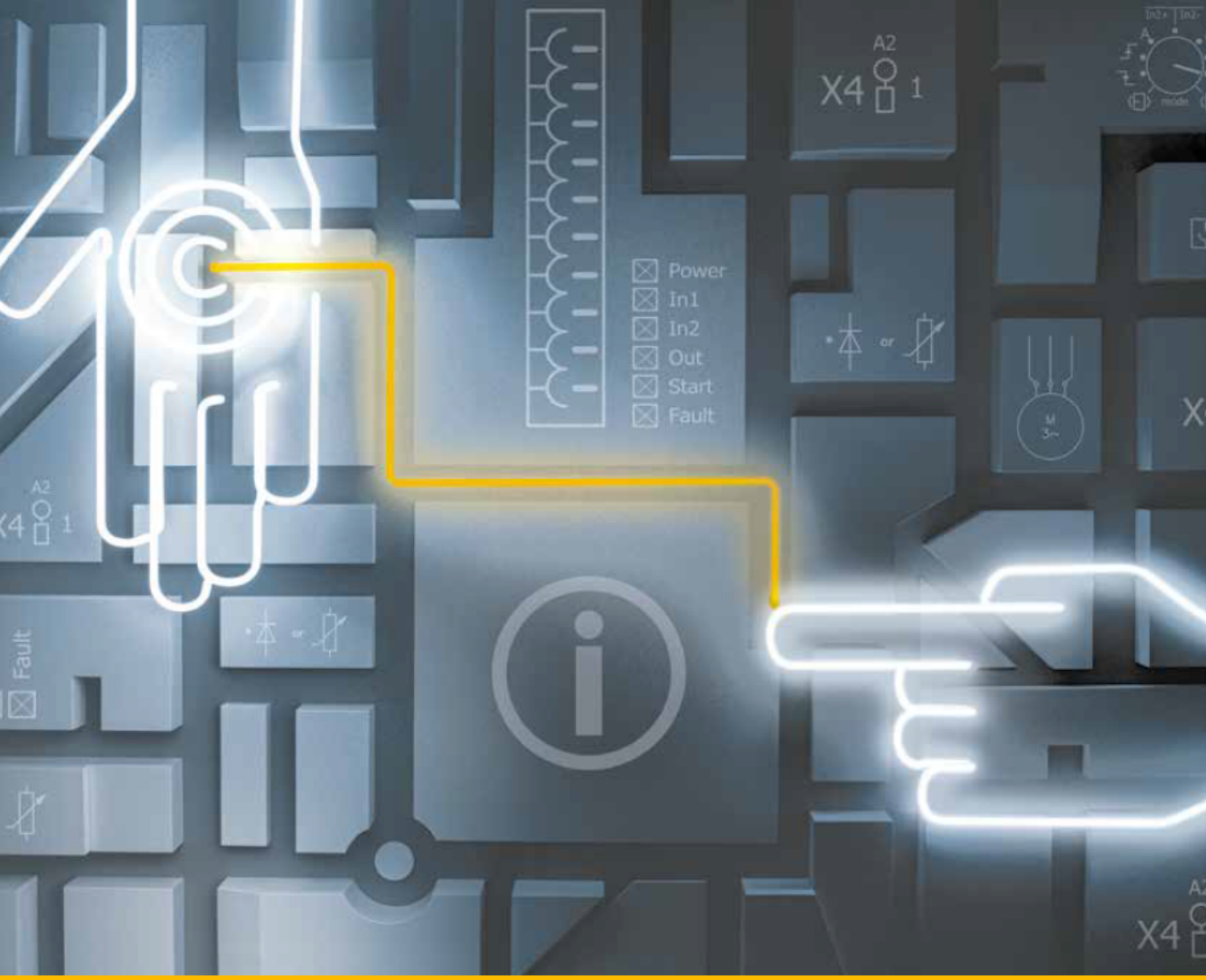


PIT Windows Logon

PILZ
THE SPIRIT OF SAFETY

Operating Manual-1007324-EN-03
- User software




This document is the original document.

Where unavoidable, for reasons of readability, the masculine form has been selected when formulating this document. We do assure you that all persons are regarded without discrimination and on an equal basis.

1 Introduction

1.1 Validity of documentation

This operating manual is valid for the software PIT Windows Logon from Version 1.0.0.

1.2 Using the documentation

This document is intended for instruction. Only install and commission the product if you have read and understood this document. The document should be retained for future reference.

1.3 Terminology

PITreader

The term "PITreader" includes all RFID authentication systems from PILZ GmbH & Co. KG on which authentication is via a transponder.

The following can be used as transponders, for example:

- PITreader transponder key
- PITreader transponder cards
- PITreader transponder sticker

The term "PITreader" is always used when the description applies to all product types.

PITreader Key

The term "PITreader Key" includes all PITreader product types on which only a PITreader transponder key can be used for authentication. The PITreader transponder key is inserted into the read head for this purpose.

One product type is the PITreader S base unit, for example.

The term "PITreader Key" is always used when the description applies exclusively to these product types.

PITreader Card

The term "PITreader Card" includes all PITreader product types on which the following transponders can be used for authentication:

- PITreader transponder card
- PITreader transponder sticker
- PITreader transponder key

The PITreader transponder is held in front of the read head for this purpose.

One product type is the PITreader S card unit, for example.

The term "PITreader Card" is always used when the description applies exclusively to these product types.

1.4 Definition of symbols

Information that is particularly important is identified as follows:

DANGER!

This warning must be heeded! It warns of a hazardous situation that poses an immediate threat of serious injury and death and indicates preventive measures that can be taken.

WARNING!

This warning must be heeded! It warns of a hazardous situation that could lead to serious injury and death and indicates preventive measures that can be taken.

CAUTION!

This refers to a hazard that can lead to a less serious or minor injury plus material damage, and also provides information on preventive measures that can be taken.

NOTICE

This describes a situation in which the product or devices could be damaged and also provides information on preventive measures that can be taken. It also highlights areas within the text that are of particular importance.

INFORMATION

This gives advice on applications and provides information on special features.

2 Safety and Security

2.1 Intended use

2.1.1 Product

The software PIT Windows Logon is used to authenticate, authorise and log user logins on Windows PCs. It is intended exclusively as an extension to the PITreader. Authentication is via RFID transponder.

2.1.2 Application ranges

PIT Windows Logon is used in industrial and commercial environments where secure access to Windows PCs is required.

2.1.3 Application conditions

Use only in conjunction with the hardware and software components provided.

Compliance with the conditions of use for PITreader and compatible RFID transponders.

2.1.4 Use of qualified personnel

Installation, programming, configuration, commissioning, operation, decommissioning and maintenance of the software may only be carried out by persons qualified to do so.

A qualified person has specialised knowledge in the following areas:

- IT security and network security, including current threats and protective measures
- Application of relevant safety standards and directives
- Knowledge of the applicable national and European regulations on security and data protection

We recommend that the operator only employs persons who

- are familiar with the basic regulations on information security and protection against cyber attacks,
- have read and understood the section on "Safety and Security" in this description,
- know and are able to apply the safety directives and standards applicable to the specific application.

2.1.5 Prerequisites for operation

- Functional PITreader hardware
- Compatible RFID transponders
- Windows PC with supported operating system
- Latest security updates and virus protection on the PC

This document is intended for instruction. Only install and commission the product if you have read and understood this document.

2.1.6 Specific measures for intended use

No specific measures are required for intended use.

2.1.7 Improper use

The following is deemed improper use in particular:

- Any modification to the product,
- Use of the product outside the areas described in this document.

2.1.8 Security environment

The device must be installed on a state-of-the-art hardened end device in a secure network.

2.1.9 Third-party manufacturer licence information

The product contains open source software, whose terms of use could further limit the product's application area. It is essential that you observe the third-party manufacturer licence information.

More detailed information is available in the product PIT Windows Logon by selecting ***About*** and then clicking on the ***Open Source licences*** button.

2.2 General security information

To protect plants, systems, machines and networks against cyberthreats it is necessary to implement (and continuously maintain) an overall Industrial Security concept that is state of the art.
Carry out a risk assessment in accordance with VDI/VDE 2182 or IEC 62443-3-2 and plan the security measures with care.

If you have any questions about implementation, please contact technical support at support@pilz.com.

You can reach the Pilz Product Security Incident Response Team (PSIRT) at https://www.pilz.com/psirt.
With regard to a Pilz product, this is where you can:

- Report security vulnerabilities and security incidents
- Ask questions about security vulnerabilities and security incidents
- View Security Advisories

2.3 Security measures

2.3.1 Implemented security measures

PIT Windows Logon protects the confidentiality, integrity and authenticity of all the system's data and functions through the following implemented security measures:

- Windows access data is stored in encrypted form only and with a rotating cryptographic key.
- Cross-device communication is always authenticated and encrypted to ensure data integrity and confidentiality.
- The PIT Windows Logon Key is stored in encrypted form on the transponders and cannot be read from a PITreader.
- Sensitive and confidential data as well as PIT Windows Logon settings can only be accessed on a Windows PC with a user account with administrator rights.

2.3.2 Required external security measures

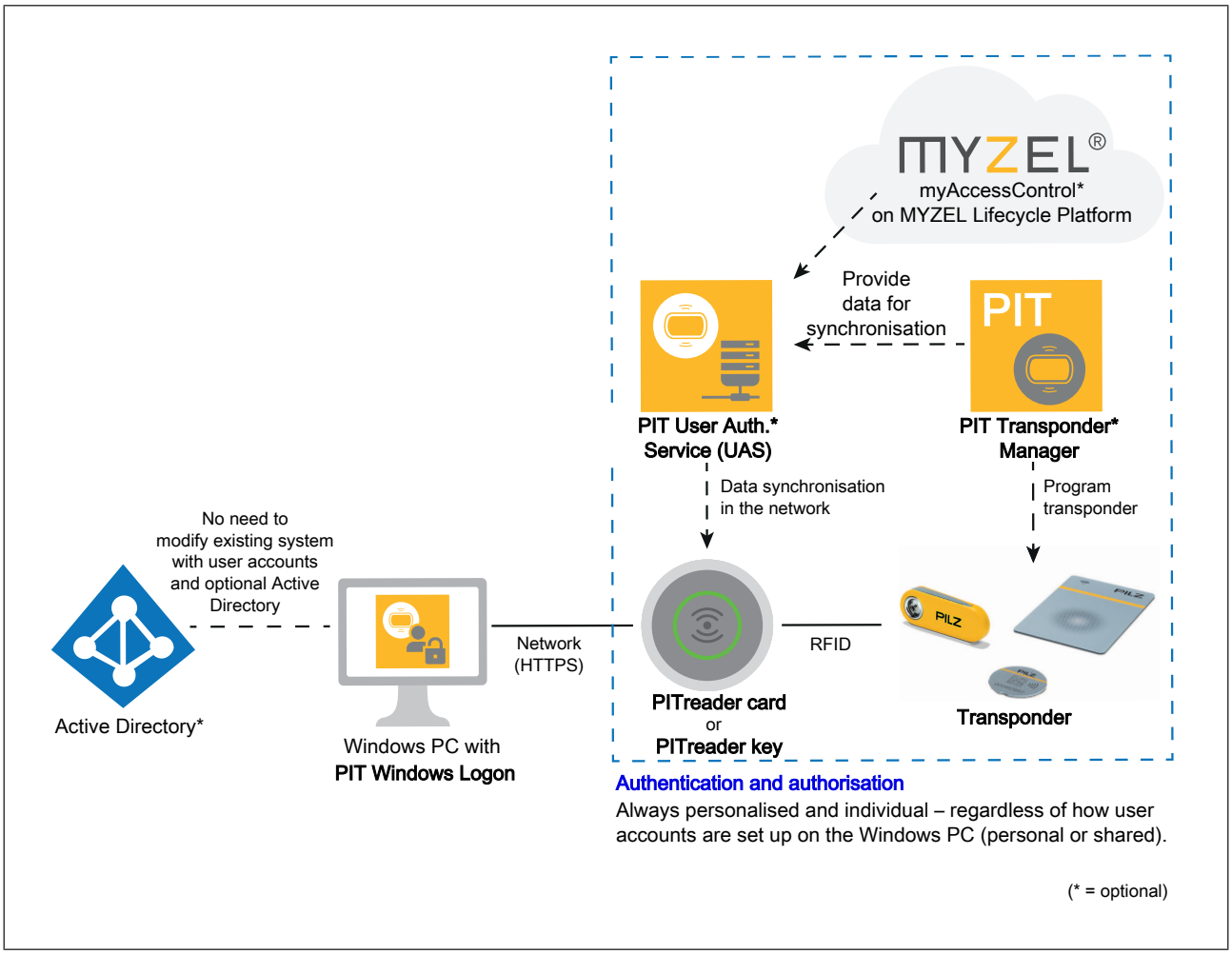
For the secure operation of PIT Windows Logon, it is your responsibility to implement the following additional measures at the system boundaries:

- Generate a secure PIT Windows Logon Key, see Generate and manage PIT Windows Logon Key [📖 30].
- Keep the PIT Windows Logon Key in a secure place, see Generate and manage PIT Windows Logon Key [📖 30].

