a dedicated network interface is connected to the Internet. This has to be configured manually.

## 6.12 User Account Control

User Account Control (UAC) is a security feature in Windows 7, Windows Server 2008 R2 and the later versions. UAC is recommended to be enabled in PCM600 and in computers that are used to access PCM600.

**Table 4: Actions if the program requires privilege elevation**

| User role | Action |
|---|---|
| Administrators | A dialog is shown for selecting Continue or Cancel. In Windows Server edition, Prompt for consent is used for non-Windows binaries. |
| Standard users | A message box is shown stating that a program has been blocked. This setting was introduced in Windows 7, Server 2008 R2 and the later versions. |

A shield in the program icon indicates that it requires administrative privileges to run. This is automatically detected by the operating system, if for example, Run as administrator flag is set in the file properties, or if the program has previously asked for administrative privileges.

It is not recommended to use administrator accounts by default. It is recommended to create limited user accounts that have privileges only to perform the necessary tasks related to the user role.

## 6.13 Intrusion detection system

An intrusion detection system (IDS) is a device or software application that monitors the network or system activities for malicious activities or policy violations and produces reports to the management station. It is recommended that organization specific IDS; to be configured manually, is deployed on the computer running PCM600.

## 6.14 Configuring of SQL Server for PCM600

PCM600 requires access to the PCMSRV22ABB and PCMSECSRV22ABB instances of SQL Server. All PCM600 users must be added to PCMSERVER2014 Users Group in Windows to provide access. PCM600 security administrators must be added also to PCM Security Administrators group.

During installation, the user logged in is automatically added to PCMSERVER2014 Users and PCM Security Administrator group. The user logged also gets a dedicated administrator access to SQL Server.

If additional users are required, they must be added to PCMSERVER2014 Users (and PCM Security Administrators group if user is security administrator of PCM600). This can be done by using lusrmgr.msc – Local Users and Groups (Local). The local Users and Groups function provides a possibility to add both local and network user accounts to the user groups.

# 7 Project backups and restoring

Backups can be created by either backing up the computer running PCM600 or by using the functionality in PCM600 that exports the project configuration to a single file.

A project can be backed up by using PCM600 backup functionality and storing the backup files in a safe location. It's important to keep backups of your substation projects so users can manage and restore configurations easily. It is important to take and manage the project backups of the engineered substations. This enables proper configuration management for the users.

## 7.1 Creating a backup of a project

1. On the **File** menu, click **Open** and select **Manage Project** to open the project management.
2. Click **Backup Projects** functionality.
3. Select the projects from the list of available projects.
4. Click **Backup Selected**.
5. Browse the target location and click **OK**.

Creating a project backup makes it easy to transfer multiple projects between computers.

## 7.2 Restoring a project

1. On the **File** menu, click **Open** and select **Manage Project** to open the project management.
2. Right-click **Projects on my computer**, and click **Import** to open the **Import project** dialog box.
3. Browse the location and type the name for the imported file.

A new project is created containing all the data from the imported file.

## 7.3 Backup file integrity

PCM600 backup file format's integrity is checked when a file of that type is imported to PCM600.

This means the following files with following file extensions:

- APCMA
- APCMP
- APCMI
- APCMT

The following functionalities are affected:

- Project Export/Import
- IED Export/Import
- IED Template creation
- Create from template

