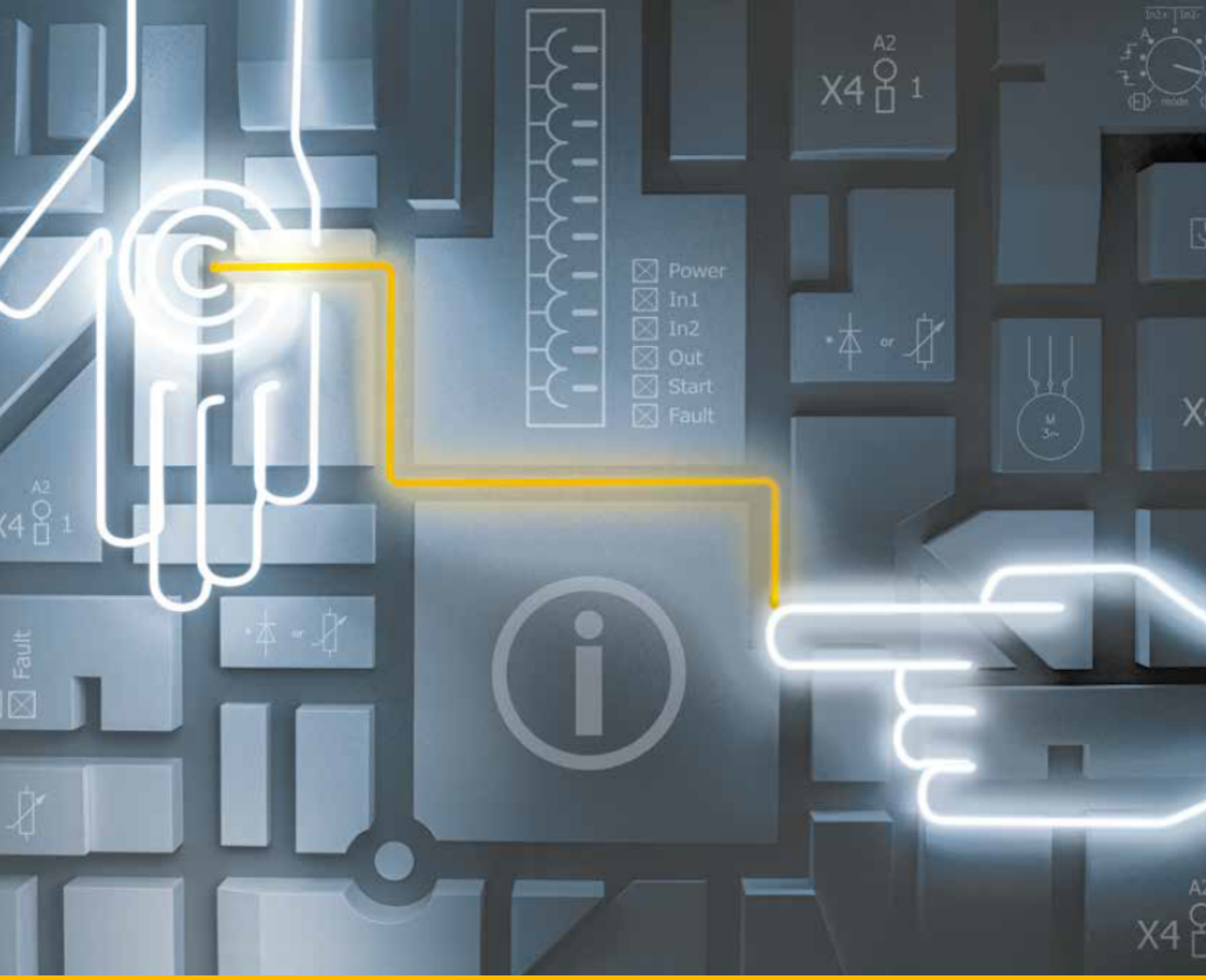


PIT Windows Logon

PILZ
THE SPIRIT OF SAFETY

Bedienungsanleitung-1007324-DE-03
- Anwendersoftware




Dieses Dokument ist das Originaldokument.

Wo unvermeidbar, wurde aus Gründen der besseren Lesbarkeit die männliche Sprachform bei der Formulierung dieses Dokuments gewählt. Es wird versichert, dass alle Personen diskriminierungsfrei und gleichberechtigt betrachtet werden.

1 Einführung

1.1 Gültigkeit der Dokumentation

Diese Bedienungsanleitung ist gültig für die Software PIT Windows Logon ab der Version 1.0.0.

1.2 Nutzung der Dokumentation

Dieses Dokument dient der Instruktion. Installieren und nehmen Sie das Produkt nur dann in Betrieb, wenn Sie dieses Dokument gelesen und verstanden haben. Bewahren Sie das Dokument für die künftige Verwendung auf.

1.3 Verwendete Begriffe

PITreader

Unter der Bezeichnung "PITreader" sind alle RFID-Authentifizierungssysteme der PILZ GmbH & Co. KG zusammengefasst, bei denen die Authentifizierung über einen Transponder erfolgt.

Als Transponder können z. B. verwendet werden:

- PITreader Transponder-Schlüssel
- PITreader Transponder-Karten
- PITreader Transponder-Sticker

Die Bezeichnung "PITreader" wird immer dann verwendet, wenn die Beschreibung für alle Produktvarianten gültig ist.

PITreader Key

Unter der Bezeichnung "PITreader Key" sind alle Produktvarianten des PITreaders zusammengefasst, bei denen ausschließlich ein PITreader Transponder-Schlüssel zur Authentifizierung verwendet werden kann. Dazu wird der PITreader Transponder-Schlüssel in den Lesekopf eingesteckt.

Eine Produktvariante ist z. B. PITreader S base unit.

Die Bezeichnung "PITreader Key" wird immer dann verwendet, wenn die Beschreibung ausschließlich für diese Produktvarianten gültig ist.

PITreader Card

Unter der Bezeichnung "PITreader Card" sind alle Produktvarianten des PITreaders zusammengefasst, bei denen folgende Transponder zur Authentifizierung verwendet werden können:

- PITreader Transponder-Karte
- PITreader Transponder-Sticker
- PITreader Transponder-Schlüssel

Dazu wird der PITreader Transponder vor den Lesekopf gehalten.

Eine Produktvariante ist z. B. PITreader S card unit.

Die Bezeichnung "PITreader Card" wird immer dann verwendet, wenn die Beschreibung ausschließlich für diese Produktvarianten gültig ist.

1.4 Zeichenerklärung

Besonders wichtige Informationen sind wie folgt gekennzeichnet:

GEFAHR!

Beachten Sie diesen Hinweis unbedingt! Er warnt Sie vor unmittelbar drohenden Gefahren, die schwerste Körperverletzungen und Tod verursachen können, und weist auf entsprechende Vorsichtsmaßnahmen hin.

WARNUNG!

Beachten Sie diesen Hinweis unbedingt! Er warnt Sie vor gefährlichen Situationen, die schwerste Körperverletzungen und Tod verursachen können, und weist auf entsprechende Vorsichtsmaßnahmen hin.

ACHTUNG!

weist auf eine Gefahrenquelle hin, die leichte oder geringfügige Verletzungen sowie Sachschaden zur Folge haben kann, und informiert über entsprechende Vorsichtsmaßnahmen.

WICHTIG

beschreibt Situationen, durch die das Produkt oder Geräte in dessen Umgebung beschädigt werden können, und gibt entsprechende Vorsichtsmaßnahmen an. Der Hinweis kennzeichnet außerdem besonders wichtige Textstellen.

INFO

liefert Anwendungstipps und informiert über Besonderheiten.

2 Sicherheit und Security

2.1 Bestimmungsgemäße Verwendung

2.1.1 Produkt

Die Software PIT Windows Logon dient zur Authentifizierung, Autorisierung und Protokollierung von Benutzeranmeldungen an Windows-PCs. Sie ist ausschließlich als Erweiterung des PITreaders vorgesehen. Die Authentifizierung erfolgt über RFID-Transponder.

2.1.2 Anwendungsbereiche

PIT Windows Logon wird in industriellen und gewerblichen Umgebungen eingesetzt, in denen ein sicherer Zugriff auf Windows-PCs erforderlich ist.

2.1.3 Einsatzbedingungen

Verwendung nur in Verbindung mit den vorgesehenen Hardware- und Softwarekomponenten.

Einhaltung der Einsatzbedingungen für PITreader und kompatible RFID-Transponder.

2.1.4 Qualifikation des Personals

Installation, Programmierung, Konfiguration, Inbetriebnahme, Betrieb, Außerbetriebnahme und Wartung der Software dürfen ausschließlich von hierfür qualifizierten Personen durchgeführt werden.

Eine qualifizierte Person verfügt über Fachkenntnisse in den Bereichen:

- IT-Sicherheit und Netzwerksicherheit, einschließlich aktueller Bedrohungen und Schutzmaßnahmen
- Anwendung relevanter Sicherheitsstandards und -richtlinien
- Kenntnisse der geltenden nationalen und europäischen Vorschriften zu Security und Datenschutz

Wir empfehlen dem Betreiber nur Personen einzusetzen, die

- mit den grundlegenden Vorschriften zur Informationssicherheit und zum Schutz vor Cyberangriffen vertraut sind,
- den Abschnitt "Sicherheit und Security" in dieser Beschreibung gelesen und verstanden haben,
- die für die spezifische Anwendung geltenden Sicherheitsrichtlinien und Normen kennen und anwenden können.

2.1.5 Voraussetzungen für den Betrieb

- funktionsfähige PITreader-Hardware
- kompatible RFID-Transponder
- Windows-PC mit unterstütztem Betriebssystem
- aktuelle Sicherheitsupdates und Virenschutz auf dem PC

Dieses Dokument dient der Instruktion. Installieren und nehmen Sie das Produkt nur dann in Betrieb, wenn Sie dieses Dokument gelesen und verstanden haben.

2.1.6 Besondere Maßnahmen zur bestimmungsgemäßen Verwendung

Es sind keine besonderen Maßnahmen für die bestimmungsgemäße Verwendung erforderlich.

2.1.7 Nicht bestimmungsgemäße Verwendung

Als nicht bestimmungsgemäß gilt insbesondere:

- jegliche Veränderung des Produkts
- ein Einsatz des Produkts außerhalb der Bereiche, die in diesem Dokument beschrieben sind

2.1.8 Security-Umfeld

Die Installation muss auf einem nach dem Stand der Technik gehärteten Endgerät in einem gesicherten Netzwerk erfolgen.

2.1.9 Fremdhersteller-Lizenzinformationen

Im Produkt ist Open Source-Software enthalten, deren Nutzungsbedingungen den Einsatzbereich des Produkts zusätzlich einschränken können. Bitte beachten Sie unbedingt die Fremdhersteller-Lizenzinformationen.

Nähere Informationen erhalten Sie, indem Sie im Produkt PIT Windows Logon die Menüoption ***Über*** wählen und dann auf den Button ***Open Source-Lizenzen*** klicken.

2.2 Allgemeine Security-Hinweise

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu schützen, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht.
Führen Sie eine Risikobeurteilung gemäß VDI/VDE 2182 oder IEC 62443-3-2 durch und planen Sie die Security-Maßnahmen sorgfältig.