- Use a PITreader with basic coding. Ensure that the basic coding is only known to the persons responsible for the installation.
- Limit administrative access on the Windows PC on which PIT Windows Logon is used. Only grant access to authorised persons who are responsible for managing access to this PC and are authorised to do so.
- Check system integrity and log data regularly.
- Update software in accordance with the manufacturer's recommendation.

3 Overview

With the software PIT Windows Logon, you can use PITreader and transponders to log in to Windows PCs without a password. Each person uses an individually configured transponder. There is no need to enter a user name and password. Authentication and authorisation are always carried out on a personal basis via PITreader. They are independent of the granularity of the user accounts in Windows. You can use the PIT User Authentication Service, the PIT Transponder Manager or myAccessControl on the MYZEL Lifecycle Platform as an option.



In order to use this function, the configuration must be carried out using the software "PIT Windows Logon Config UI", which is installed on a PC with a Windows operating system.

3.1 System requirements

Minimum requirement:

- Windows 10 operating system (64-bit), version 1909 or higher
- PITreader firmware version from 02.03.01

3.2 System components

PIT Windows Logon installs its own Windows Credential Provider, which integrates itself into the Windows login screen.

Communication between the Credential Provider and Windows is via the PIT Windows Logon Service.

The configuration of the installation and the assignment of transponders to Windows users takes place via the user interface PIT Windows Logon Config UI.

Properties of the PIT Windows Logon Service

- **Service name:** PITWindowsLogonService
- **Display name:** PIT Windows Logon Service
- **Service account:** Local system
- **Start type:** Automatic

Properties of the PIT Windows Logon Credential Provider

- **Component:** PITWindowsLogonCredentialProvider.dll
  A Windows component to display and process login information during login.
- **Function:** Extension of the Windows login screen
  This function supplements the standard "Change password" function.
- **CLSID:** 611814b0-cb75-4cdf-9bce-d459b38469aa

4 Function description

4.1 Application scenarios for PIT Windows Logon

PIT Windows Logon supports two basic application scenarios:

- Shared user accounts
- Personal user accounts

Regardless of the application scenario, login is always personalised. Each login is individually authenticated, authorised and logged.

After successful authorisation, an optional assignment to shared Windows user accounts can be made.

Permission management is based on the proven principle with:

- Support for device groups
- Control of permissions per station via the PITreader device groups
- Option for centralised administration via the PIT User Authentication Service (UAS)

Shared user accounts

Several people access one or more non-personal Windows user accounts together. This is often the case in a manufacturing environment.

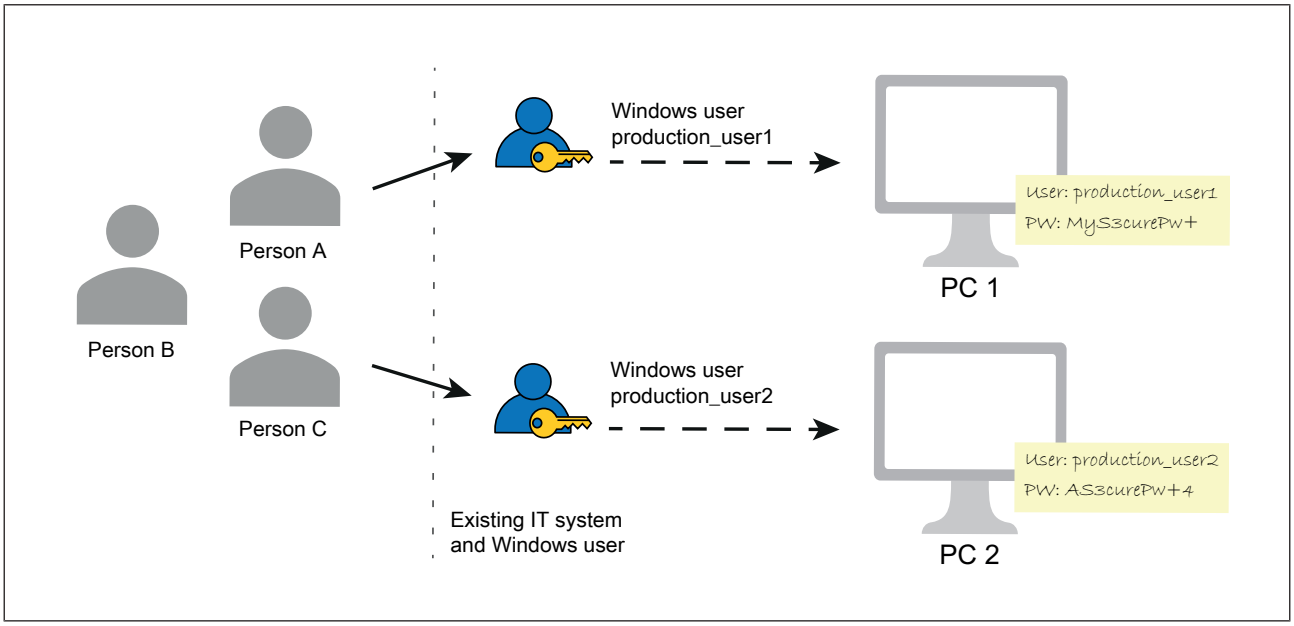


Fig.: Typical installation without PIT Windows Logon

Unique, personal authentication and authorisation are carried out via PITreader, transponders and other components in the Identification and Access Management System from Pilz. This happens outside of the Windows system. There is no need to modify existing installations in production plants without personal user accounts. Access can still be controlled and monitored on an individual personal basis.

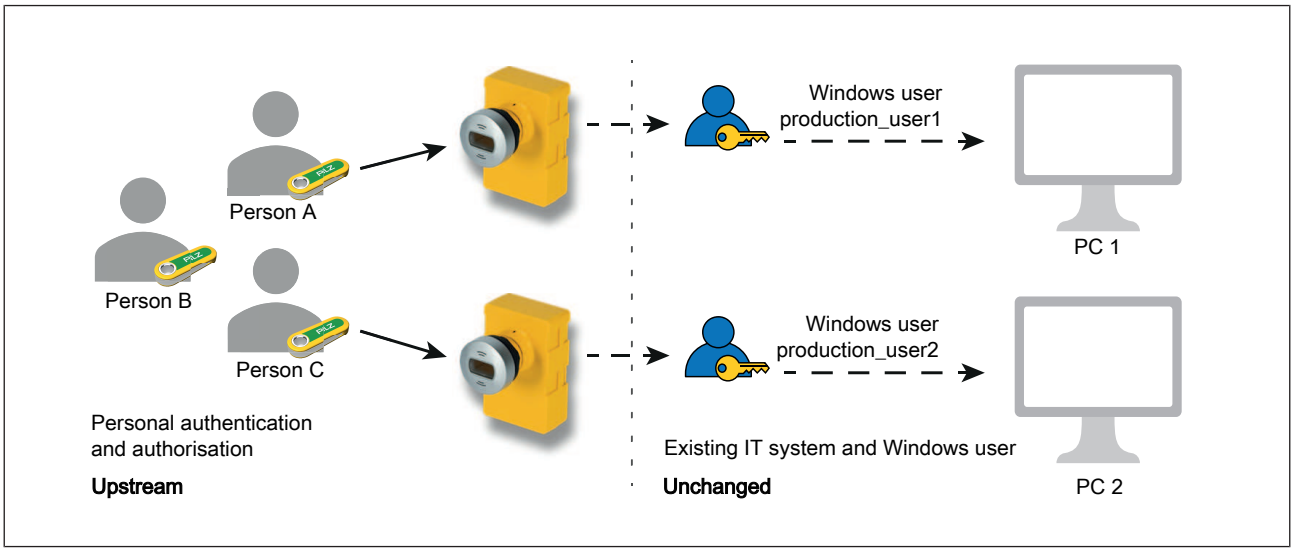
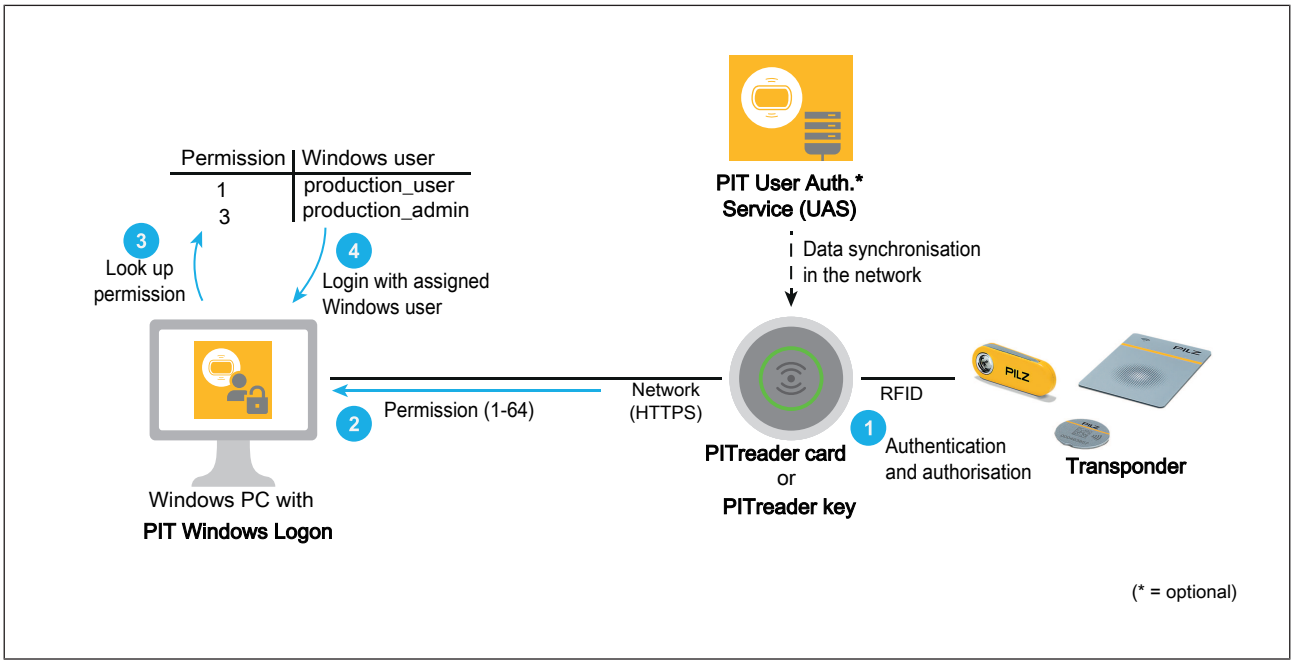


Fig.: Adding PITreader and PIT Windows Logon to the existing installation

New employees or employees with only temporary authorisation can be created in the PIT Transponder Manager, for example. Permissions for employees and transponders can also be edited there. Changes can be made without having to adjust the configuration of the Windows PC or the user rights in the Active Directory.