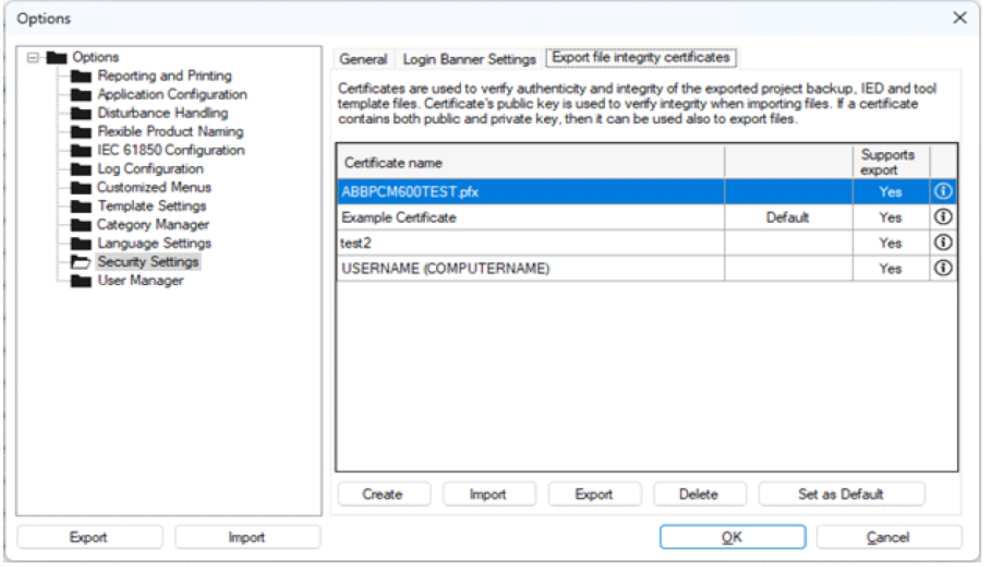
Integrity is ensured by using Certificates. They are stored as User Certificates. When PCM600 is opened first time by user, new certificate is created if none exists in the user store. The user can manage certifications via **PCM600 Options** > **Security Settings** > **Backup file certificates**.

In general, exported backups/templates and exported public key certificates should be stored and shared separately from each other.

## 7.4 Certificate Management

### 7.4.1 Security Settings

Each row in dialog represents one installed certificate in User Store. Certificate name identifies a certificate. One of the certificates can be assigned as Default certificate which is used by default in operations.



Certificates are used to verify authenticity and integrity of the exported project backup, IED and tool template files. Certificate's public key is used to verify integrity when importing files. If a certificate contains both public and private key, then it can be used also to export files.

| Certificate name | | Supports export | |
|---|---|---|---|
| ABBPCM600TEST.pfx | | Yes | ⓘ |
| Example Certificate | Default | Yes | ⓘ |
| test2 | | Yes | ⓘ |
| USERNAME (COMPUTERNAME) | | Yes | ⓘ |

*Figure 14: Security settings*

**Supports export** column informs the user whether the certificate can be used by export functionality (ie. Contains private key). Last column displays tooltip giving additional information regarding certificate issuer.

## 7.4.2 Create New Certificate

The user can create a new certificate. Certificate name is requested when a certificate is created.

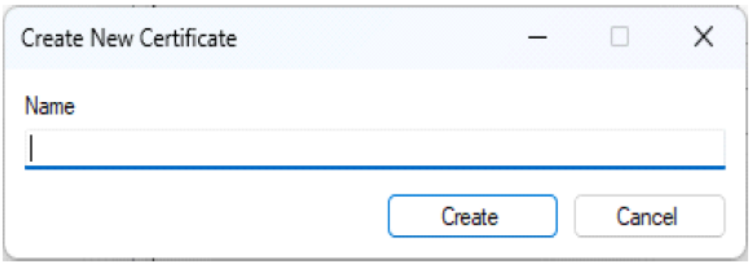
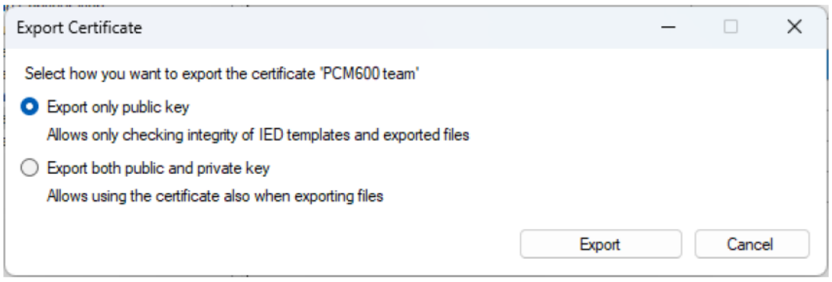


*Figure 15: Naming a new certificate*

## 7.4.3 Export Certificate

The user can export certificates to be used in another PC. Certificates can be exported with or without a private key.