Wenn Sie Fragen zur Umsetzung haben, wenden Sie sich an den technischen Support support@pilz.com.

Unter https://www.pilz.com/psirt erreichen Sie das Pilz Product Security Incident Response Team (PSIRT).
Dort können Sie im Zusammenhang mit einem Pilz-Produkt:

- Security-Schwachstellen und Security-Vorfälle melden
- Fragen zu Security-Schwachstellen und Security-Vorfällen stellen
- Security Advisories einsehen

2.3 Security-Maßnahmen

2.3.1 Implementierte Security-Maßnahmen

PIT Windows Logon schützt Vertraulichkeit, Integrität und Authentizität aller Daten und Funktionen innerhalb des Systems durch die folgenden, implementierten Security-Maßnahmen:

- Windows-Zugangsdaten werden ausschließlich verschlüsselt und mit einem rotierenden, kryptographischen Schlüssel gespeichert.
- Geräteübergreifende Kommunikation erfolgt stets authentifiziert und verschlüsselt, um Datenintegrität und Vertraulichkeit sicherzustellen.
- Der PIT Windows Logon Key wird verschlüsselt auf den Transpondern abgelegt und kann nicht aus einem PITreader ausgelesen werden.
- Sensitive und vertrauliche Daten sowie Einstellungen von PIT Windows Logon sind auf einem Windows-PC ausschließlich mit einem Benutzerkonto mit Administratorrechten zugänglich.

2.3.2 Erforderliche externe Security-Maßnahmen

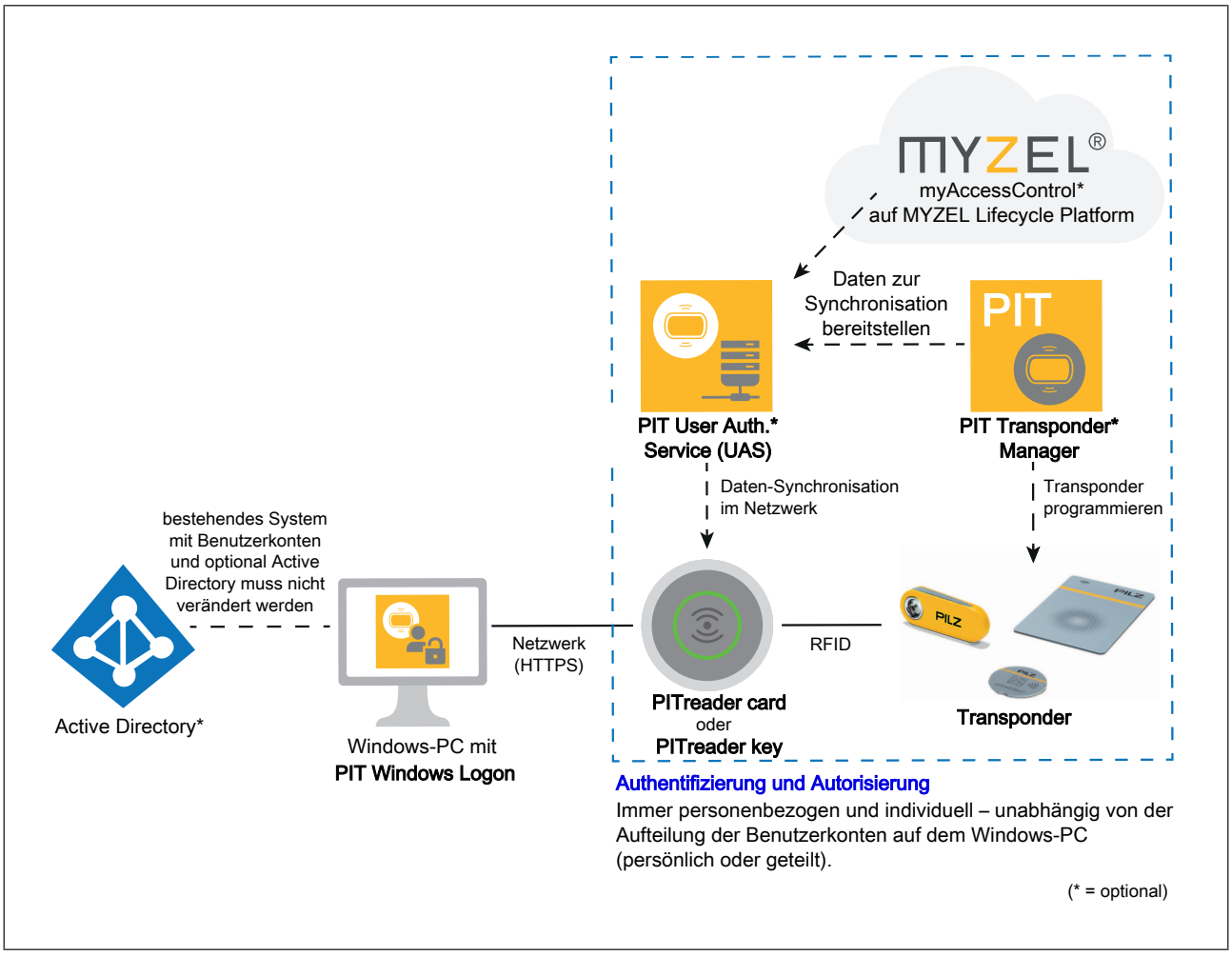
Für einen sicheren Betrieb von PIT Windows Logon sind Sie zur Umsetzung der folgenden weiteren Maßnahmen an den Systemgrenzen verantwortlich:

- Generieren Sie einen sicheren PIT Windows Logon Key, siehe PIT Windows Logon Key generieren und verwalten [📖 30].

- Bewahren Sie den PIT Windows Logon Key sicher auf, siehe PIT Windows Logon Key generieren und verwalten [📖 30].
- Verwenden Sie einen PITreader mit Basis-Codierung. Stellen Sie sicher, dass die Basis-Codierung ausschließlich den mit der Einrichtung betrauten Personen bekannt ist.
- Schränken Sie den administrativen Zugang auf dem Windows-PC ein, auf dem PIT Windows Logon verwendet wird. Gewähren Sie den Zugriff ausschließlich autorisierten Personen, die für die Verwaltung des Zugangs zu diesem PC verantwortlich und dazu ermächtigt sind.
- Regelmäßige Prüfung der Systemintegrität und der Protokolldaten.
- Durchführung von Software-Updates gemäß Herstellerempfehlung.

3 Übersicht

Mit der Software PIT Windows Logon können Sie PITreader und Transponder nutzen, um sich passwortlos an Windows-PCs anzumelden. Jede Person verwendet dafür einen individuell eingerichteten Transponder. Die Eingabe von Benutzername und Passwort entfällt. Die Authentifizierung und Autorisierung erfolgen immer personenbezogen über PITreader. Sie sind unabhängig von der Granularität der Benutzerkonten in Windows. Optional können Sie den PIT User Authentication Service, den PIT Transponder Manager oder myAccess-Control auf der MYZEL Lifecycle Platform verwenden.



Damit diese Funktion genutzt werden kann, muss die Konfiguration über die Software "PIT Windows Logon Config UI" vorgenommen werden, die auf einem PC mit Windows-Betriebssystem installiert wird.

3.1 Systemvoraussetzungen

Mindestanforderung:

- Betriebssystem Windows 10 (64-Bit), Version 1909 oder höher
- PITreader-Firmware-Version ab 02.03.01

3.2 Systembestandteile

PIT Windows Logon installiert einen eigenen Windows Credential Provider der sich in die Windows-Anmeldemaske integriert.

Die Kommunikation zwischen dem Credential Provider und Windows erfolgt über den Dienst PIT Windows Logon Service.

Die Konfiguration der Installation sowie die Zuordnung von Transpondern zu Windows-Benutzern wird über die Benutzeroberfläche PIT Windows Logon Config UI vorgenommen.

Eigenschaften des Dienstes PIT Windows Logon Service

- **Dienstname:** PITWindowsLogonService
- **Anzeigename:** PIT Windows Logon Service
- **Dienstkonto:** Lokales System
- **Starttyp:** Automatisch

Eigenschaften des PIT Windows Logon Credential Provider

- **Komponente:** PITWindowsLogonCredentialProvider.dll
  Eine Windows-Komponente zur Anzeige und Verarbeitung von Anmeldeinformationen beim Login.
- **Funktion:** Erweiterung der Windows-Anmeldemaske
  Diese Funktion ergänzt die Standardfunktion "Kennwort ändern".
- **CLSID:** 611814b0-cb75-4cdf-9bce-d459b38469aa

4 Funktionsbeschreibung

4.1 Einsatzszenarien von PIT Windows Logon

PIT Windows Logon unterstützt zwei grundlegende Einsatzszenarien:

- geteilte Benutzerkonten
- persönliche Benutzerkonten

Unabhängig vom Einsatzszenario erfolgt die Anmeldung stets personenbezogen. Jede Anmeldung wird individuell authentifiziert, autorisiert und protokolliert.

Nach erfolgreicher Autorisierung kann optional eine Zuordnung zu geteilten Windows-Benutzerkonten erfolgen.

Die Verwaltung der Berechtigungen basiert auf dem bewährten Prinzip mit:

- Unterstützung für Gerätegruppen
- Steuerung der Berechtigungen pro Station über die PITreader Gerätegruppen
- Möglichkeit zur zentralen Verwaltung über den PIT User Authentication Service (UAS)

Geteilte Benutzerkonten

Mehrere Personen greifen gemeinsam auf ein oder mehrere nicht personalisierte Windows-Benutzerkonten zu. Dies ist im Fertigungsumfeld häufig der Fall.

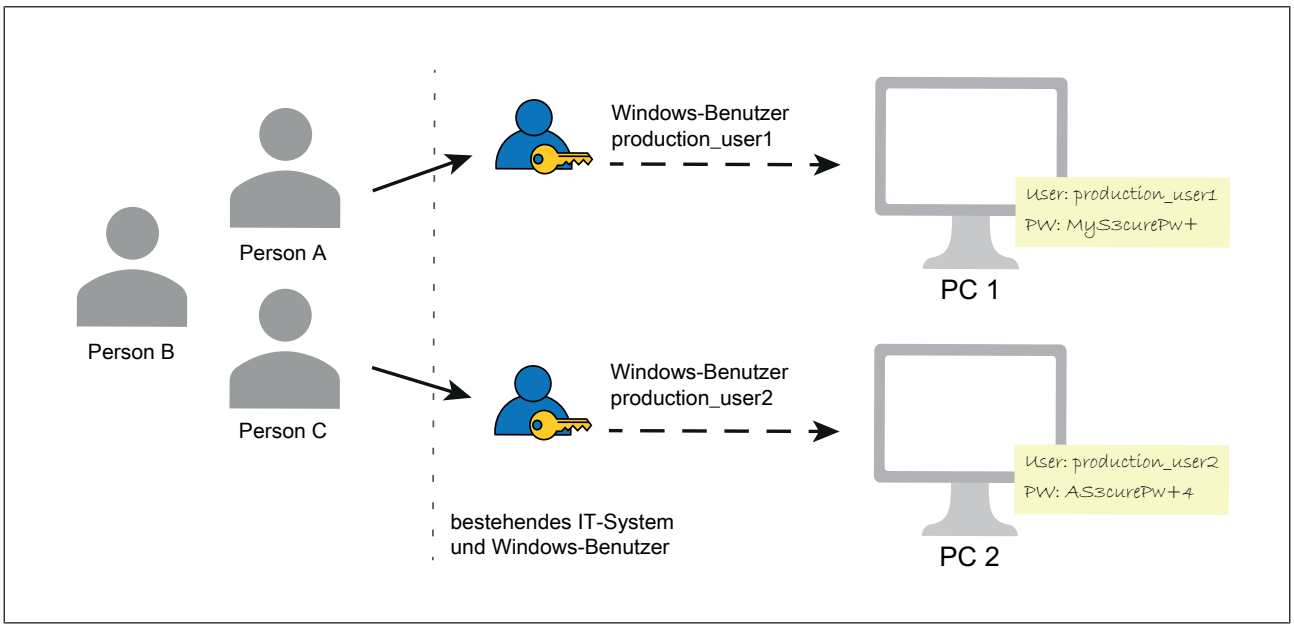


Abb.: Typische Installation ohne PIT Windows Logon

Über PITreader, Transponder und weitere Komponenten des Identification- und Access-Management-Systems von Pilz erfolgt die Authentifizierung und Autorisierung eindeutig und personenbezogen. Dies geschieht außerhalb des Windows-Systems. Bestehende Installationen in Fertigungsanlagen ohne persönliche Benutzerkonten müssen nicht geändert werden. Der Zugriff kann trotzdem personenindividuell gesteuert und kontrolliert werden.