Windows accounts are assigned to transponders via the transponder's permission (0 to 64). This applies per PC. It is therefore flexible and adaptable, and can be scaled as required.

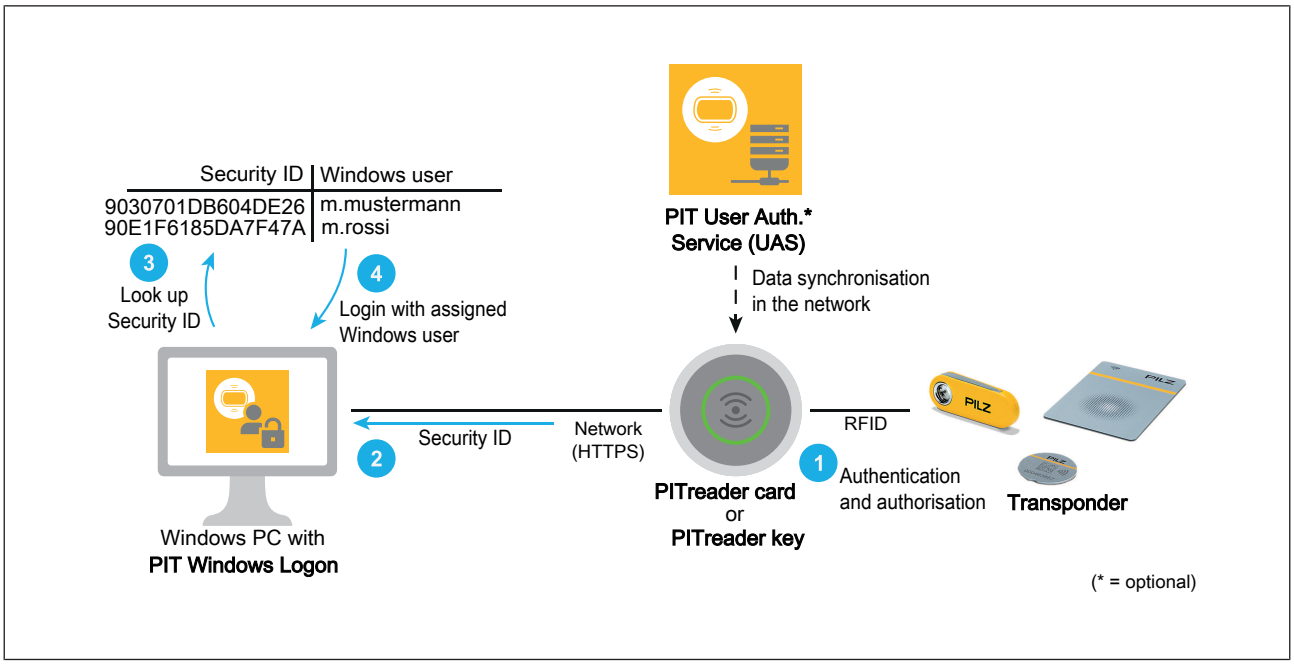


	Function:
[1]	Authentication and authorisation are via the PITreader. This is based on the data on the transponder, the permission list or data provided by the PIT User Authentication Service (UAS). The authenticated permission is determined in the process.
[2]	PIT Windows Logon receives the authenticated permission (0 to 64) from the PITreader.

[3]	PIT Windows Logon assigns the permission to a Windows user account. The assignment is created using the PIT Windows Logon Config UI and stored securely on the PC.
[4]	The assigned Windows user account is used to log in to the PC.

Personal user accounts

An account can be uniquely assigned to a transponder for the use of personal Windows accounts. This assignment is made via the transponder's Security ID. The Security ID is a unique identifier, which cannot be manipulated or duplicated. This restricts the user account to a specific transponder. Login is password-free and takes place exclusively via this transponder.



	Function:
[1]	Authentication and authorisation are via the PITreader. This is based on the data on the transponder, the permission list or data provided by the PIT User Authentication Service (UAS). The authenticated permission is determined in the process.
[2]	PIT Windows Logon receives the transponder's authenticated Security ID from the PITreader.
[3]	PIT Windows Logon assigns the Security ID to a Windows user account. The assignment is created using the PIT Windows Logon Config UI and is stored securely on the PC.
[4]	The assigned Windows user account is used to log in to the PC.

4.2 Optional functions

Automatic logon

The ***Automatic logon*** function can be activated in PIT Windows Logon, see Configure function settings [📖 27].

If the function is activated, the user is logged into the Windows system automatically. Login takes place as soon as a transponder with an assigned user account is detected.

Automatic lock

The ***Automatic lock*** function can be activated in PIT Windows Logon, see Configure function settings [📖 27].

If the function is activated, the screen is locked automatically. The transponder is locked as soon as it is removed from the reading range of the PITreader.

Self-registration

The ***Enable self-registration for users*** function can be activated in PIT Windows Logon, see Configure function settings [📖 27].

If the function is activated, a user can register an unassigned transponder. Registration is via the Windows login screen. The user enters the user name and password for their Windows account. The assignment is saved in the personal user account using the transponder's Security ID.

Change password

The ***Change password*** function can be activated in PIT Windows Logon, see Configure function settings [📖 27].

PIT Windows Logon integrates itself into the Windows screen for changing the password. When passwords are changed, the encrypted data record for the access data is updated.

If a password has been changed outside of PIT Windows Logon, it can be updated via the PIT Windows Logon Config UI.

Alternatively, the current password can be entered during the next login via a transponder.

4.3 Security through the PIT Windows Logon Key

The security of the PIT Windows Logon system is based on the PIT Windows Logon Key – a security key, which you can define yourself.

PIT Windows Logon Key

- You define an individual AES-256 key.
- This key is stored securely on the transponders.
- The key encrypts and decrypts your Windows access data.

Protection mechanisms

- The stored key cannot be read.
- The access data has double protection:
  - through the transponder with the PIT Windows Logon Key
  - through the PITreader with appropriate coding

High security thanks to combined access requirements

With PIT Windows Logon, access to your Windows PC is secured by a combination of the following three components:

- Encrypted access data
- PITreader with appropriate coding
- Transponder with customised key

Additional security measures

- The access data remains in the Windows system and is not transferred via external interfaces.
- The access data is secured with a rotating key, which changes each time it is used.

5 Install PIT Windows Logon

Prerequisites

- The PC is switched on.
- You have administrator rights on the Windows PC.
- CodeMeter Runtime is installed, see Install CodeMeter Runtime [39].
- The PIT Windows Logon licence is activated in CodeMeter Runtime, see Licensing [47].

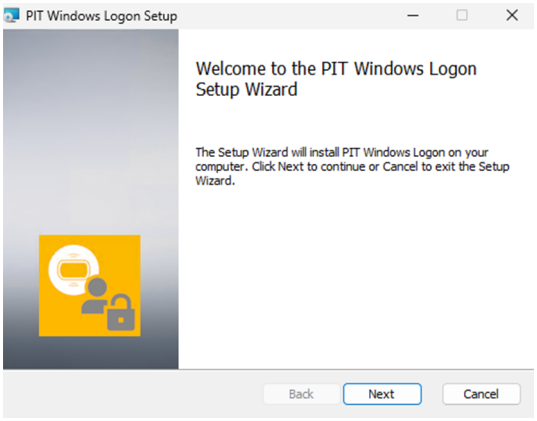
KeePass 2 with KeePassHttp plugin can be used to secure the PIT Windows Logon Key.

Procedure

1. Open the Pilz E-Shop, https://www.pilz.com/eshop.
2. Login with your access data.
3. Enter one of the following options in the search field:
   the product ID for PIT Windows Logon, see Order reference [49]
   or
   the term "PIT Windows Logon"
4. Select the folder "PITWindowsLogon_<Version>.zip".
5. Click on ***Download***.

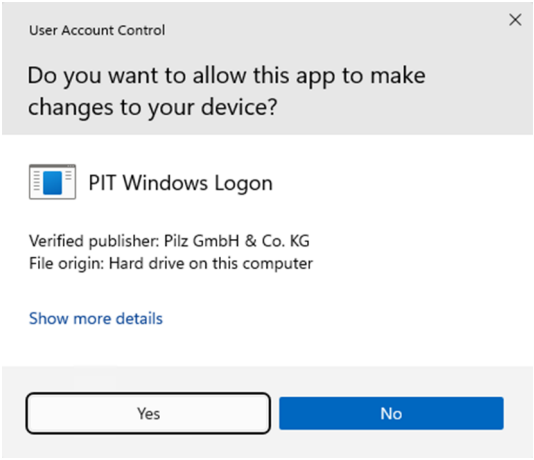
   The zip file is downloaded.
6. Unpack the zip file.
7. Double-click on the installation file "PITWindowsLogon_<Version>msi".

   The setup window is displayed:



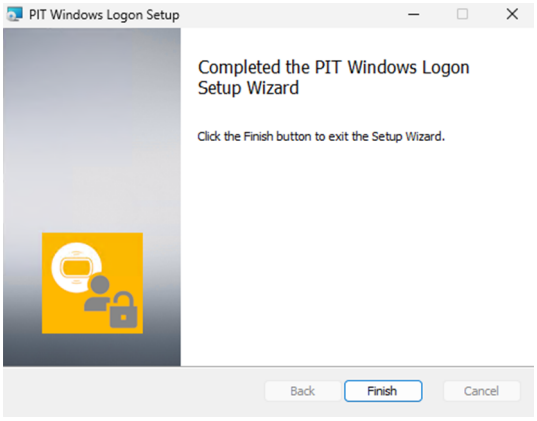
8. Click ***Next*** to start the installation wizard.
9. Follow the instructions in the setup:
   Accept the licence conditions.
   Adjust the installation path if necessary.
10. Click on ***Install***.

    If the ***User account control*** menu appears:



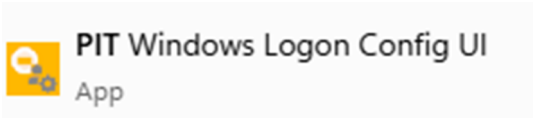
Click ***Yes*** first.

PIT Windows Logon is installed. The following window then appears:



11. Click ***Finish*** to complete the installation.

    An icon with the name "PIT Windows Logon Config UI" is added to the Windows start menu:



    You can use this icon to configure further system settings, see Configure PIT Windows Logon [20].