Export Certificate

Select how you want to export the certificate 'PCM600 team'

● Export only public key

Allows only checking integrity of IED templates and exported files

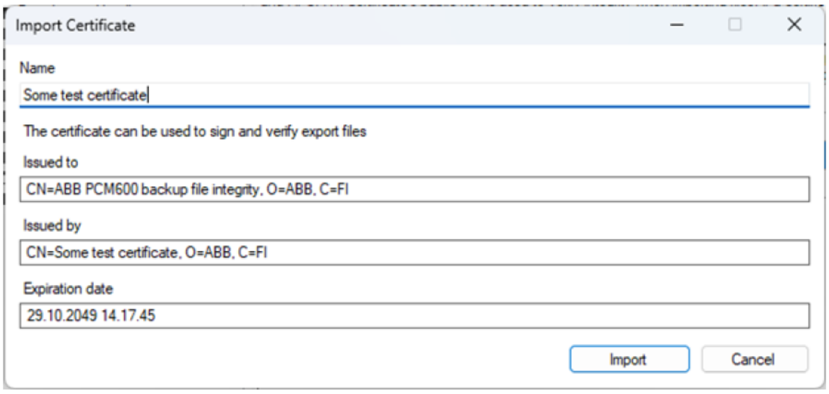
○ Export both public and private key

Allows using the certificate also when exporting files

*Figure 16: Exporting a certificate*

## 7.4.4 Import Certificate

The user can import a certificate from another PCM Installation or by 3rd party. Certificate information is displayed when imported certificate is selected. When importing backup/template file to a different PC, the corresponding certificate has to be transferred also.



Import Certificate

Name: Some test certificate

The certificate can be used to sign and verify export files

Issued to: CN=ABB PCM600 backup file integrity, O=ABB, C=FI

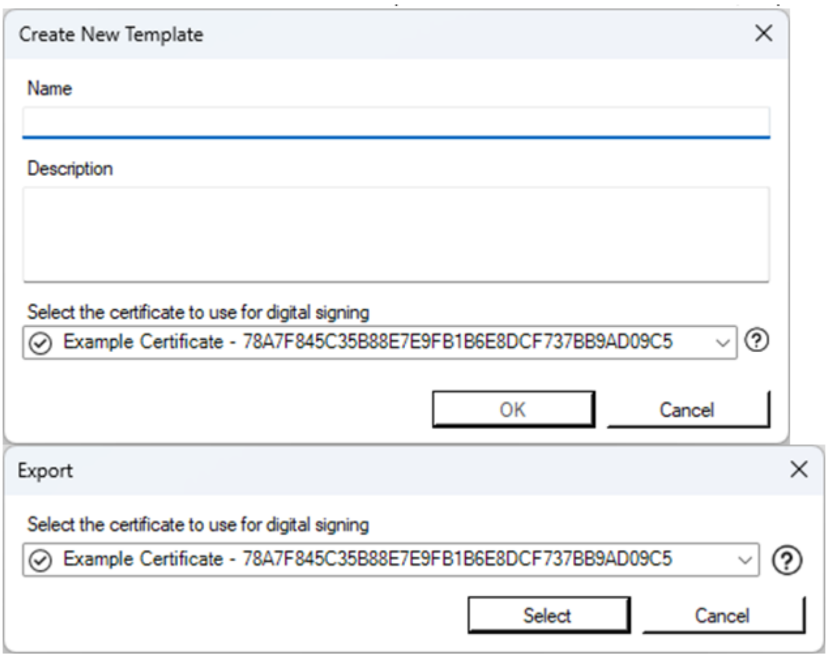
Issued by: CN=Some test certificate, O=ABB, C=FI

Expiration date: 29.10.2049 14.17.45

*Figure 17: Importing a certificate*

## 7.4.5 Certificate Selections

A certificate is requested from the user when template creation or export operations are done.