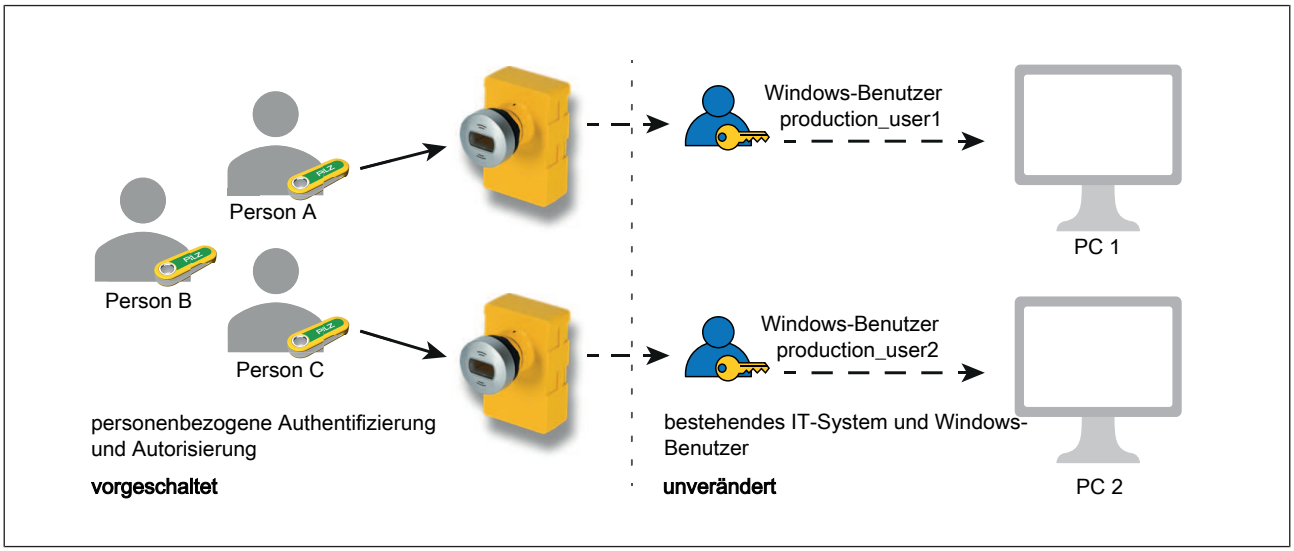
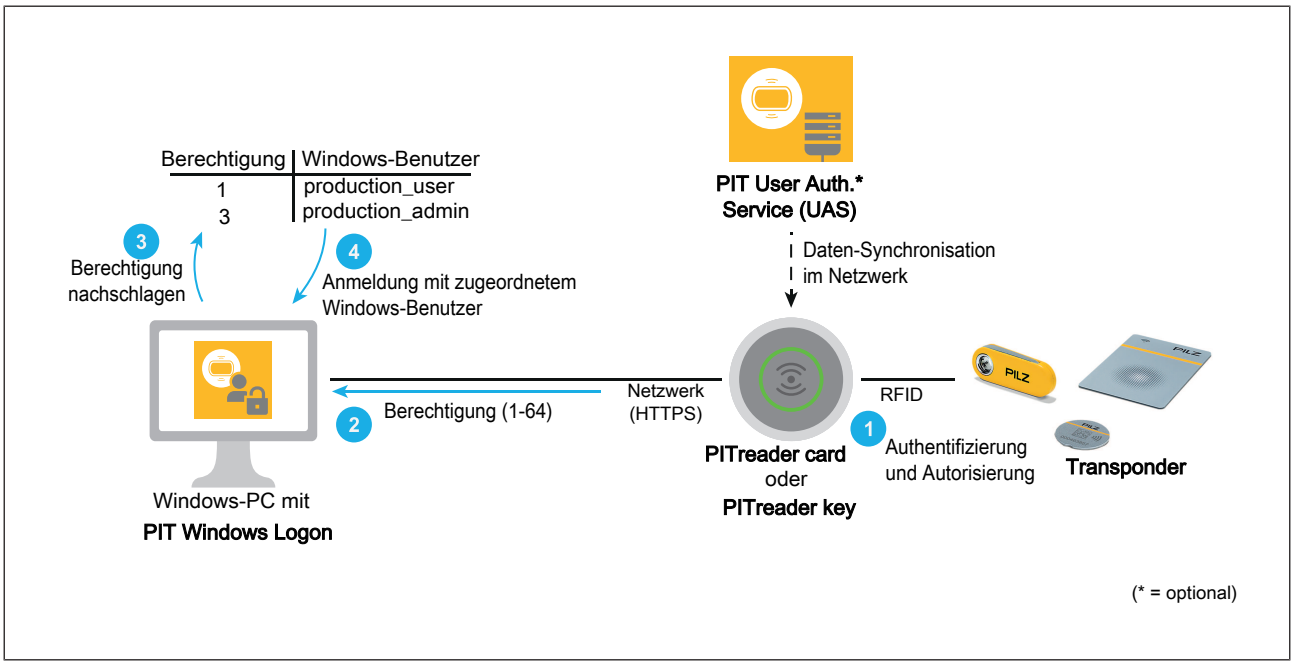


Abb.: Erweiterung der bestehenden Installation um PITreader und PIT Windows Logon

Neue oder nur zeitweise autorisierte Mitarbeiter können z. B. im PIT Transponder Manager angelegt werden. Dort lassen sich auch Berechtigungen von Mitarbeitern und Transpondern bearbeiten. Änderungen sind möglich, ohne die Konfiguration des Windows-PCs oder die Benutzerrechte im Active Directory anzupassen.

Die Zuordnung von Windows-Konten zu Transpondern erfolgt über die Berechtigung des Transponders (0 bis 64). Sie gilt pro PC und ist dadurch flexibel anpassbar und beliebig skalierbar.

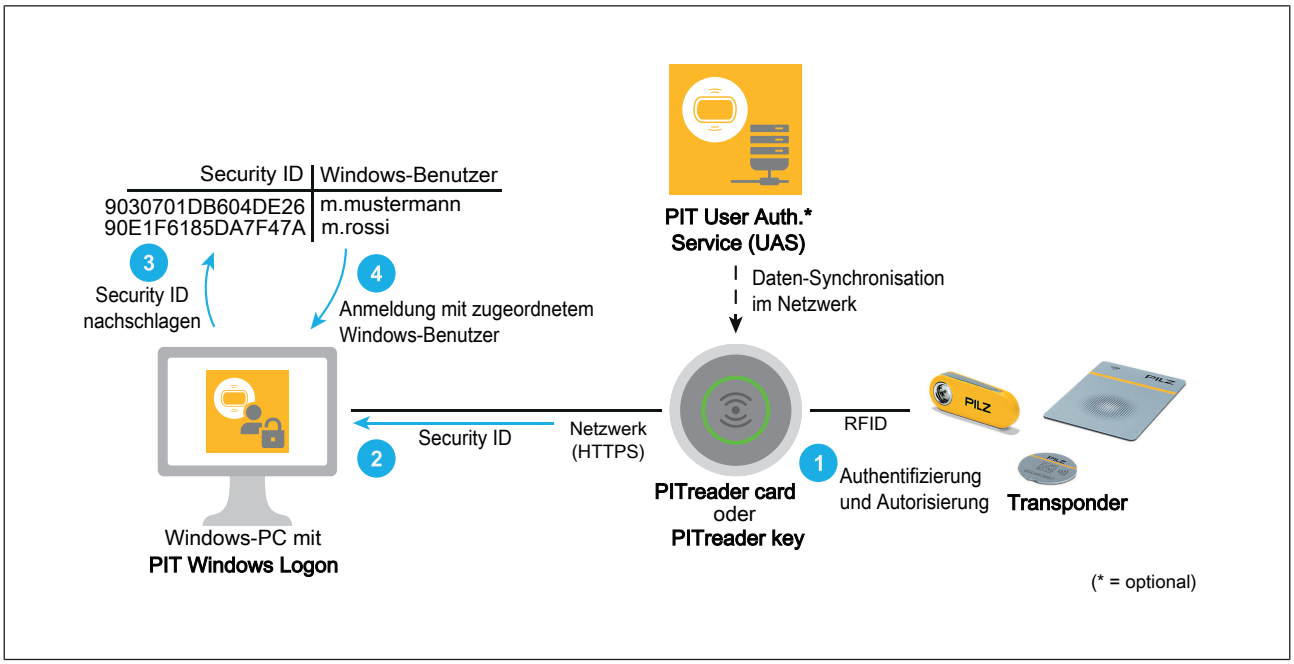


	Funktion:
[1]	Authentifizierung und Autorisierung erfolgen über den PITreader. Grundlage sind die Daten auf dem Transponder, die Berechtigungsliste oder vom PIT User Authentication Service (UAS) bereitgestellte Daten. Dabei wird die authentifizierte Berechtigung ermittelt.
[2]	PIT Windows Logon erhält die authentifizierte Berechtigung (0 bis 64) vom PITreader.

[3]	PIT Windows Logon ordnet die Berechtigung einem Windows-Benutzerkonto zu. Die Zuordnung wird mit der PIT Windows Logon Config UI erstellt und sicher auf dem PC gespeichert.
[4]	Anmeldung am PC erfolgt mit dem zugeordneten Windows-Benutzerkonto.

Persönliche Benutzerkonten

Für die Nutzung persönlicher Windows-Konten kann ein Konto eindeutig einem Transponder zugeordnet werden. Diese Zuordnung erfolgt über die Security-ID des Transponders. Die Security-ID ist eine eindeutige Kennung, die nicht manipuliert oder dupliziert werden kann. Dadurch wird das Benutzerkonto auf einen bestimmten Transponder beschränkt. Die Anmeldung erfolgt passwortlos und ausschließlich über diesen Transponder.