6 Configure PIT Windows Logon

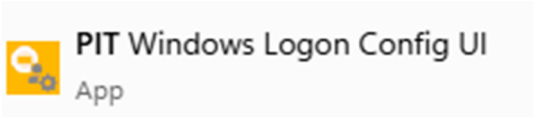
6.1 Start PIT Windows Logon Config UI

Prerequisites

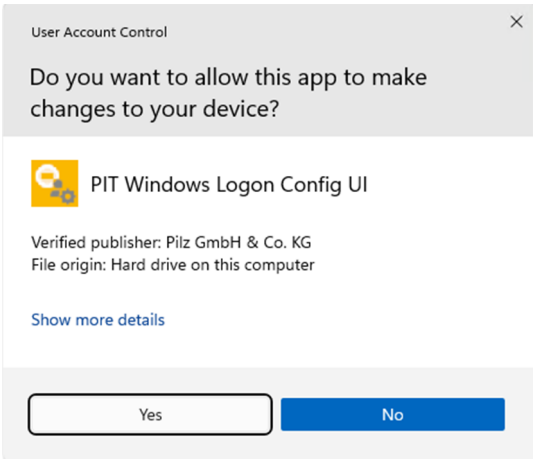
- The PC is switched on.
- You have installed PIT Windows Logon, Install PIT Windows Logon [📖 18].

Procedure

1. In the Windows Start menu, Click on the PIT Windows Logon Config UI icon:

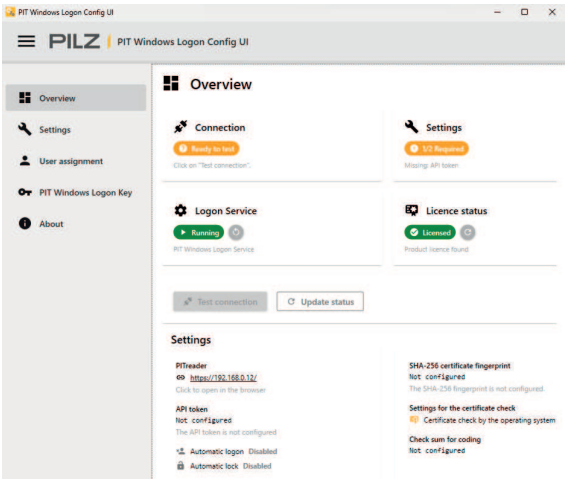


If the ***User account control*** menu appears:

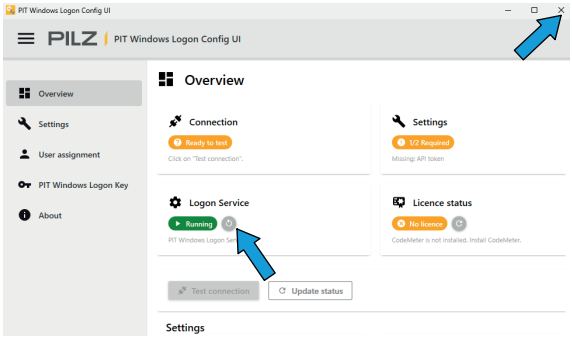


Click ***Yes*** first.

The configuration menu is displayed:

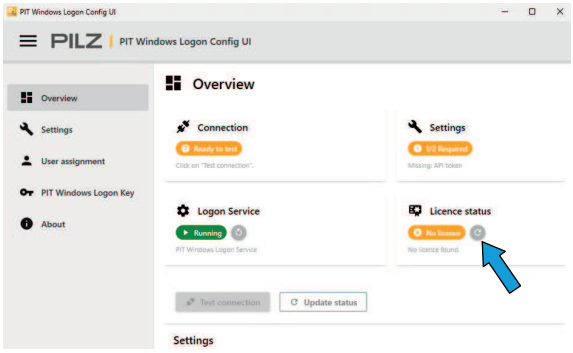


6.1.1 If CodeMeter Runtime is not yet installed



After starting PIT Windows Logon Config UI, the message appears briefly:
The licence check failed. ***CodeMeter is not installed. Install CodeMeter.***
You can also see this information in the configuration menu under ***Licence status***.

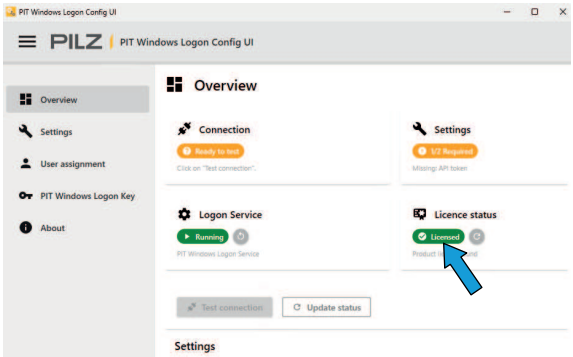
1. Install CodeMeter Runtime, see Install CodeMeter Runtime [📖 39].
2. Restart the ***Logon Service***. To do this, press the corresponding button.
3. Close PIT Windows Logon Config UI. To do this, press the "X" in the top right-hand corner.
4. Start PIT Windows Logon Config UI, see Start PIT Windows Logon Config UI [📖 20].



After starting PIT Windows Logon Config UI, the message appears briefly: ***The licence check failed. No product licence was found***. You can also see this information in the configuration menu under ***Licence status***.

5. Activate the PIT Windows Logon licence in CodeMeter Runtime, see Licensing [📖 47].
6. Refresh the ***Licence status*** display. To do this, press the corresponding button.

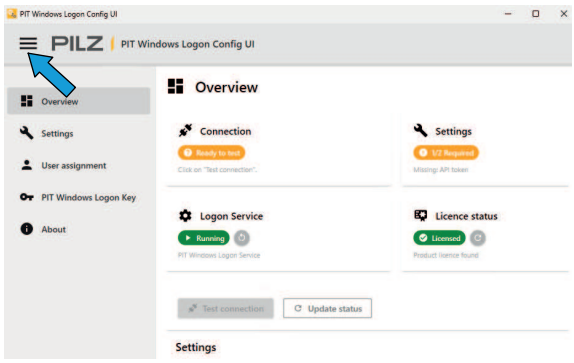
   The status is displayed in green:



6.2 Set language

Prerequisites

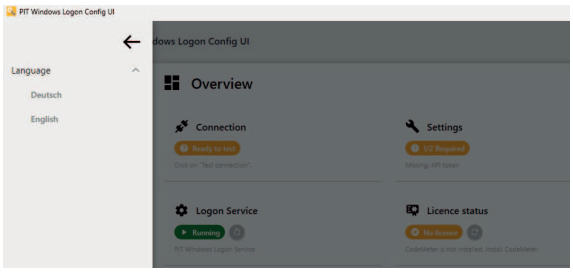
- PIT Windows Logon Config UI is started, see Start PIT Windows Logon Config UI [20].



Procedure

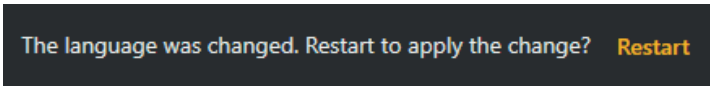
1. Click on the burger menu in the top left corner.

   The ***Language*** drop-down menu is displayed:



2. Open the ***Language*** drop-down menu and select ***English*** or ***Deutsch***.

   A prompt message appears briefly at the bottom, in the selected language, e.g:



3. Click on the yellow prompt text, e.g. ***Restart***.

   PIT Windows Logon Config UI is restarted and displayed in the selected language.

6.3 Create basic configuration

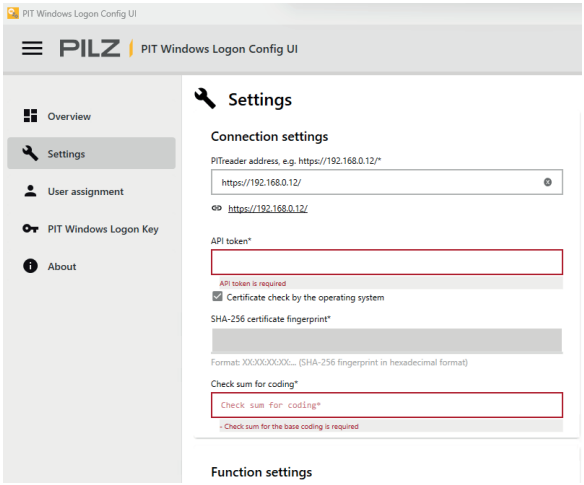
Prerequisites

- The PITreader is installed and connected to the PC, see PITreader operating manual (1004806).
- The PITreader's web application can be configured, see PITreader operating manual (1004806).
- The basic coding in the PITreader must be set, see PITreader operating manual (1004806).
- PIT Windows Logon Config UI is started, see Start PIT Windows Logon Config UI [20].
- You are logged into the PC as administrator.

Procedure

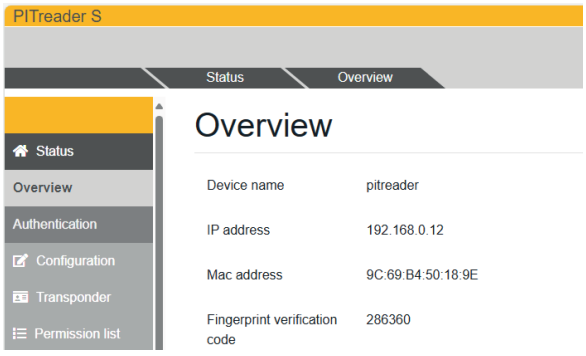
1. Click on ***Settings***.

   The ***Settings*** menu is displayed:



2. Open the PITreader web application, see PITreader operating manual (1004806).
3. Select ***Status*** in the web application.

   The ***Overview*** window is displayed:

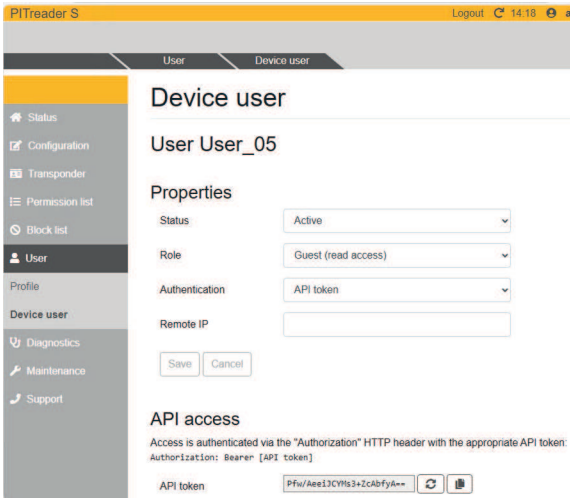


4. Copy the PITreader's ***IP address***.
5. Switch to PIT Windows Logon Config UI.

6. Under ***Connection settings***, paste the IP address copied from the PITreader into the field ***PITreader address, e.g. https://192.168.0.12/****.
7. Open the PITreader web application.
8. In the web application, select ***User -> Device user***.

   The ***Device user*** window is displayed.
9. Select the desired device user or create a new device user.
10. Under Properties, ***Role***, select ***Guest (read access)***.
11. Under Properties, ***Authentication***, select ***API token***.