Select the certificate to use for digital signing: Example Certificate - 78A7F845C35B88E7E9FB1B6E8DCF737BB9AD09C5

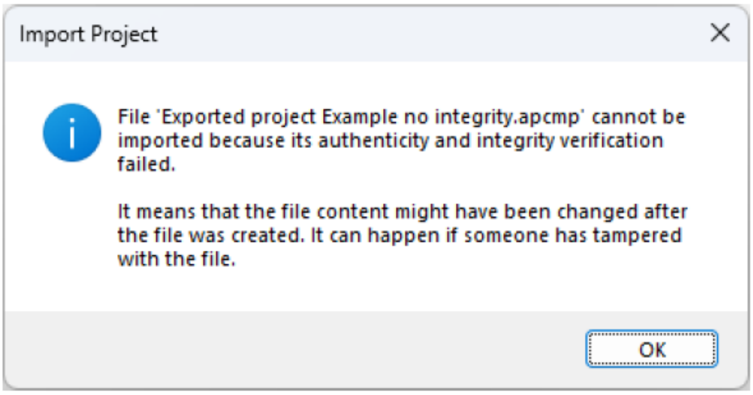
Select the certificate to use for digital signing: Example Certificate - 78A7F845C35B88E7E9FB1B6E8DCF737BB9AD09C5

*Figure 18: Certificate selections*

## 7.4.6 Integrity file missing

Import behavior depends on the security level setting of PCM600.

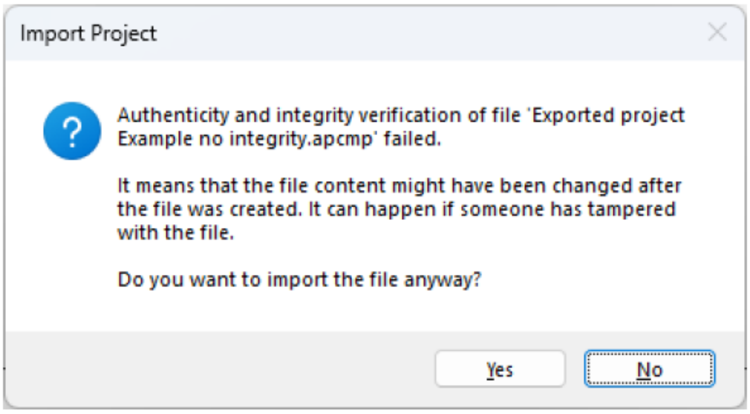
- High: unsigned files cannot be imported
- Medium: user can select to import unsigned file
- Low: unsigned file is imported



File 'Exported project Example no integrity.apcmp' cannot be imported because its authenticity and integrity verification failed.

It means that the file content might have been changed after the file was created. It can happen if someone has tampered with the file.

*Figure 19: High dialog when integrity file is missing*



Import Project

Authenticity and integrity verification of file 'Exported project Example no integrity.apcmp' failed.

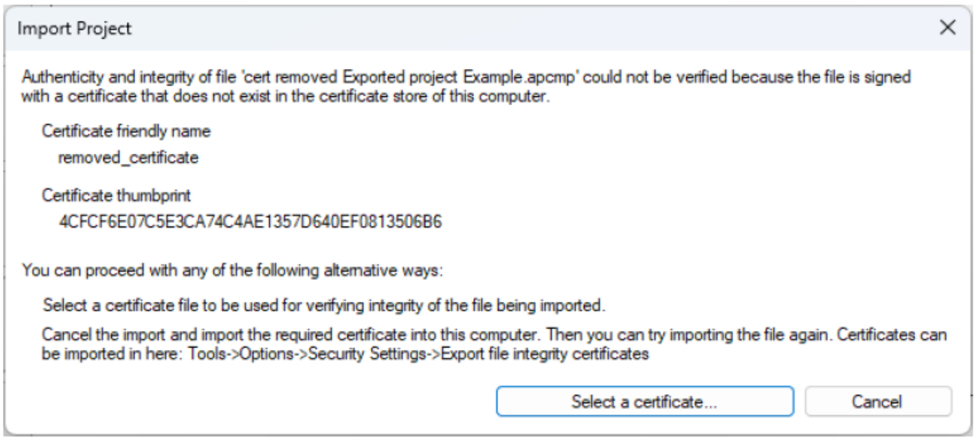
It means that the file content might have been changed after the file was created. It can happen if someone has tampered with the file.

Do you want to import the file anyway?