	Funktion:
[1]	Authentifizierung und Autorisierung erfolgen über den PITreader. Grundlage sind die Daten auf dem Transponder, die Berechtigungsliste oder vom PIT User Authentication Service (UAS) bereitgestellte Daten. Dabei wird die authentifizierte Berechtigung ermittelt.
[2]	PIT Windows Logon erhält die authentifizierte Security ID des Transponders vom PITreader.
[3]	PIT Windows Logon ordnet die Security ID einem Windows-Benutzerkonto zu. Die Zuordnung wird mit PIT Windows Logon Config UI erstellt und auf dem PC sicher gespeichert.
[4]	Anmeldung am PC erfolgt mit dem zugeordneten Windows-Benutzerkonto.

4.2 Optionale Funktionen

Automatische Anmeldung

Die Funktion ***Automatische Anmeldung*** kann in PIT Windows Logon aktiviert werden, siehe Funktionseinstellungen vornehmen [📖 27].

Ist die Funktion aktiviert, wird der Benutzer automatisch am Windows-System angemeldet. Die Anmeldung erfolgt, sobald ein Transponder mit einem zugeordneten Benutzerkonto erkannt wird.

Automatische Sperre

Die Funktion ***Automatische Sperre*** kann in PIT Windows Logon aktiviert werden, siehe Funktionseinstellungen vornehmen [📖 27].

Ist die Funktion aktiviert, wird der Bildschirm automatisch gesperrt. Die Sperrung erfolgt, sobald der Transponder aus dem Lesebereich des PITreader entfernt wird.

Selbstregistrierung

Die Funktion ***Selbstregistrierung für Benutzer aktivieren*** kann in PIT Windows Logon aktiviert werden, siehe Funktionseinstellungen vornehmen [📖 27].

Ist die Funktion aktiviert, kann ein Benutzer einen nicht zugeordneten Transponder registrieren. Die Registrierung erfolgt über die Windows-Anmeldemaske. Dazu gibt der Benutzer den Benutzernamen und das Kennwort seines Windows-Kontos ein. Die Zuordnung wird anhand der Security ID des Transponders im persönlichen Benutzerkonto gespeichert.

Kennwort ändern

Die Funktion ***Ändern des Kennworts*** kann in PIT Windows Logon aktiviert werden, siehe Funktionseinstellungen vornehmen [📖 27].

PIT Windows Logon integriert sich in die Windows-Maske zum Ändern des Kennworts. Bei Kennwortänderungen wird der verschlüsselte Datensatz der Zugangsdaten aktualisiert.

Wurde ein Kennwort außerhalb von PIT Windows Logon geändert, kann es über die PIT Windows Logon Config UI aktualisiert werden.

Alternativ kann bei der nächsten Anmeldung über einen Transponder das aktuelle Kennwort eingegeben werden.

4.3 Sicherheit durch den PIT Windows Logon Key

Die Sicherheit des PIT Windows Logon Systems basiert auf dem PIT Windows Logon Key – einem Sicherheitsschlüssel, den Sie selbst definieren können.

PIT Windows Logon Key

- Sie legen einen individuellen AES-256-Schlüssel fest.
- Dieser Schlüssel wird sicher auf den Transpondern gespeichert.
- Der Schlüssel verschlüsselt und entschlüsselt Ihre Windows-Zugangsdaten.

Schutzmechanismen

- Der gespeicherte Schlüssel kann nicht ausgelesen werden.
- Die Zugangsdaten sind zweifach abgesichert:
  - durch den Transponder mit dem PIT Windows Logon Key
  - durch den PITreader mit passender Codierung

Hohe Security durch kombinierte Zugriffsvoraussetzungen

Der Zugang zu Ihrem Windows-PC wird bei PIT Windows Logon durch die Kombination der folgenden drei Komponenten abgesichert:

- verschlüsselte Zugangsdaten
- PITreader mit passender Codierung
- Transponder mit kundenspezifischem Schlüssel

Weitere Sicherheitsmaßnahmen

- Die Zugangsdaten verbleiben im Windows-System und werden nicht über externe Schnittstellen übertragen.
- Die Zugangsdaten werden mit einem rotierenden Schlüssel abgesichert, der sich bei jeder Verwendung ändert.

5 PIT Windows Logon installieren

Voraussetzungen

- Der PC ist eingeschaltet.
- Sie verfügen über Administratorrechte auf dem Windows-PC.
- CodeMeter Runtime ist installiert, siehe CodeMeter Runtime installieren [39].
- Die PIT Windows Logon Lizenz ist in CodeMeter Runtime aktiviert, siehe Lizenzierung [48].

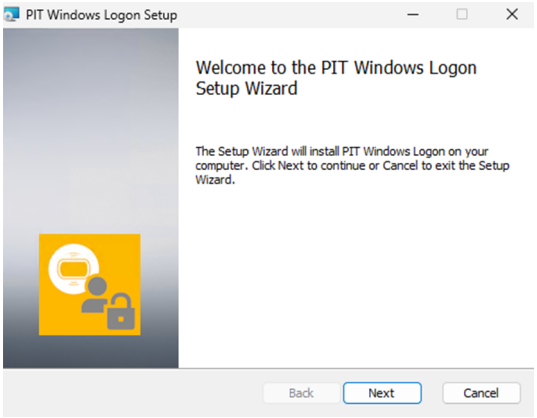
Zur Sicherung des PIT Windows Logon Key kann KeePass 2 mit KeePassHttp-Plugin verwendet werden.

Vorgehensweise

1. Öffnen Sie den Pilz E-Shop, https://www.pilz.com/eshop.
2. Melden Sie sich mit Ihren Zugangsdaten an.
3. Geben Sie im Suchfeld eine der folgenden Optionen ein:
   die Artikelnummer von PIT Windows Logon, siehe Bestelldaten [50]
   oder
   den Begriff "PIT Windows Logon"
4. Wählen Sie die Mappe "PITWindowsLogon_<Version>.zip".
5. Klicken Sie auf ***Download***.

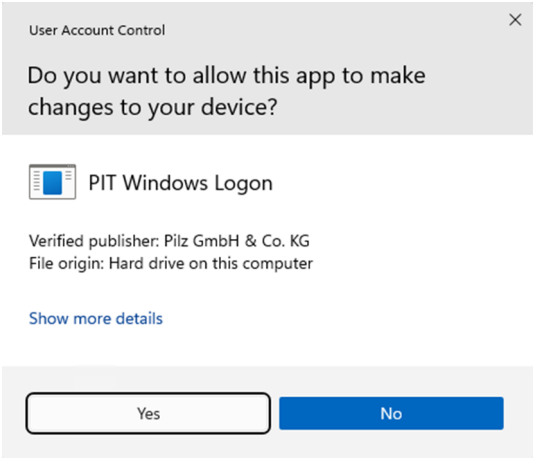
   Die Zip-Datei wird heruntergeladen.
6. Entpacken Sie die Zip-Datei.
7. Doppelklicken Sie auf die Installationsdatei "PITWindowsLogon_<Version>msi".

   Das Setup-Fenster wird angezeigt:



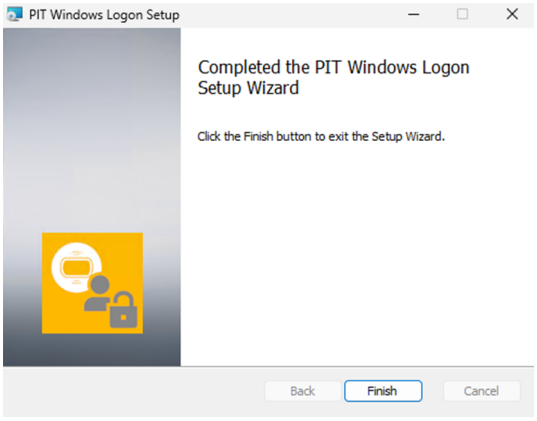
8. Klicken Sie auf ***Weiter*** um den Installationsassistenten zu starten.
9. Folgen Sie den Anweisungen im Setup:
   Akzeptieren Sie die Lizenzbedingungen.
   Passen Sie bei Bedarf den Installationspfad an.
10. Klicken Sie auf ***Installieren***.

    Falls das Menü ***Benutzerkontensteuerung*** erscheint:



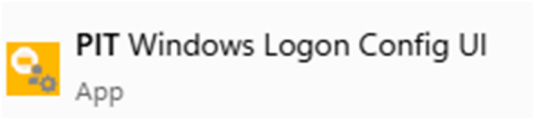
Klicken Sie zuerst auf ***Ja***.

PIT Windows Logon wird installiert. Danach erscheint folgendes Fenster:



11. Klicken Sie auf ***Fertig stellen***, um die Installation abzuschließen.

    Im Windows-Startmenü wird ein Icon mit dem Namen "PIT Windows Logon Config UI" hinzugefügt:



    Über dieses Icon können Sie die weitere Systemeinrichtung vornehmen, siehe PIT Windows Logon konfigurieren [📖 20].

6 PIT Windows Logon konfigurieren

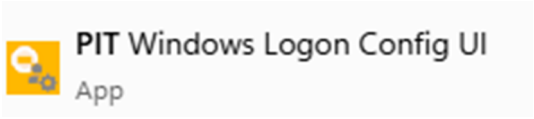
6.1 PIT Windows Logon Config UI starten

Voraussetzungen

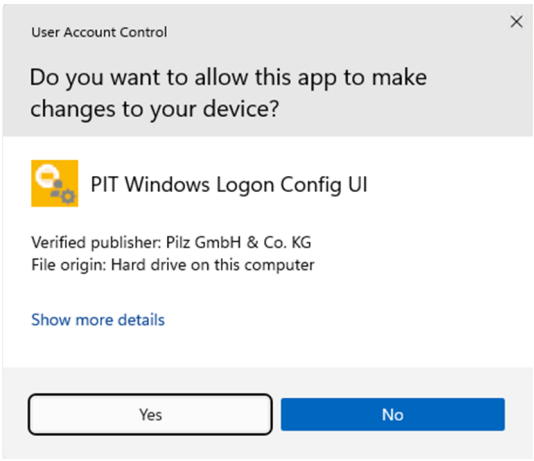
- Der PC ist eingeschaltet.
- Sie haben PIT Windows Logon installiert, PIT Windows Logon installieren [📖 18].

Vorgehensweise

1. Klicken Sie im Windows-Startmenü auf das PIT Windows Logon Config UI Icon:

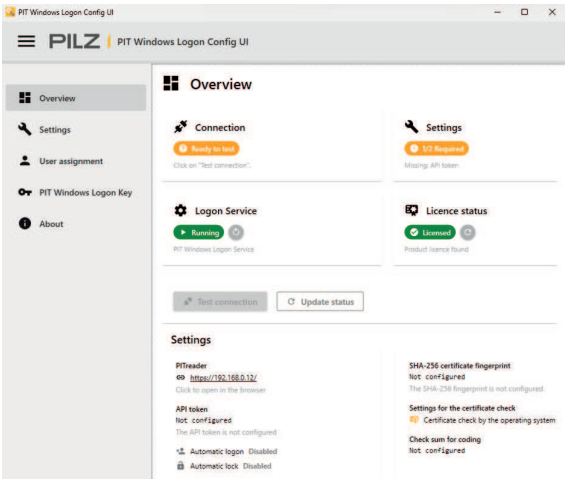


Falls das Menü ***Benutzerkontensteuerung*** erscheint:

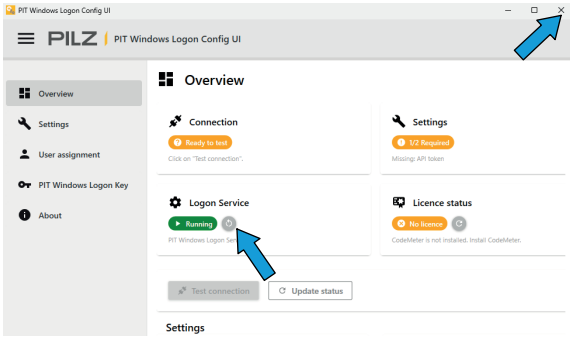


Klicken Sie zuerst auf ***Ja***.