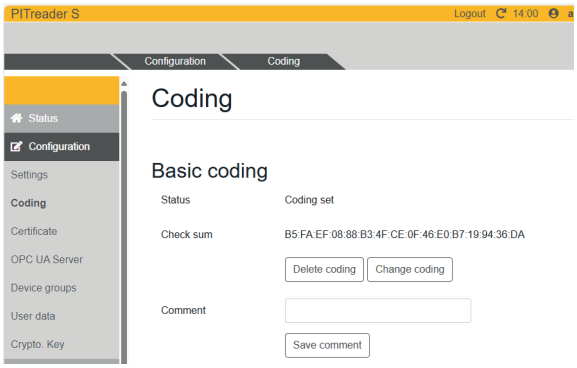
    The API token is generated and displayed:



12. Click ***Save***.

    The API token is saved.
13. Copy the displayed API token.
14. Switch to PIT Windows Logon Config UI.
15. Select the ***Settings*** menu.
16. Under ***Connection settings***, paste the copied API token into the field ***API token***.
17. Open the PITreader web application.
18. In the web application, select ***Configuration -> Coding***.

    The ***Coding*** window is displayed:



19. Copy the coding's check sum under ***Basic coding***, ***Check sum***.

20. Switch to PIT Windows Logon Config UI.
21. Select the ***Settings*** menu.
22. Under ***Connection settings***, paste the check sum copied from the web application into the field ***Check sum for coding***.
23. Click ***Save***.

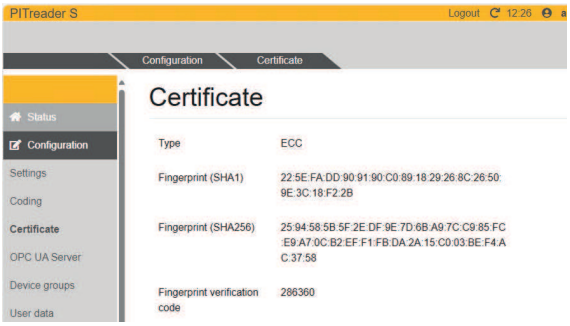
    All entries are saved. The message ***The PIT Windows Logon Service must be re-started*** appears top right.
24. In the top right corner, click the button next to the message.

    The service is restarted.

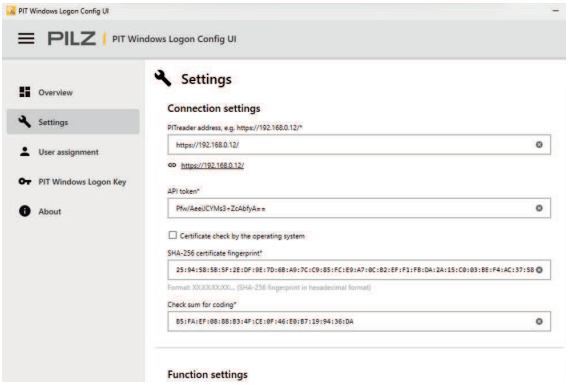
Optional: The certificate check is not to be performed by the operating system:

1. Open the PITreader web application, see PITreader operating manual (1004806).
2. In the web application, select ***Configuration -> Certificate***.

   The ***Certificate*** window is displayed:



3. Copy the fingerprint under ***Fingerprint (SHA256).***
4. Switch to PIT Windows Logon Config UI.
5. Deactivate the checkbox ***Certificate check by the operating system.***
6. Under ***Connection settings***, paste the fingerprint from the web application into the field ***SHA256 certificate fingerprint***.



7. Click ***Save***.

   All entries are saved. The message ***The PIT Windows Logon Service must be re-started*** appears top right.
8. In the top right corner, click the button next to the message.

The service is restarted.

6.4 Configure function settings

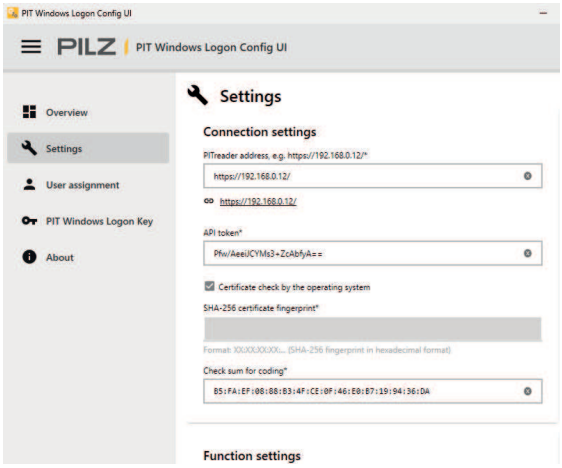
Prerequisites

- PIT Windows Logon Config UI is started, see Start PIT Windows Logon Config UI [20].
- You have carried out the basic configuration, see Create basic configuration [23].
- You are logged into the PC as administrator.

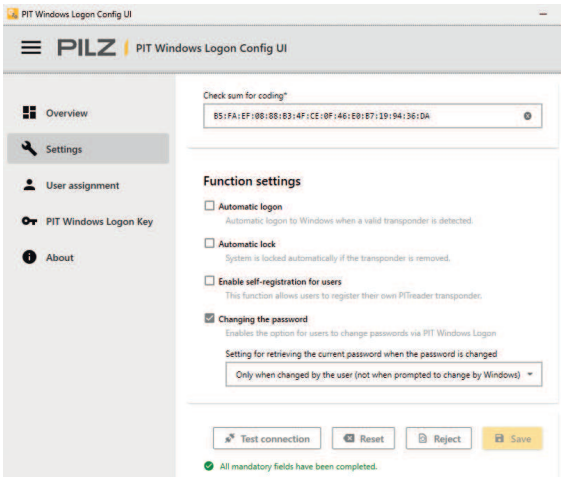
Procedure

1. Click on ***Settings***.

   The ***Settings*** menu is displayed:



2. Configure your individual settings under ***Function settings***, see Description of functions [28].



3. Click ***Save***.

   All entries are saved. The message ***The PIT Windows Logon Service must be re-started*** appears top right.

4. In the top right corner, click the button next to the message.

   The service is restarted.

6.4.1 Description of functions

6.4.1.1 Automatic logon

If the ***Automatic logon*** checkbox is activated:

If you position a valid transponder on the PITreader, you will automatically be logged in to the PC.

6.4.1.2 Automatic lock

If the ***Automatic lock*** checkbox is activated:

If you remove the registered transponder from the PITreader, you will automatically be logged out of the PC.

INFORMATION

The automatic lock function is only available if

- The PIT Windows Logon Service has been restarted and
- You have logged back in to your PC.

6.4.1.3 Enable self-registration for users

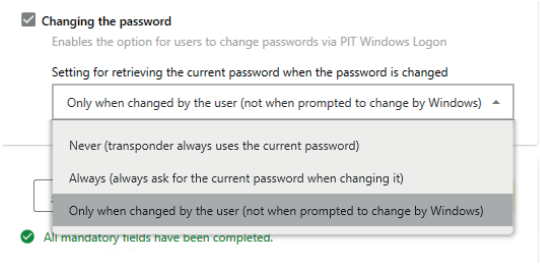
If

- the ***Enable self-registration for users*** checkbox is activated,
- the PIT Windows Logon Key is on the transponder, see Generate and manage PIT Windows Logon Key [30],
- a valid Windows user account exists on the PC:

Users can self-register their own transponder.

6.4.1.4 Changing the password

If the ***Changing the password*** checkbox is activated, you can select one of the following options from the drop-down menu:



- ***Never (transponder always uses the current password)***

  The current password is always taken from the transponder.
  When you change it, you will need to enter the new password twice on the Windows login screen.

- ***Always (always ask for the current password when changing it)***

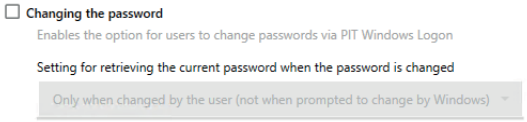
When you change it, you will need to enter the current password once and the new password twice on the Windows login screen.
This is Windows standard behaviour.

- ***Only when changed by the user (not when prompted to change by Windows)***

  If you initiate the password change on the PC using the Ctrl + Alt + Del keys:
  On the Windows login screen, you will need to enter the current password once and the new password twice.

  If Windows forces the change, due to an expired password for example, you can assign a new password without entering the current password.

If the ***Changing the password*** checkbox is deactivated:



The password is changed via the standard Windows function.
If you change the password via Windows or Active Directory, you will need to enter the new password the next time you log in using PIT Windows Logon. That is the only way to log in.

6.5 Generate and manage PIT Windows Logon Key

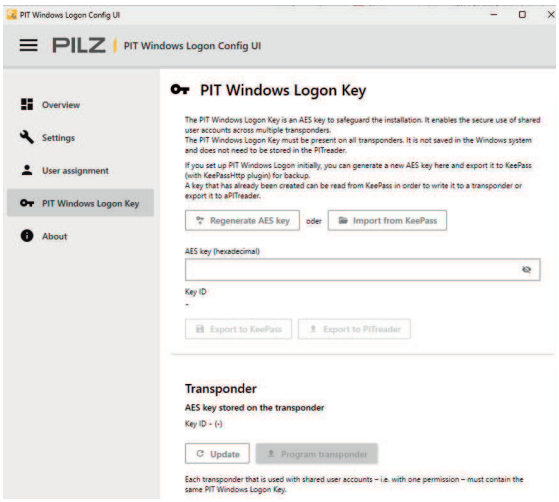
Prerequisites

- PIT Windows Logon Config UI is started, see Start PIT Windows Logon Config UI [20].
- You have carried out the basic configuration, Create basic configuration [23].
- You are logged into the PC as administrator.

Procedure

1. Click on ***PIT Windows Logon Key***.

   The ***PIT Windows Logon Key*** menu is displayed:

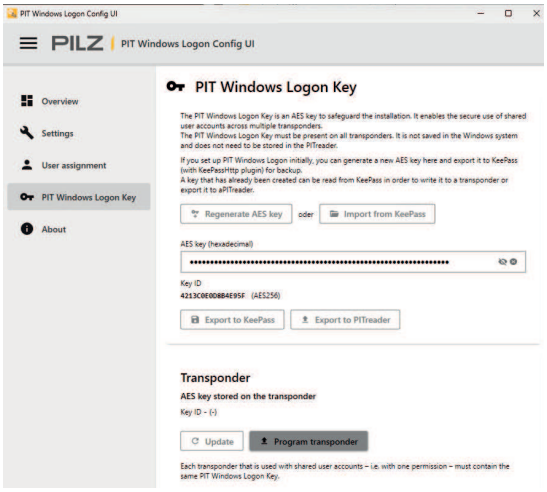


2. Select

   Regenerate AES key – the AES key is generated and is displayed in the field ***AES key (hexadecimal)***.

   or

   Import from KeePass - the AES key saved in KeePass is imported and is displayed in the field ***AES key (hexadecimal)***:



3. Select

   Export to KeePass if you wish to save the AES key in KeePass.

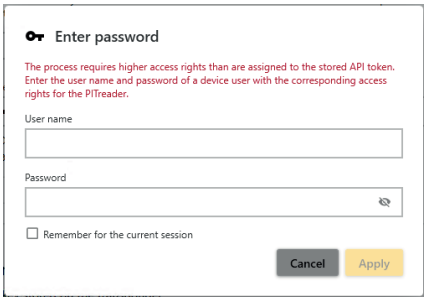
and/or

Export to PITreader if you wish to save the AES key in the PITreader, see Export PIT Windows Logon Key from PIT Windows Logon [📖 46].