*Figure 20: Medium dialog when integrity file is missing*

## 7.4.7 Certificate missing from certificate store

- High: the user is asked to provide a path to certificate file
- Medium/Low: the user is asked to provide a path to certificate file or the project can be imported without verifying its authenticity and integrity



Import Project

Authenticity and integrity of file 'cert removed Exported project Example.apcmp' could not be verified because the file is signed with a certificate that does not exist in the certificate store of this computer.

Certificate friendly name
removed_certificate

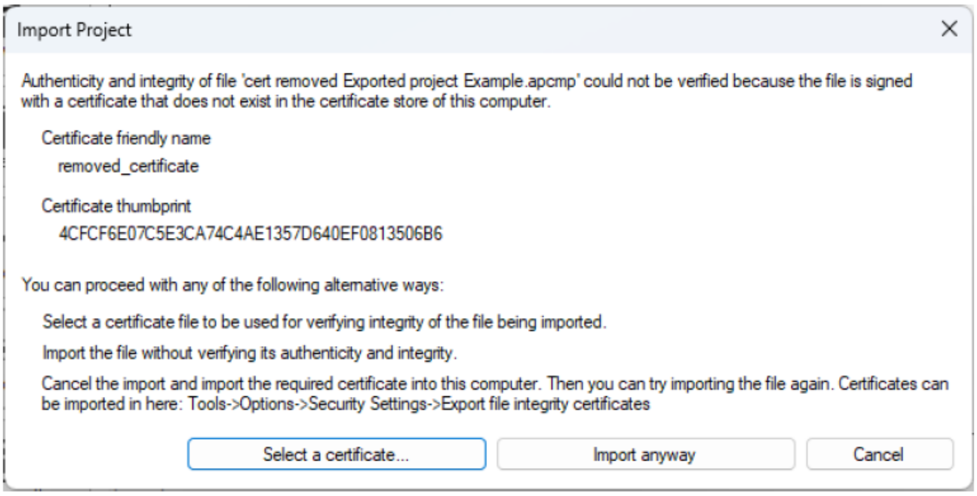
Certificate thumbprint
4CFCF6E07C5E3CA74C4AE1357D640EF0813506B6

You can proceed with any of the following alternative ways:

Select a certificate file to be used for verifying integrity of the file being imported.

Cancel the import and import the required certificate into this computer. Then you can try importing the file again. Certificates can be imported in here: Tools->Options->Security Settings->Export file integrity certificates

*Figure 21: High dialog when certificate is missing from certificate store*



Authenticity and integrity of file 'cert removed Exported project Example.apcmp' could not be verified because the file is signed with a certificate that does not exist in the certificate store of this computer.

Certificate friendly name
removed_certificate

Certificate thumbprint
4CFCF6E07C5E3CA74C4AE1357D640EF0813506B6

You can proceed with any of the following alternative ways:

Select a certificate file to be used for verifying integrity of the file being imported.

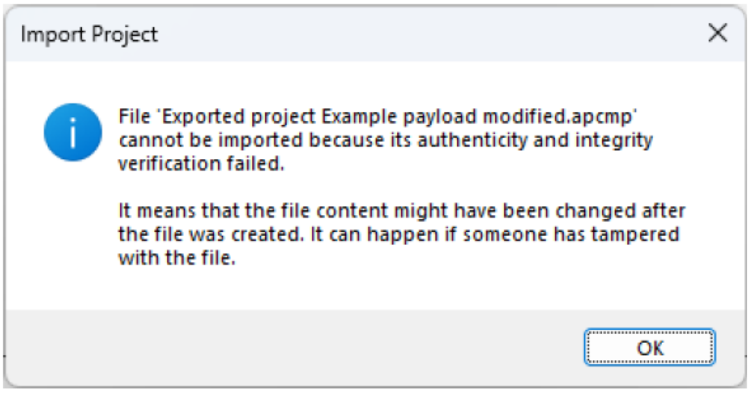
Import the file without verifying its authenticity and integrity.