Das Konfigurationsmenü wird angezeigt:

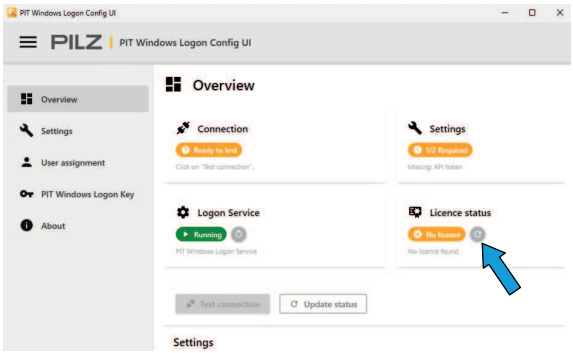


6.1.1 Falls CodeMeter Runtime noch nicht installiert ist



Nach dem Starten von PIT Windows Logon Config UI erscheint kurz die Meldung: ***Die Lizenzprüfung ist fehlgeschlagen***. ***CodeMeter ist nicht installiert. Installieren Sie CodeMeter.***
Diese Information sehen Sie auch im Konfigurationsmenü unter ***Lizenzstatus***.

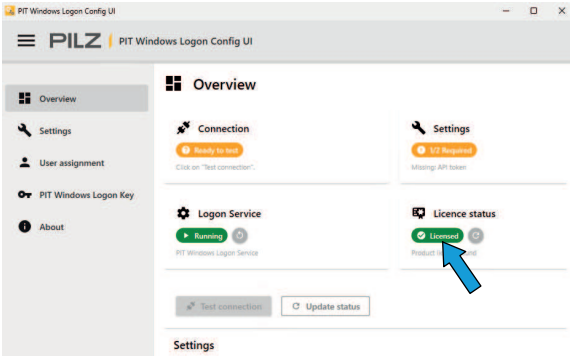
1. Installieren Sie CodeMeter Runtime, siehe CodeMeter Runtime installieren [📖 39].
2. Starten Sie den ***Logon Service*** neu. Drücken Sie dazu den entsprechenden Button.
3. Schließen Sie PIT Windows Logon Config UI. Drücken Sie dazu oben rechts auf das "X".
4. Starten Sie PIT Windows Logon Config UI, siehe PIT Windows Logon Config UI starten [📖 20].



   Nach dem Starten von PIT Windows Logon Config UI erscheint kurz die Meldung ***Die Lizenzprüfung ist fehlgeschlagen Es wurde keine Produktlizenz gefunden***. Diese Information sehen Sie auch im Konfigurationsmenü unter ***Lizenzstatus***.

5. Aktivieren Sie die PIT Windows Logon Lizenz in CodeMeter Runtime, siehe Lizenzierung [📖 48].
6. Aktualisieren Sie die Anzeige ***Lizenzstatus***. Drücken Sie dazu den entsprechenden Button.

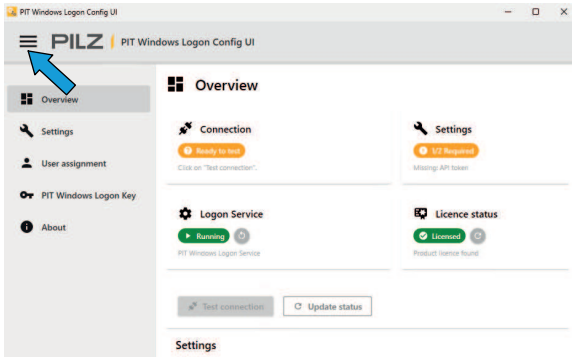
   Der Status wird grün angezeigt:



6.2 Sprache einstellen

Voraussetzungen

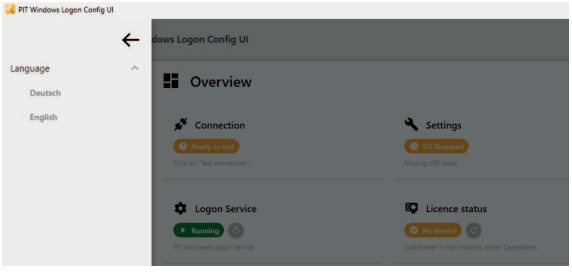
- PIT Windows Logon Config UI ist gestartet, siehe PIT Windows Logon Config UI starten [20].



Vorgehensweise

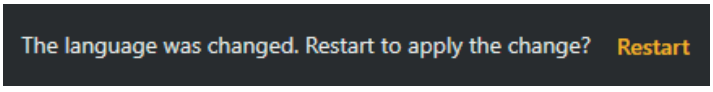
1. Klicken Sie oben links auf das Burgermenü.

   Das Dropdown-Menü ***Sprache*** wird angezeigt:



2. Öffnen Sie das Dropdown-Menü ***Sprache*** und wählen Sie ***English*** oder ***Deutsch***.

   Unten erscheint kurz eine Aufforderungsmeldung in der gewählten Sprache, z. B.:



3. Klicken Sie auf den gelben Aufforderungstext, z. B. ***Restart***.

   PIT Windows Logon Config UI wird neu gestartet und in der gewählten Sprache angezeigt.

6.3 Grundkonfiguration vornehmen

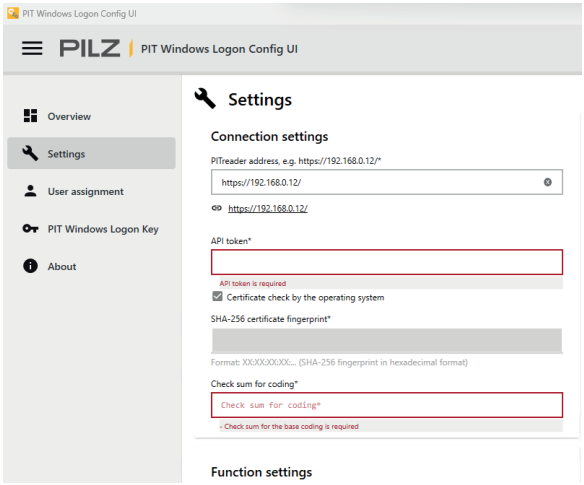
Voraussetzungen

- Der PITreader ist montiert und mit dem PC verbunden, siehe PITreader Bedienungsanleitung (1004806).
- Die Web-Anwendung des PITreaders kann konfiguriert werden, siehe PITreader Bedienungsanleitung (1004806).
- Die Basis-Codierung im PITreader muss gesetzt sein, siehe PITreader Bedienungsanleitung (1004806).
- PIT Windows Logon Config UI ist gestartet, siehe PIT Windows Logon Config UI starten [20].
- Sie sind als Administrator am PC angemeldet.

Vorgehensweise

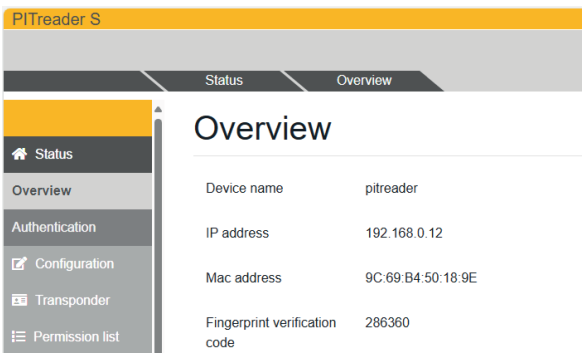
1. Klicken Sie auf ***Einstellungen***.

   Das Menü ***Einstellungen*** wird angezeigt:



2. Öffnen Sie die PITreader Web-Anwendung, siehe PITreader Bedienungsanleitung (1004806).
3. Wählen Sie in der Web-Anwendung ***Status***.

   Das Fenster ***Übersicht*** wird angezeigt:

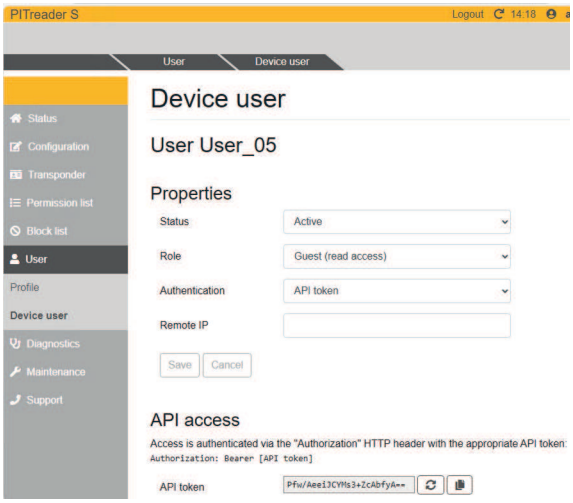


4. Kopieren Sie die ***IP-Adresse*** des PITreaders.
5. Wechseln Sie zu PIT Windows Logon Config UI.

6. Fügen Sie die kopierte IP-Adresse des PITreaders ein unter ***Verbindungseinstellungen*** im Feld ***PITreader-Adresse z. B. https://192.168.0.12/****.
7. Öffnen Sie die PITreader Web-Anwendung.
8. Wählen Sie in der Web-Anwendung ***Anwender -> Geräteanwender***.

   Das Fenster ***Geräteanwender*** wird angezeigt.
9. Wählen Sie den gewünschten Geräteanwender oder legen Sie einen neuen Geräteanwender an.
10. Wählen Sie bei Eigenschaften im Feld ***Rolle*** den Eintrag ***Gast (Lesezugriff)***.
11. Wählen Sie bei Eigenschaften im Feld ***Authentifizierung*** den Eintrag ***API-Token***.

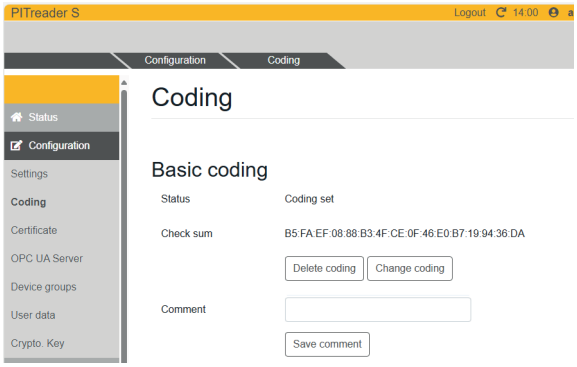
    Der API-Token wird erzeugt und angezeigt:



12. Klicken Sie auf ***Speichern***.

    Der API-Token wird gespeichert.
13. Kopieren Sie den angezeigten API-Token.
14. Wechseln Sie zu PIT Windows Logon Config UI.
15. Wählen Sie das Menü ***Einstellungen***.
16. Fügen Sie den kopierten API-Token ein unter ***Verbindungseinstellungen*** im Feld ***API-Token***.
17. Öffnen Sie die PITreader Web-Anwendung.
18. Wählen Sie in der Web-Anwendung ***Konfiguration -> Codierung***.