In order to use the transponder, the PIT Windows Logon Key must be stored on the transponder:

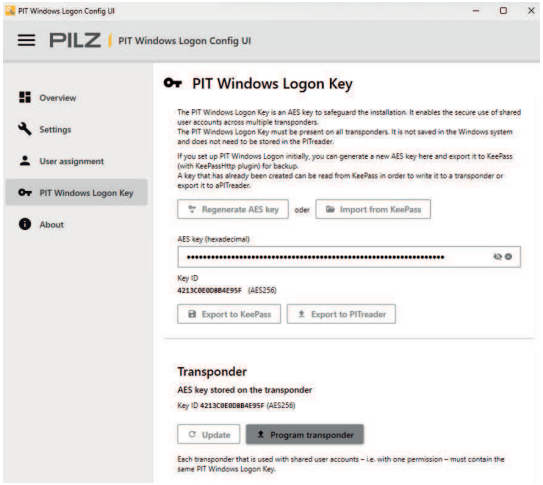
1. Position a transponder on the PITreader, see PITreader operating manual (1004806).
2. Click on ***Program transponder***.

   The ***Enter password*** window is displayed:



3. Enter your user name and password for the PITreader.
4. Click on ***Apply***.

   The PIT Windows Logon Key is written to the transponder and displayed:



5. If you wish to display the transponder's current AES key, click on ***Update***.

6.6 Perform user assignment

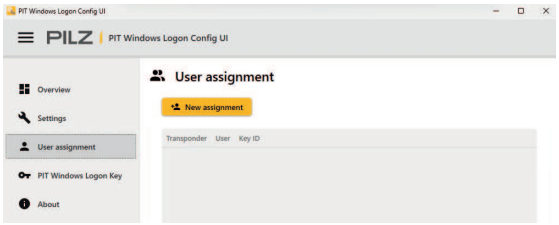
Prerequisites

- You are logged into the PC as administrator.
- PIT Windows Logon Config UI is started, see Start PIT Windows Logon Config UI [📖 20].
- You have carried out the basic configuration, see Create basic configuration [📖 23].
- A PITreader is connected to the PC.
- A transponder with PIT Windows Logon Key is in the reading range of the PITreader.

Procedure

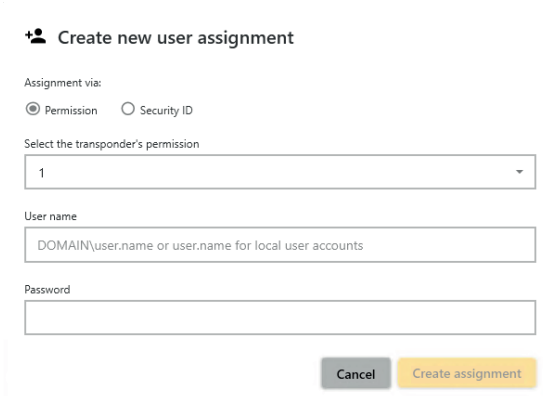
1. Click on ***User assignment***.

   The ***User assignment*** menu is displayed:



2. Click on ***New assignment***.

   The ***Create new user assignment*** menu is displayed:



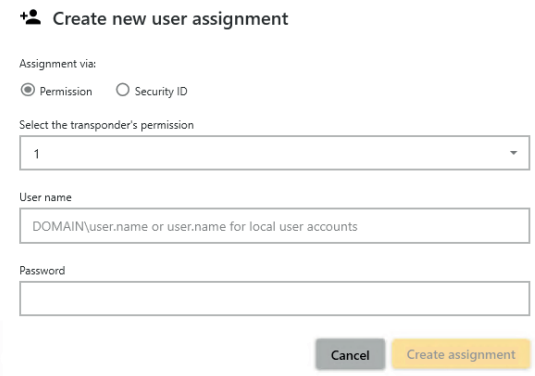
3. Select ***Assignment via:***

   Permission, if it is to be possible to log in to this user account via several transponders (shared user accounts), see Permission [📖 32].

   or

   Security ID, if it is to be possible to log in to this user account via one transponder only (personal user accounts), see Security ID [📖 33].

6.6.1 Permission



1. In the ***Select the transponder's permission*** drop-down menu, select the minimum permission that a transponder must have in order to log in to this user account.
2. Enter the user name of the Windows account under ***User name***.

For domain accounts in a corporate network, the domain must be specified along with the user name, e.g. COMPANY\user.name or as a "user principal name" (UPN), e.g. user.name@company.com.

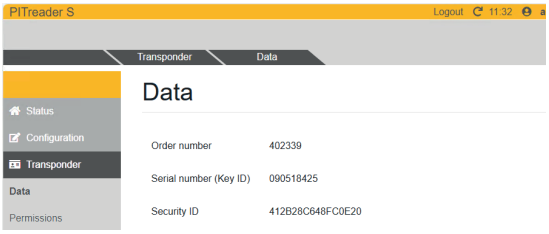
3. Enter the password of the Windows user account under ***Password***.
4. Click on ***Create assignment***.

6.6.2 Security ID

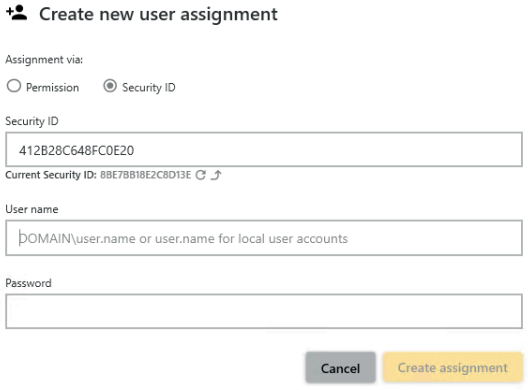
If the ***Enable self-registration for users*** function is activated, users without admin permission can also use the login screen to register their transponder independently to log in with their personal Windows user account, see Self-register transponder [📖 37].

1. Open the PITreader web application, see PITreader operating manual (1004806).
2. In the web application, select ***Transponder***.

   The ***Data*** window is displayed:



3. Copy the transponder's Security ID.
4. Switch to PIT Windows Logon Config UI.
5. Paste the transponder's Security ID into the ***Security ID*** field.



This Security ID will then be used during login.

6. Enter the user name of the Windows account under ***User name***.

   For domain accounts in a corporate network, the domain must be specified along with the user name, e.g. COMPANY\user.name or as a "user principal name" (UPN), e.g. user.name@company.com.

7. Enter the password of the Windows user account under ***Password***.
8. Click on ***Create assignment***.

7 Install updates

Updates can be installed via an existing version. All settings, user assignments and access data are copied over from the previous version.

If the login screen is open with the PIT Windows Logon Credential Provider loaded, the PC must be restarted after the update. This applies, for example, if an update is installed via a remote connection or automatically in the background.

8 Operation

8.1 Position transponder on the PITreader

You can find out how to position the different transponders on the PITreader in the PITreader operating manual (1004806).

8.2 Log in on the Windows PC

8.2.1 Login via the Windows login screen

Prerequisites

- PIT Windows Logon is configured, see Configure PIT Windows Logon [📖 20].
- The PC is switched on.
- A transponder is positioned on the PITreader.

Procedure

1. On the Windows login screen, click on ***Login***.

   The login data is checked.

   If the login data is correct, the login is carried out and the Windows desktop is displayed.

8.2.2 Automatic logon

Prerequisites

- PIT Windows Logon is configured, see Configure PIT Windows Logon [📖 20].
- The ***Automatic logon*** checkbox is activated in the configuration under ***Function settings***, see Configure function settings [📖 27].
- The PC is switched on.

Procedure

1. Position transponder on the PITreader.

   The login data is checked.

   If the login data is correct, the login is carried out and the Windows desktop is displayed.

8.3 Log out of the Windows PC

8.3.1 Logging out via the Windows desktop

- The PC is switched on.
- You are logged in to the PC.

Procedure

1. Log out of Windows, as you would on a PC without PITreader.

   The Windows login screen is displayed.

8.3.2 Automatic logout

Prerequisites

- PIT Windows Logon is configured, see Configure PIT Windows Logon [📖 20].
- The ***Automatic lock*** checkbox is activated in the configuration under ***Function settings***, see Configure function settings [📖 27].
- The PC is switched on.
- You are logged in to the PC.

Procedure

1. Remove the transponder from the PITreader.

   The Windows login screen is displayed.

INFORMATION

The ***Automatic lock*** function is only available once you have logged back in to the PC.

8.4 Self-register transponder

Prerequisites

- PIT Windows Logon is configured, see Create basic configuration [📖 23].
- The ***Enable self-registration for users*** checkbox is activated in the configuration under ***Function settings***, see Configure function settings [📖 27].
- The PC is switched on.
- A transponder is positioned on the PITreader.

Procedure

1. On the Windows login screen, click on ***Register transponder....***

   The input fields for the user name and password are displayed.
2. Enter your user name and password.
3. Confirm the entry.

   The transponder is registered. You will be able to use this transponder to log in to this Windows PC in future.

8.5 Update Windows passwords

Prerequisites

- PIT Windows Logon is configured, see Configure PIT Windows Logon [📖 20].
- The ***Changing the password*** checkbox is activated in the configuration under ***Function settings***, see Configure function settings [📖 27].
  PIT Windows Logon is then integrated by default into the Windows interface for changing passwords.
- The PC is switched on.

▶ You are logged in to the PC.

Procedure

1. On the PC, press Ctrl + Alt + Delete to change the password.

   The fields displayed depend on the setting in PIT Windows Logon Config UI, see Changing the password [📖 28].

9 Install CodeMeter Runtime

To operate PIT Windows Logon, you need a licence installed on the PC via CodeMeter (WIBU Systems AG).

INFORMATION

Install CodeMeter Runtime before you install PIT Windows Logon. This will save you having to restart the PIT Windows Logon Service after installation.

If a restart is required, you can use the function in the PIT Windows Logon Config UI interface.

Prerequisites

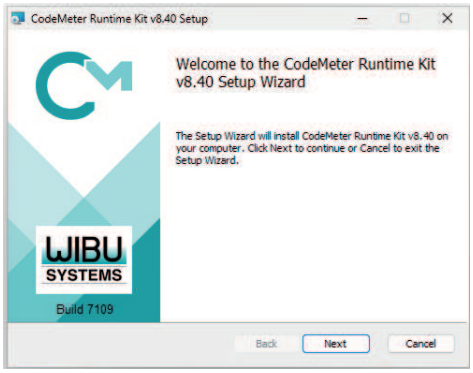
- The PC is switched on.
- You have administrator rights on the Windows PC.

Installation

The CodeMeter Runtime software can be found in the PIT Windows Logon download package.

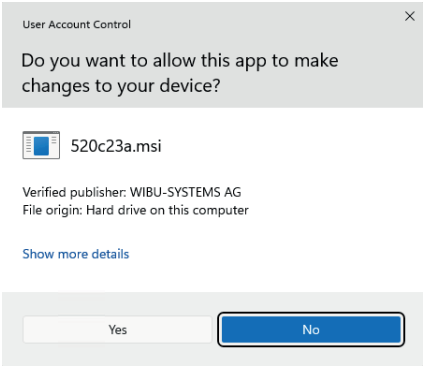
1. Download "PITWindowsLogon_<Version>.zip", see Install PIT Windows Logon [18].
2. Unpack the zip file.
3. Double-click on the installation file "CodeMeterRuntime64.msi".

   The setup window is displayed:



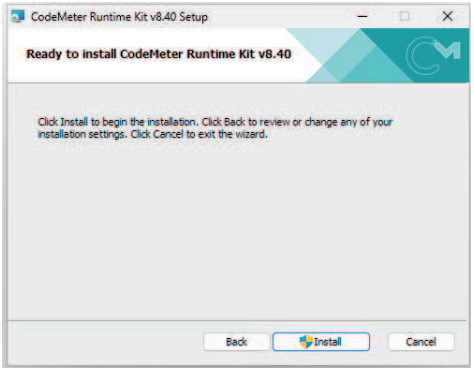
4. Click ***Next*** to start the installation wizard.
5. Follow the instructions in the setup:
   Accept the licence conditions.
   Select the standard installation (recommended).
6. Click on ***Install***.