Cancel the import and import the required certificate into this computer. Then you can try importing the file again. Certificates can be imported in here: Tools->Options->Security Settings->Export file integrity certificates

*Figure 22: Medium/Low dialog when certificate is missing from certificate store*

## 7.4.8 Payload tampered

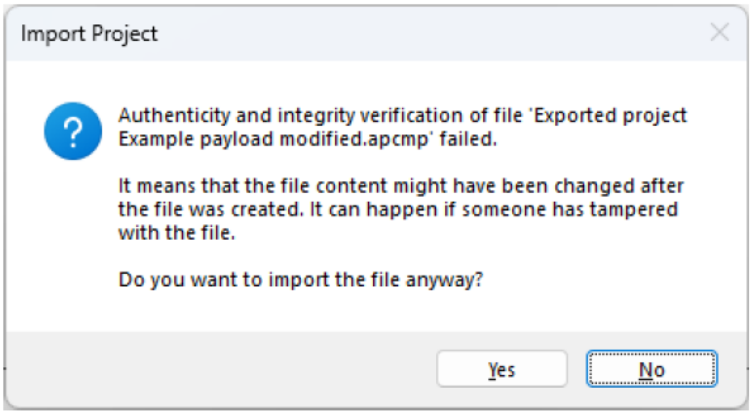
- High: import is prevented
- Medium/Low: the user can import the file



File 'Exported project Example payload modified.apcmp' cannot be imported because its authenticity and integrity verification failed.

It means that the file content might have been changed after the file was created. It can happen if someone has tampered with the file.

*Figure 23: High dialog when payload is tampered*



Authenticity and integrity verification of file 'Exported project Example payload modified.apcmp' failed.

It means that the file content might have been changed after the file was created. It can happen if someone has tampered with the file.

Do you want to import the file anyway?

*Figure 24: Medium/Low dialog when payload is tampered*

Backups/exports done in earlier versions of PCM600 2.14 do not contain necessary information for integrity check which means that the information dialog will be shown.

# 8 Standard compliance statement

Cyber security issues have been the subject of standardization initiatives by ISA, IEEE or IEC for some time. 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, such as IEC 62351 and IEC 62443 (former ISA S99), are still under active development. ABB participates 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 available in the market, for example, VPN for secure Ethernet communication.

**Table 5: Overview of cyber security standards**

| Standard | Main focus | Status |
|---|---|---|
| NERC CIP | NERC CIP cyber security regulation for North American power utilities | Released, ongoing [1] |
| IEC 62351 | Data and communications security | Partly released, ongoing |
| IEEE 1686 | IEEE standard for substation intelligent electronic devices (IEDs) cyber security capabilities | Finalized |

ABB has identified cyber security as a key requirement and has developed a large number of product features to support the international cyber security standards such as NERC CIP, IEEE 1686, as well as local activities like the German BDEW white paper.

[1] Ongoing: major changes will affect the final solution

# 9 Glossary

| | |
|---|---|
| BDEW | Bundesverband der Energie- und Wasserwirtschaft |
| Connectivity package | A collection of software and information related to a specific protection and control IED, providing system products and tools to connect and interact with the IED |
| 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. |
| Ethernet | A standard for connecting a family of frame-based computer networking technologies into a LAN |
| FTP | File transfer protocol |
| FTPS | FTP Secure |
| IDS | Intrusion detection system |
| IEC | International Electrotechnical Commission |
| IEC 60870-5-104 | Network access for IEC 60870-5-101 |
| IEC 61850 | International standard for substation communication and modeling |
| IED | Intelligent electronic device |
| IEEE | Institute of Electrical and Electronics Engineers, Inc. |
| IEEE 1686 | Standard for Substation Intelligent Electronic Devices' (IEDs') Cyber Security Capabilities |
| IP | Internet protocol |
| ISO | International Standard Organization |
| LAN | Local area network |
| NERC CIP | North American Electric Reliability Corporation - Critical Infrastructure Protection |
| OS | Operating system |
| PCM600 | Protection and Control IED Manager |
| TCP | Transmission Control Protocol |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TLS | Transport layer security |
| UAC | User account control |
| VPN | Virtual Private Network |
| WHMI | Web human-machine interface |

—

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

**abb.com/mediumvoltage**
**abb.com/relion**
**go.abb/digitalsubstations**

© Copyright 2025 ABB. All rights reserved.