    Das Fenster ***Codierung*** wird angezeigt:



19. Kopieren Sie die Prüfsumme der Codierung unter ***Basis-Codierung***, ***Prüfsumme***.
20. Wechseln Sie zu PIT Windows Logon Config UI.
21. Wählen Sie das Menü ***Einstellungen***.
22. Fügen Sie die kopierte Prüfsumme, aus der Web-Anwendung, ein unter ***Verbindungseinstellungen*** im Feld ***Prüfsumme der Codierung***.
23. Klicken Sie auf ***Speichern.***

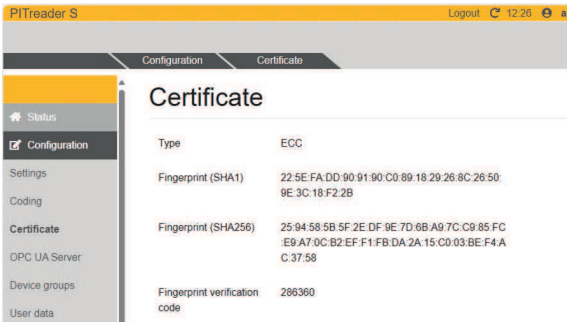
    Alle Eingaben werden gespeichert. Oben rechts erscheint die Meldung ***Der PIT Windows Logon Service muss neu gestartet werden***.
24. Klicken Sie oben rechts den Button neben der Meldung.

    Der Service wird neu gestartet.

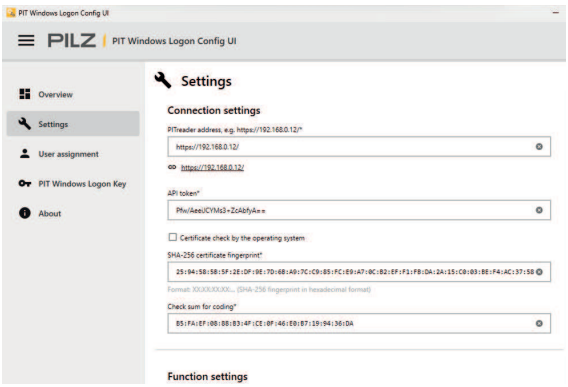
Optional: Die Zertifikatsprüfung soll nicht durch das Betriebssystem erfolgen:

1. Öffnen Sie die PITreader Web-Anwendung, siehe PITreader Bedienungsanleitung (1004806).
2. Wählen Sie in der Web-Anwendung ***Konfiguration -> Zertifikat***.

   Das Fenster ***Zertifikat*** wird angezeigt:



3. Kopieren Sie den Fingerabdruck unter ***Fingerabdruck (SHA256).***
4. Wechseln Sie zu PIT Windows Logon Config UI.
5. Deaktivieren Sie das Kontrollkästchen ***Zertifikatsprüfung durch das Betriebssystem***.
6. Fügen Sie den Fingerabdruck, aus der Web-Anwendung, ein unter ***Verbindungseinstellungen*** im Feld ***SHA256 Fingerabdruck des Zertifikats***.



7. Klicken Sie auf ***Speichern.***

Alle Eingaben werden gespeichert. Oben rechts erscheint die Meldung ***Der PIT Windows Logon Service muss neu gestartet werden***.

8. Klicken Sie oben rechts den Button neben der Meldung.

   Der Service wird neu gestartet.

6.4 Funktionseinstellungen vornehmen

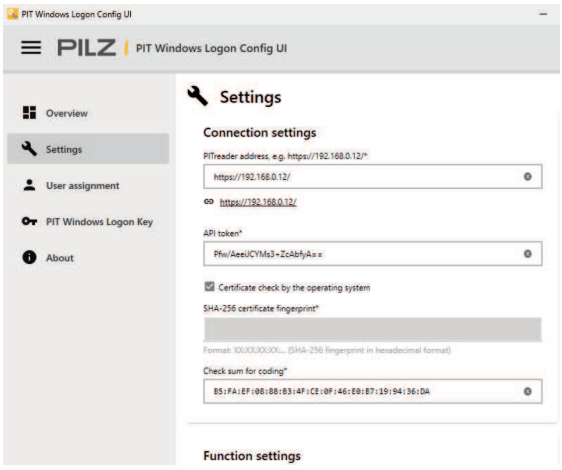
Voraussetzungen

- PIT Windows Logon Config UI ist gestartet, siehe PIT Windows Logon Config UI starten [20].
- Sie haben die Grundkonfiguration vorgenommen, siehe Grundkonfiguration vornehmen [23].
- Sie sind als Administrator am PC angemeldet.

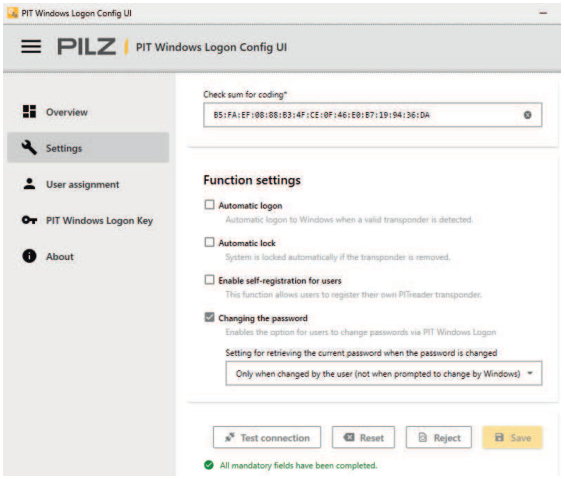
Vorgehensweise

1. Klicken Sie auf ***Einstellungen***.

   Das Menü ***Einstellungen*** wird angezeigt:



2. Nehmen Sie unter ***Funktionseinstellungen*** Ihre individuellen Einstellungen vor, siehe Beschreibung der Funktionen [28].



3. Klicken Sie auf ***Speichern***.

   Alle Eingaben werden gespeichert. Oben rechts erscheint die Meldung ***Der PIT Windows Logon Service muss neu gestartet werden***.

4. Klicken Sie oben rechts den Button neben der Meldung.

   Der Service wird neu gestartet.

6.4.1 Beschreibung der Funktionen

6.4.1.1 Automatische Anmeldung

Wenn das Kontrollkästchen ***Automatische Anmeldung*** aktiviert ist:

Wenn Sie einen gültigen Transponder am PITreader platzieren, werden Sie automatisch am PC angemeldet.

6.4.1.2 Automatische Sperre

Wenn das Kontrollkästchen ***Automatische Sperre*** aktiviert ist:

Wenn Sie den angemeldeten Transponder am PITreader entfernen, werden Sie automatisch am PC abgemeldet.

INFO

Die Funktion Automatische Sperre steht erst zur Verfügung, wenn

- der Dienst PIT Windows Logon Service neu gestartet wurde und
- Sie sich erneut am PC angemeldet haben.

6.4.1.3 Selbstregistrierung für Benutzer aktivieren

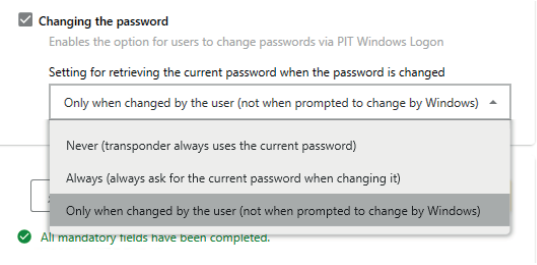
Wenn

- das Kontrollkästchen ***Selbstregistrierung für Benutzer aktivieren*** aktiviert ist,
- sich der PIT Windows Logon Key auf dem Transponder befindet, siehe PIT Windows Logon Key generieren und verwalten [📖 30],
- auf dem PC ein gültiges Windows-Benutzerkonto existiert:

Benutzer können ihren eigenen Transponder selbst registrieren.

6.4.1.4 Ändern des Kennworts

Wenn das Kontrollkästchen ***Ändern des Kennworts*** aktiviert ist, können Sie im Dropdown-Menü eine der folgenden Optionen wählen:



- ***Niemals (aktuelles Kennwort wird immer vom Transponder verwendet)***

  Das aktuelle Kennwort wird immer vom Transponder übernommen.
  Beim Ändern müssen Sie auf der Windows-Anmeldemaske zweimal das neue Kennwort eingeben.

- ***Immer (beim Ändern immer nach dem aktuellen Kennwort fragen)***

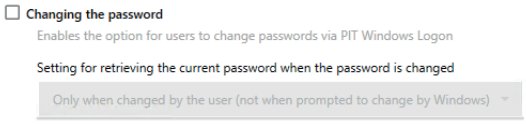
Beim Ändern müssen Sie auf der Windows-Anmeldemaske einmal das aktuelle Kennwort und zweimal das neue Kennwort eingeben.
Dies entspricht dem Standardverhalten von Windows.

- ***Nur bei Änderung durch den Benutzer (nicht bei Aufforderung zum Ändern durch Windows)***

  Wenn Sie die Kennwortänderung am PC über die Tasten Strg + Alt + Entf starten:
  Auf der Windows-Anmeldemaske müssen Sie einmal das aktuelle Kennwort und zweimal das neue Kennwort eingeben.

  Erzwingt Windows die Änderung, z. B. wegen eines abgelaufenen Kennworts, können Sie ein neues Kennwort vergeben, ohne das aktuelle Kennwort einzugeben.

Wenn das Kontrollkästchen ***Ändern des Kennworts*** deaktiviert ist:



Die Kennwortänderung erfolgt über die Standardfunktion von Windows.
Wenn Sie das Kennwort über Windows oder Active Directory ändern, müssen Sie bei der nächsten Anmeldung über PIT Windows Logon das neue Kennwort eingeben. Nur so kann die Anmeldung erfolgen.

6.5 PIT Windows Logon Key generieren und verwalten

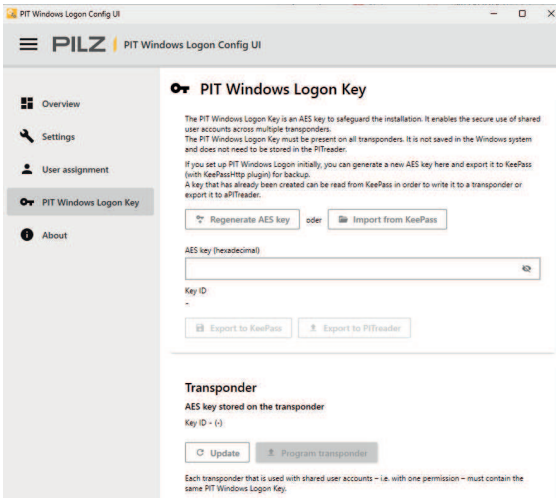
Voraussetzungen

- PIT Windows Logon Config UI ist gestartet, siehe PIT Windows Logon Config UI starten [📖 20].
- Sie haben die Grundkonfiguration vorgenommen, Grundkonfiguration vornehmen [📖 23].
- Sie sind als Administrator am PC angemeldet.