   If the User account control menu appears:



Click ***Yes*** first.

CodeMeter is installed. The following window then appears:



7. Click ***Finish*** to complete the installation.

   An icon with the name "CodeMeter Control Center" is added to the Windows start menu

The CodeMeter icon also appears  in the Windows status bar.

10 Save the PIT Windows Logon Key in KeePass

To save the PIT Windows Logon Key via KeePass 2:

- The KeePassHttp plugin must be installed
- A KeePass database must be created.

10.1 Install KeePassHttp plugin

Prerequisites

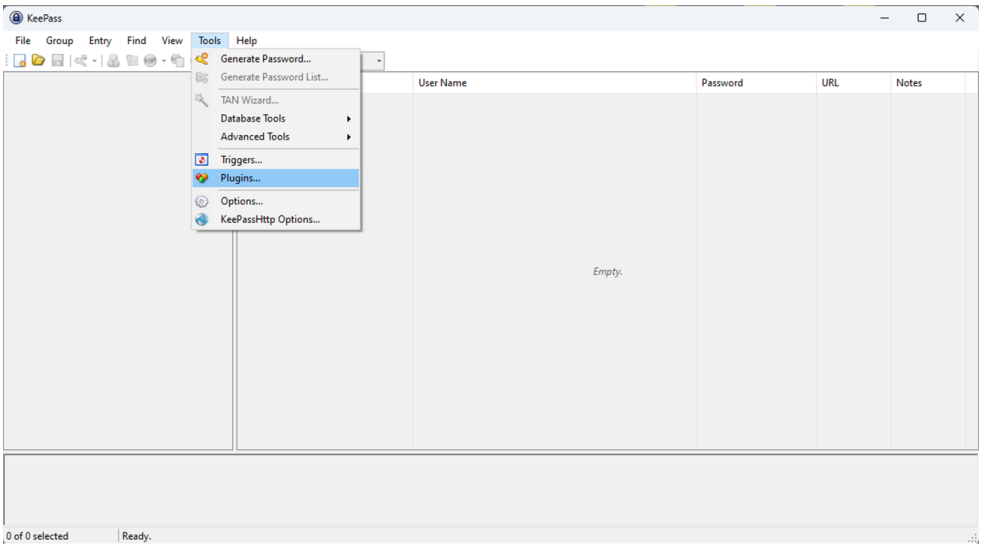
- KeePass 2 is installed.

  You can find the download link for KeePass 2 at:
  https://keepass.info/download.html
- The PC is switched on.
- You have administrator rights on the Windows PC.

Procedure

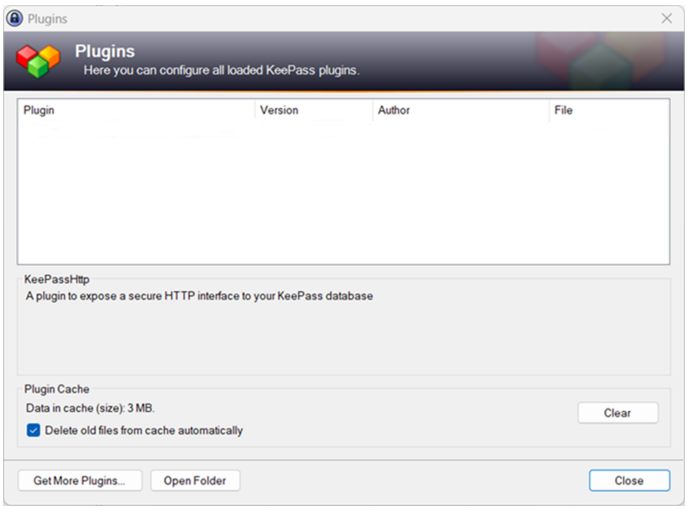
1. Download the KeePassHttp plugin via the following link:
   https://raw.github.com/pfn/keepasshttp/master/KeePassHttp.plgx
2. Start the KeePass 2 program.

   The menu window is displayed.

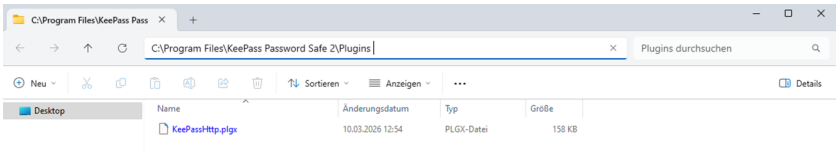


3. Select ***Tools*** -> ***Plugins*** from the menu bar.

   The "Plugins" menu is displayed.



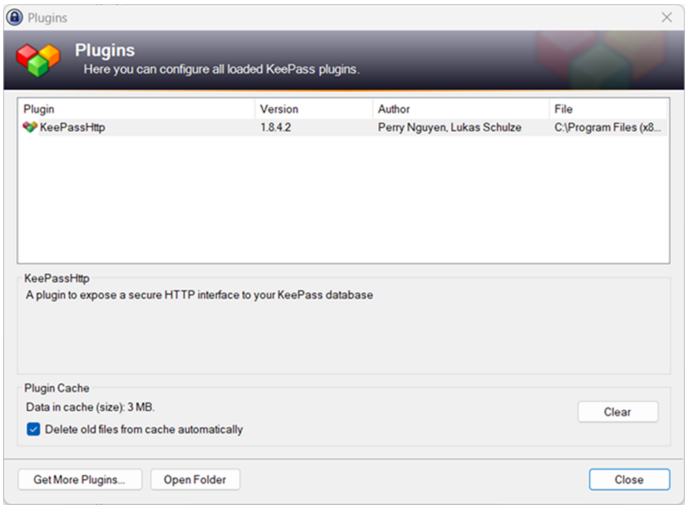
4. Click on ***Open Folder.***
5. Open the folder containing the downloaded file "KeePassHttp.plgx".
6. Copy the file "KeePassHttp.plgx" to the "Plugins" menu and add it to the installation folder (C:\Program Files\KeePass Password Safe 2\Plugins) for the KeePass plugins.



7. Click on ***Close***.

   The "Plugins" menu is closed.
8. Exit KeePass 2 and then restart KeePass 2.

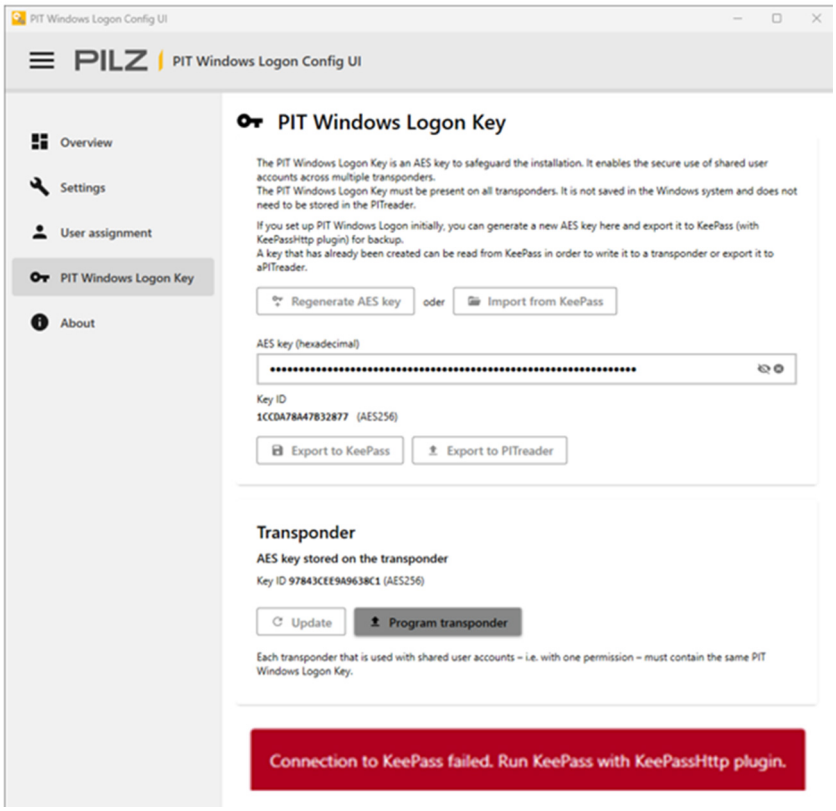
   After the restart, the KeePassHttp plugin is installed. The KeePassHttp plugin "KeePassHttp" is displayed in the "Plugins" menu.



10.2 Create database in KeePass 2

A KeePass database must be created so that the PIT Windows Logon Key can be exported.

If there is no KeePass database available, the following error message is displayed in a red box – even if the KeePassHttp plugin is installed:
Connection to KeePass failed. Run KeePass with KeePassHTTP plugin



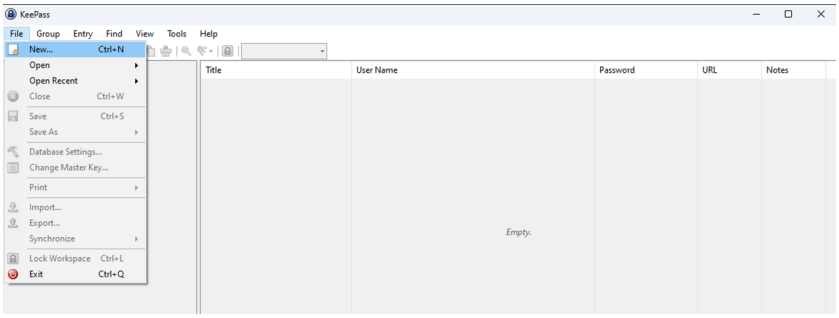
Prerequisites

- KeePass 2 and KeePassHttp plugin are installed, see Install KeePassHttp plugin [41].
- The PC is switched on.
- You have administrator rights on the Windows PC.

Procedure

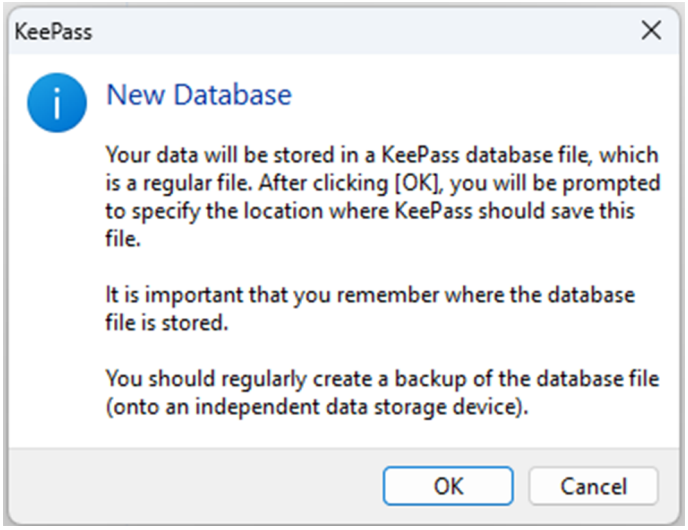
1. Start the "KeePass 2" program.

   The program is displayed.