Vorgehensweise

1. Klicken Sie auf ***PIT Windows Logon Key***.

   Das Menü ***PIT Windows Logon Key*** wird angezeigt:

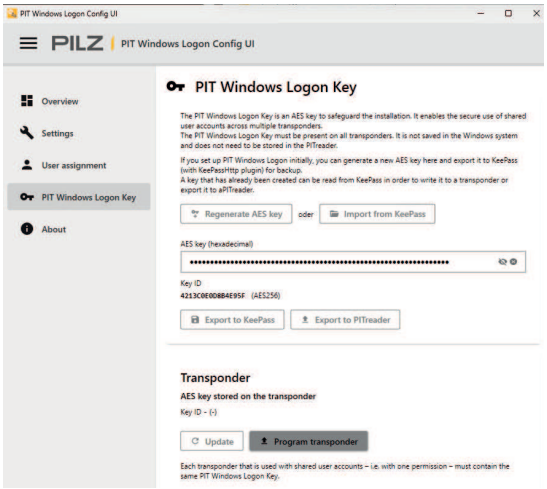


2. Wählen Sie

   AES-Schlüssel neu generieren – der AES-Schlüssel wird generiert und im Feld ***AES-Schlüssel (Hexadezimal)*** angezeigt.

   oder

   Importieren aus KeePass - der in KeePass gesicherte AES-Schlüssel wird importiert und im Feld ***AES-Schlüssel (Hexadezimal)*** angezeigt:



3. Wählen Sie

Export nach KeePass, wenn Sie den AES-Schlüssel in KeePass sichern möchten.

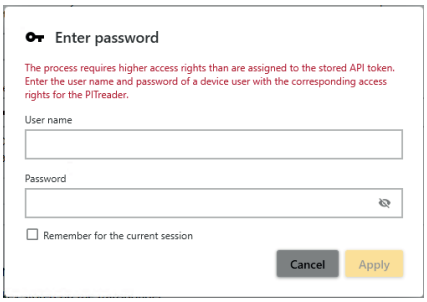
und/oder

Export an PITreader, wenn Sie den AES-Schlüssel im PITreader sichern möchten, siehe PIT Windows Logon Key von PIT Windows Logon exportieren [📖 46].

Um den Transponder nutzen zu können, muss der PIT Windows Logon Key auf dem Transponder hinterlegt werden:

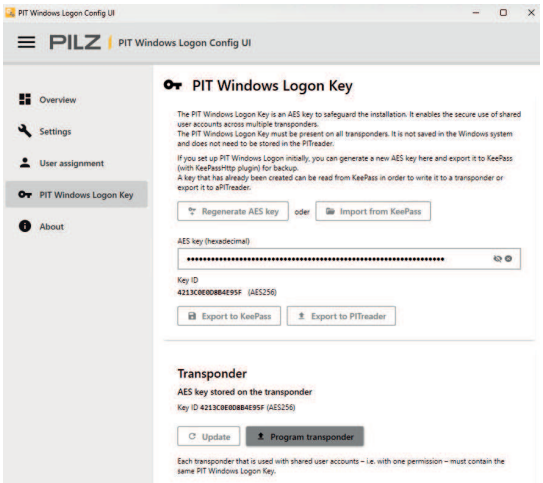
1. Platzieren Sie einen Transponder am PITreader, siehe PITreader Bedienungsanleitung (1004806).
2. Klicken Sie auf ***Transponder programmieren***.

   Das Fenster ***Kennwort eingeben*** wird angezeigt:



3. Geben Sie Ihren Benutzernamen und das Kennwort für den PITreader ein.
4. Klicken Sie auf ***Anwenden***.

   Der PIT Windows Logon Key wird auf den Transponder geschrieben und angezeigt:



5. Wenn Sie den aktuellen AES-Schlüssel des Transponders anzeigen möchten, klicken Sie auf ***Aktualisieren***.

6.6 Benutzerzuordnung vornehmen

Voraussetzungen

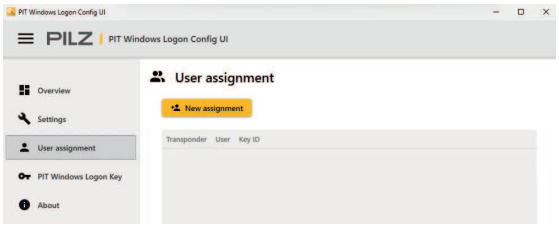
- Sie sind als Administrator am PC angemeldet.
- PIT Windows Logon Config UI ist gestartet, siehe PIT Windows Logon Config UI starten [📖 20].

- Sie haben die Grundkonfiguration vorgenommen, siehe Grundkonfiguration vornehmen [23].
- Ein PITreader ist mit dem PC verbunden.
- Ein Transponder mit PIT Windows Logon Key ist im Lesebereich des PITreaders.

Vorgehensweise

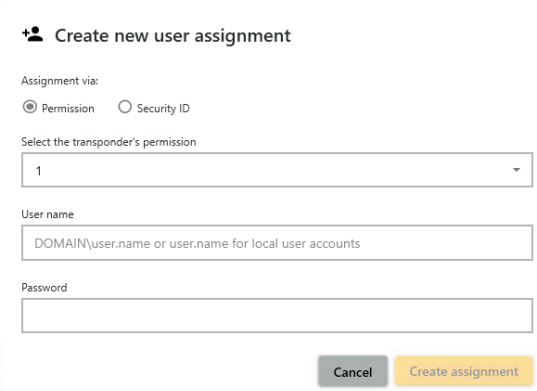
1. Klicken Sie auf ***Benutzerzuordnung***.

   Das Menü ***Benutzerzuordnung*** wird angezeigt:



2. Klicken Sie auf ***Neue Zuordnung***.

   Das Menü ***Neue Benutzerzuordnung anlegen*** wird angezeigt:



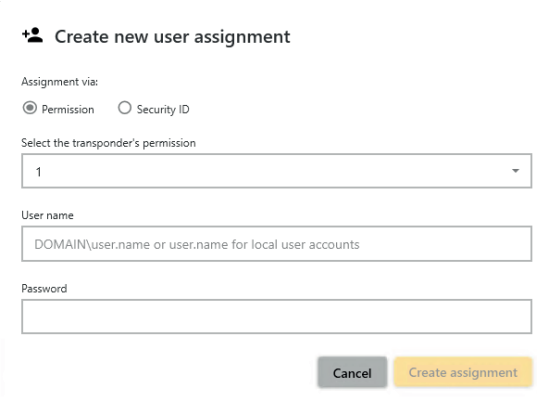
3. Wählen Sie bei ***Zuordnung über:***

   Berechtigung, wenn die Anmeldung zu diesem Benutzerkonto über mehrere Transponder möglich sein soll (geteilte Benutzerkonten), siehe Berechtigung [33].

   oder

   Security ID, wenn die Anmeldung zu diesem Benutzerkonto nur über einen Transponder möglich sein soll (persönliche Benutzerkonten), siehe Security ID [33].

6.6.1 Berechtigung



1. Wählen Sie im Dropdown-Menü ***Berechtigung des Transponders wählen*** die Berechtigung aus, die ein Transponder mindestens haben muss, damit man sich an diesem Benutzerkonto anmelden kann.
2. Geben Sie im Feld ***Benutzername*** den Benutzername des Windows-Kontos ein.

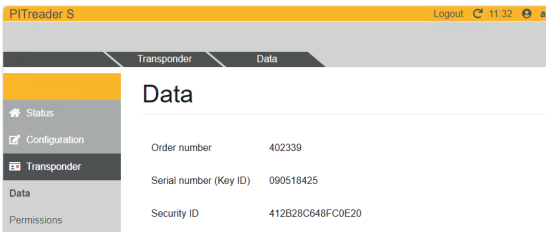
   Bei Domainkonten in einem Unternehmensnetzwerk muss der Benutzername mit Angabe der Domain angegeben werden, z. B. COMPANY\user.name oder als "Benutzerprinzipalname" (UPN), z. B. user.name@company.com.
3. Geben Sie im Feld ***Kennwort*** das Kennwort des Windows-Benutzerkontos ein.
4. Klicken Sie auf ***Zuordnung anlegen***.

6.6.2 Security ID

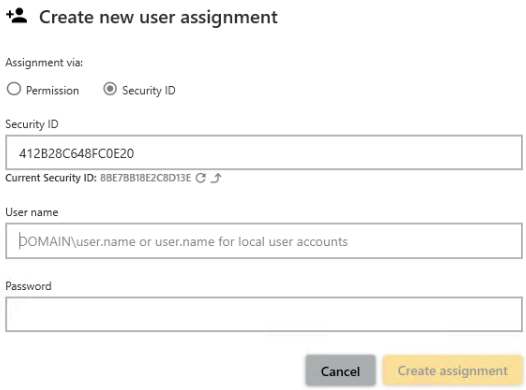
Wenn die Funktion ***Selbstregistrierung für Benutzer aktivieren*** aktiviert ist, können Anwender ohne Admin-Berechtigung über die Anmeldemaske auch selbstständig ihren Transponder zur Anmeldung mit ihrem persönlichen Windows-Benutzer registrieren, siehe Transponder selbst registrieren [📖 37].

1. Öffnen Sie die PITreader Web-Anwendung, siehe PITreader Bedienungsanleitung (1004806).
2. Wählen Sie in der Web-Anwendung ***Transponder***.

   Das Fenster ***Daten*** wird angezeigt:



3. Kopieren Sie die Security-ID des Transponders.
4. Wechseln Sie zu PIT Windows Logon Config UI.
5. Fügen Sie die kopierte Security ID des Transponders im Feld ***Security ID*** ein.



   Diese Security ID wird dann für die Anmeldung verwendet.
6. Geben Sie im Feld ***Benutzername*** den Benutzername des Windows-Kontos ein.

   Bei Domainkonten in einem Unternehmensnetzwerk muss der Benutzername mit Angabe der Domain angegeben werden, z. B. COMPANY\user.name oder als "Benutzerprinzipalname" (UPN), z. B. user.name@company.com.
7. Geben Sie im Feld ***Kennwort*** das Kennwort des Windows-Benutzerkontos ein.
8. Klicken Sie auf ***Zuordnung anlegen***.

7 Updates installieren

Updates können über eine vorhandene Version installiert werden. Dabei werden alle Einstellungen, Benutzerzuordnungen und Zugangsdaten aus der vorherigen Version übernommen.

Wenn die Anmeldemaske mit geladenem PIT Windows Logon Credential Provider geöffnet ist, muss der PC nach dem Update neu gestartet werden. Dies gilt z. B, wenn ein Update über eine Remote-Verbindung oder automatisiert im Hintergrund installiert wird.

8 Betrieb

8.1 Transponder am PITreader platzieren

Wie Sie die unterschiedlichen Transponder am PITreader platzieren finden Sie in der PITreader Bedienungsanleitung (1004806).

8.2 Am Windows-PC anmelden

8.2.1 Anmeldung über den Windows-Anmeldebildschirm

Voraussetzungen

- PIT Windows Logon ist konfiguriert, siehe PIT Windows Logon konfigurieren [📖 20].
- Der PC ist eingeschaltet.
- Ein Transponder ist am PITreader platziert.