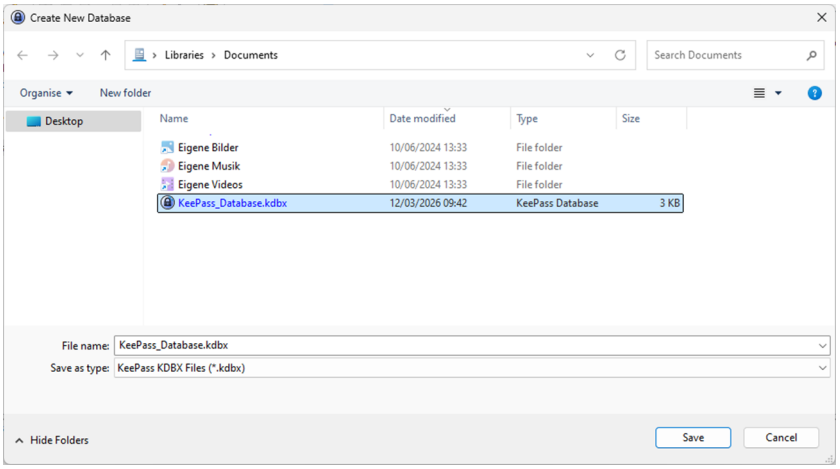
2. Select ***File*** in the menu bar and then ***New.***

   The "KeePass" window is displayed, showing information on the database.



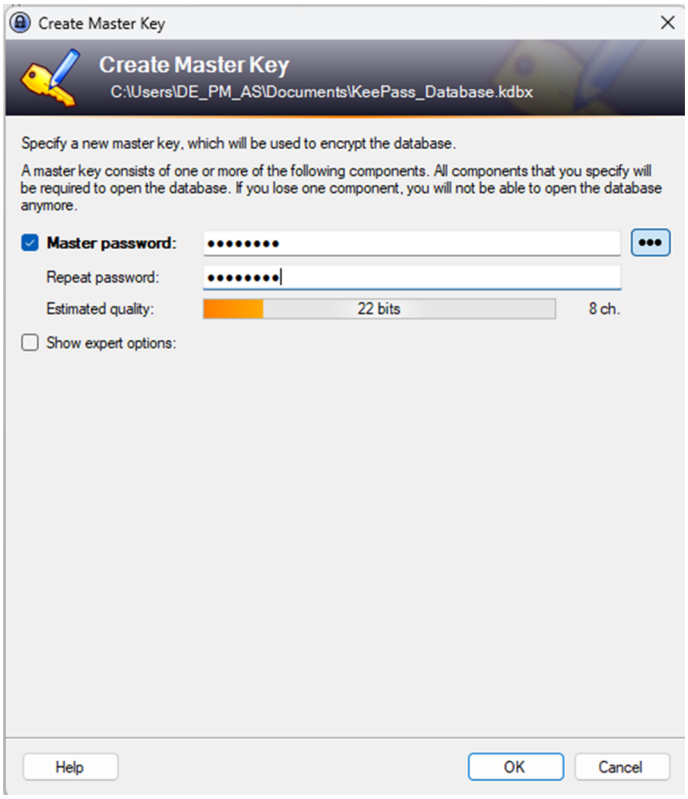
3. Click ***OK***.

   The "Create New Database" window appears.



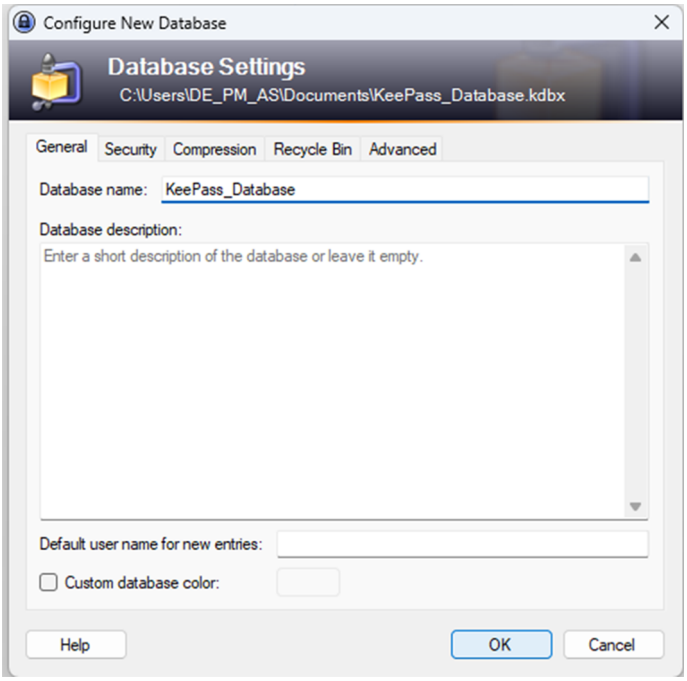
4. Select a suitable storage location and assign a unique name for the database, e.g. "KeePass_Database".
5. Click ***Save***.

   The "Create Master Key" window appears.



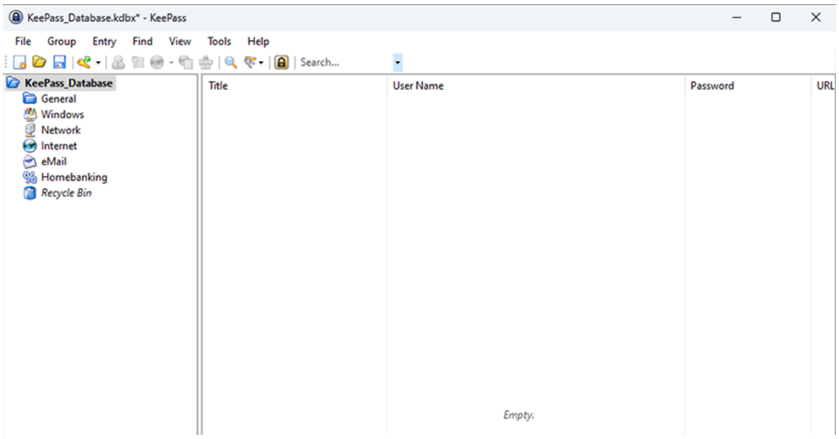
6. Create the main password for the database.
7. Click ***OK***.

   The "Configure New Database" menu appears.



8. If necessary, configure the database.
9. Click ***OK***.

The newly created, empty KeePass database is displayed, e.g. "KeePass_Database.kdbx* - KeePass".



10.3 Export PIT Windows Logon Key from PIT Windows Logon

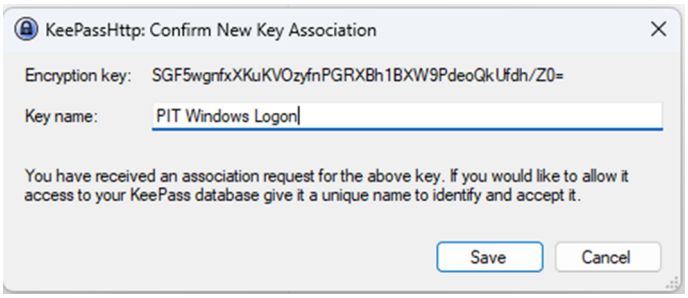
Prerequisites

- KeePass 2 with KeePassHttp plugin is installed, Install KeePassHttp plugin [41].
- A KeePass database is created, Create database in KeePass 2 [42].
- You have administrator rights on the Windows PC.
- KeePass 2 has been started.

Procedure

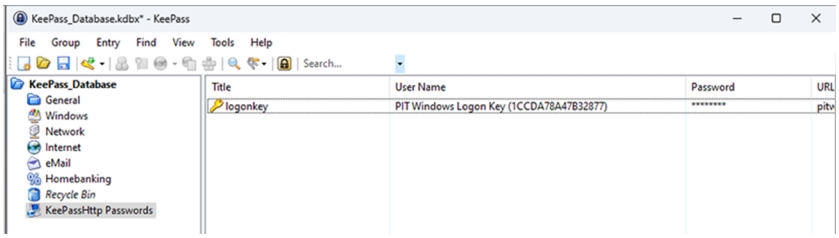
1. Export the PIT Windows Logon Key from PIT Windows Logon, Generate and manage PIT Windows Logon Key [30].

   When you export the PIT Windows Logon Key for the first time, the window "KeePassHttp. Confirm New Key Association" appears.



2. Enter a suitable name for the connection between KeePass 2 and PIT Windows Logon Config UI.
3. Click ***Save***.

   The PIT Windows Logon Key is created and stored in the KeePass database.



11 Licensing

The software PIT Windows Logon is available to download from the Pilz website. You can install and set up the software even if no licence is activated.

However, you need an activated licence to log in to a Windows PC with a transponder.

The licences are managed in licence containers. They are managed using CodeMeter software from WIBU SYSTEMS. CodeMeter is included in the PIT Windows Logon download package and must be installed separately. After installation, the CodeMeter Icon appears

 in the Windows status bar.

11.1 Purchase a licence

You need a separate licence for each installation of PIT Windows Logon. This applies to every Windows system on which you wish to log in. You can purchase licences in the Pilz eShop or via other sales channels.

Once purchased, you will receive a product certificate with a licence ticket.
To enable the software to recognise the licence, you must use CodeMeter to import the licence ticket into the licence container.

11.2 Activate licence

The licence must be available on the PC on which PIT Windows Logon is used. To do this, the licence must be activated on this PC. Once activated, the licence is bound to this PC. If necessary, you can transfer the licence to another PC later.

To activate the licence, proceed in the usual way with Pilz products.

12 Uninstall PIT Windows Logon

When PIT Windows Logon is uninstalled, all settings, user assignments and saved access data are deleted from the Windows PC.

Prerequisites

- You have administrator rights on the Windows PC.

Procedure

- To uninstall PIT Windows Logon, use the usual uninstall functions in Windows.

13 Order reference

Product type	Features	Product ID
PIT Windows Logon Licence 1	PIT Windows Logon licence for 1 activation	402356

Support

Technical support is available from Pilz round the clock.

Americas
Brazil
+55 11 97569-2804
Canada
+1 888 315 7459
Mexico
+52 55 5572 1300
USA (toll-free)
+1 877-PILZUSA (745-9872)

Asia
China
+86 400-088-3566
Japan
+81 45 471-2281
South Korea
+82 31 778 3390

Australia and Oceania
Australia
+61 3 95600621
New Zealand
+64 9 6345350

Europe
Austria
+43 1 7986263-444
Belgium, Luxembourg
+32 9 3217570
France
+33 3 88104003
Germany
+49 711 3409-444
Ireland
+353 21 4804983
Italy, Malta
+39 0362 1826711
Scandinavia
+45 74436332
Spain
+34 938497433
Switzerland
+41 62 88979-32
The Netherlands
+31 347 320477
Türkiye
+90 216 5775552
United Kingdom
+44 1536 460866

You can reach our international hotline on:
+49 711 3409-222
support@pilz.com

Reporting security vulnerabilities or security incidents
If you would like to report a security vulnerability or a security incident in connection with a Pilz product, please contact our **Pilz Product Security Incident Response Team (PSIRT).**
You can reach us at: www.pilz.com/psirt

Pilz develops environmentally-friendly products using ecological materials and energy-saving technologies. Offices and production facilities are ecologically designed, environmentally-aware and energy-saving. So Pilz offers sustainability, plus the security of using energy-efficient products and environmentally-friendly solutions.

www.pilz.com/facebook
www.pilz.com/xing
www.pilz.com/linkedin
www.pilz.com/youtube

1007324-EN-03, 2026-05 Printed in Germany

We are represented internationally. Please refer to our homepage www.pilz.com for further details or contact our headquarters.

Headquarters: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Germany
Telephone: +49 711 3409-0, E-Mail: info@pilz.com, Internet: www.pilz.com

PILZ
THE SPIRIT OF SAFETY