Vorgehensweise

1. Klicken Sie auf dem Windows-Anmeldebildschirm auf ***Anmelden***.

   Die Anmeldedaten werden geprüft.

   Wenn die Anmeldedaten korrekt sind, wird die Anmeldung durchgeführt und der Windows-Desktop angezeigt.

8.2.2 Automatische Anmeldung

Voraussetzungen

- PIT Windows Logon ist konfiguriert, siehe PIT Windows Logon konfigurieren [📖 20].
- In der Konfiguration ist unter ***Funktionseinstellungen*** das Kontrollkästchen ***Automatische Anmeldung*** aktiviert, siehe Funktionseinstellungen vornehmen [📖 27].
- Der PC ist eingeschaltet.

Vorgehensweise

1. Platzieren Sie einen Transponder am PITreader.

   Die Anmeldedaten werden geprüft.

   Wenn die Anmeldedaten korrekt sind, wird die Anmeldung durchgeführt und der Windows-Desktop angezeigt.

8.3 Am Windows-PC abmelden

8.3.1 Abmeldung über den Windows-Desktop

- Der PC ist eingeschaltet.
- Sie sind am PC angemeldet.

Vorgehensweise

1. Melden Sie sich in Windows ab, wie bei einem PC ohne PITreader.

   Der Windows-Anmeldebildschirm wird angezeigt.

8.3.2 Automatische Abmeldung

Voraussetzungen

- PIT Windows Logon ist konfiguriert, siehe PIT Windows Logon konfigurieren [20].
- In der Konfiguration ist unter ***Funktionseinstellungen*** das Kontrollkästchen ***Automatische Sperre*** aktiviert, siehe Funktionseinstellungen vornehmen [27].
- Der PC ist eingeschaltet.
- Sie sind am PC angemeldet.

Vorgehensweise

1. Entfernen Sie den Transponder am PITreader.

   Der Windows-Anmeldebildschirm wird angezeigt.

INFO

Die Funktion ***Automatische Sperre*** steht erst zur Verfügung, wenn Sie sich erneut am PC angemeldet haben.

8.4 Transponder selbst registrieren

Voraussetzungen

- PIT Windows Logon ist konfiguriert, siehe Grundkonfiguration vornehmen [23].
- In der Konfiguration ist unter ***Funktionseinstellungen*** das Kontrollkästchen ***Selbstregistrierung für Benutzer aktivieren*** aktiviert, siehe Funktionseinstellungen vornehmen [27].
- Der PC ist eingeschaltet.
- Ein Transponder ist am PITreader platziert.

Vorgehensweise

1. Klicken Sie auf dem Windows-Anmeldebildschirm auf ***Transponder registrieren…***.

   Die Eingabefelder für Benutzernamen und Kennwort werden angezeigt.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.
3. Bestätigen Sie die Eingabe.

   Der Transponder ist registriert. Sie können sich künftig mit diesem Transponder an diesem Windows-PC anmelden.

8.5 Windows-Kennwörter aktualisieren

Voraussetzungen

- PIT Windows Logon ist konfiguriert, siehe PIT Windows Logon konfigurieren [20].
- In der Konfiguration ist unter ***Funktionseinstellungen*** das Kontrollkästchen ***Ändern des Kennworts*** aktiviert, siehe Funktionseinstellungen vornehmen [27].
  PIT Windows Logon ist dann standardmäßig in die Windows-Oberfläche zum Ändern von Kennwörtern integriert.

- Der PC ist eingeschaltet.
- Sie sind am PC angemeldet.

Vorgehensweise

1. Rufen Sie am PC die Kennwortänderung über die Tasten Strg + Alt + Entf auf.

   Die angezeigten Felder hängen von der Einstellung in PIT Windows Logon Config UI ab, siehe Ändern des Kennworts [📖 28].

9 CodeMeter Runtime installieren

Für den Betrieb von PIT Windows Logon benötigen Sie eine Lizenz, die über CodeMeter (WIBU Systems AG) auf dem PC installiert ist.

INFO

Installieren Sie CodeMeter Runtime, bevor Sie PIT Windows Logon installieren. So vermeiden Sie, dass der PIT Windows Logon Service nach der Installation neu gestartet werden muss.

Falls ein Neustart erforderlich ist, führen Sie ihn über die Funktion in der Oberfläche von PIT Windows Logon Config UI aus.

Voraussetzungen

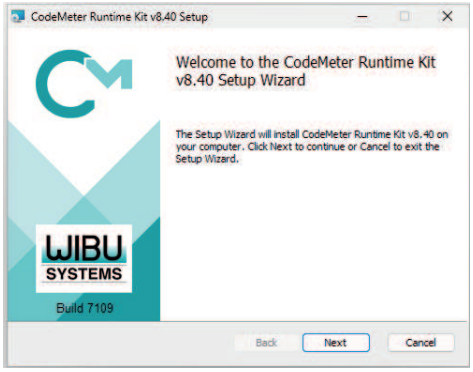
- Der PC ist eingeschaltet.
- Sie verfügen über Administratorrechte auf dem Windows-PC.

Installation

Die Software CodeMeter Runtime finden Sie im Downloadpaket von PIT Windows Logon.

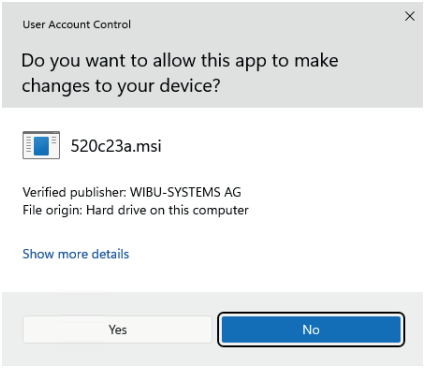
1. Führen Sie den Download durch von "PITWindowsLogon_<Version>.zip, siehe PIT Windows Logon installieren [📖 18].
2. Entpacken Sie die Zip-Datei.
3. Doppelklicken Sie auf die Installationsdatei "CodeMeterRuntime64.msi".

   Das Setup-Fenster wird angezeigt:



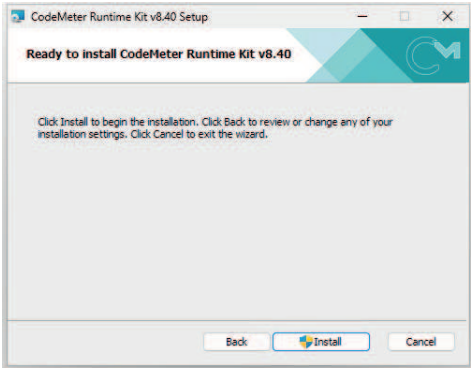
4. Klicken Sie auf ***Weiter*** um den Installationsassistenten zu starten.
5. Folgen Sie den Anweisungen im Setup:
   Akzeptieren Sie die Lizenzbedingungen.
   Wählen Sie die Standardinstallation (empfohlen).
6. Klicken Sie auf ***Installieren***.

   Falls das Menü Benutzerkontensteuerung erscheint:



Klicken Sie zuerst auf ***Ja***.

CodeMeter wird installiert. Danach erscheint folgendes Fenster:



7. Klicken Sie auf ***Fertig stellen***, um die Installation abzuschließen.

   Im Windows-Startmenü wird ein Icon mit dem Namen "CodeMeter Contol Center" hinzugefügt

Zusätzlich erscheint das CodeMeter-Icon in der Windows-Statusleiste.

10 PIT Windows Logon Key in KeePass sichern

Um den PIT Windows Logon Key über KeePass 2 zu sichern, muss

- das KeePassHttp-Plugin installiert sein
- eine KeePass-Datenbank angelegt sein.

10.1 KeePassHttp-Plugin installieren

Voraussetzungen

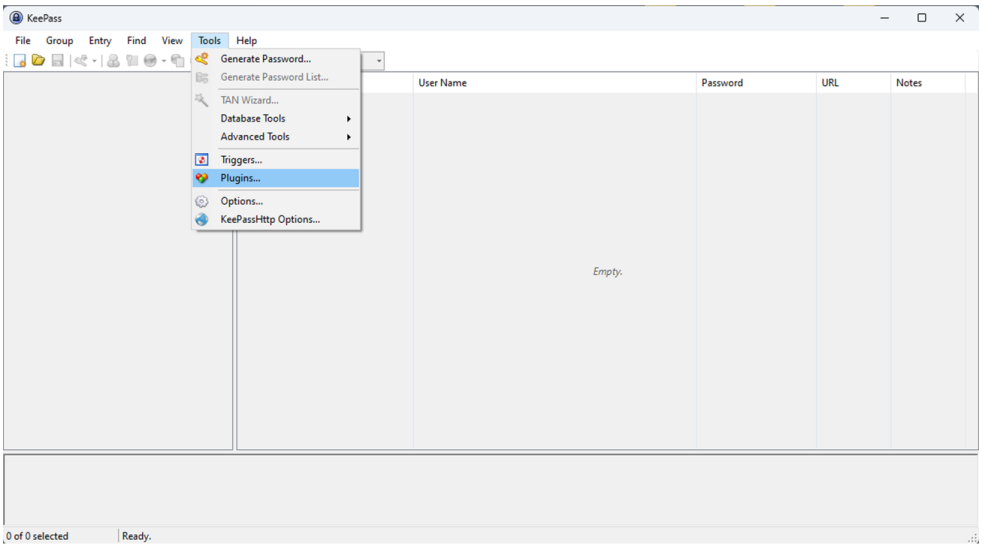
- KeePass 2 ist installiert.

  Den Download-Link für KeePass 2 finden Sie unter:
  https://keepass.info/download.html
- Der PC ist eingeschaltet.
- Sie verfügen über Administratorrechte auf dem Windows-PC.

Vorgehensweise

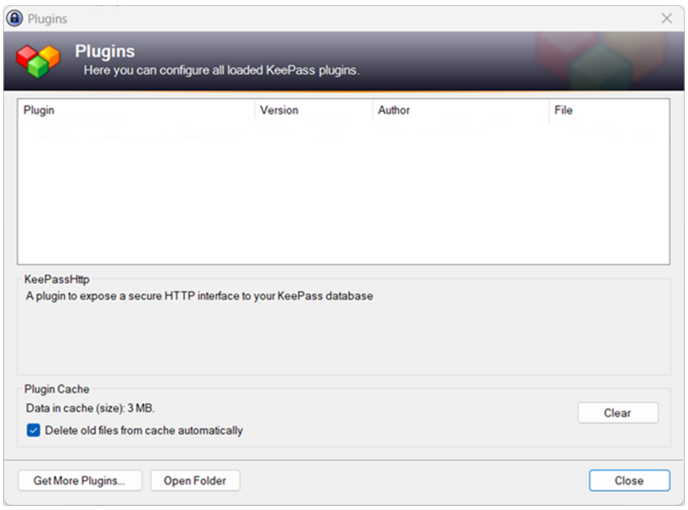
1. Laden Sie das KeePassHttp-Plugin über den folgenden Link herunter:
   https://raw.github.com/pfn/keepasshttp/master/KeePassHttp.plgx
2. Starten Sie das Programm KeePass 2.

   Das Menüfenster wird angezeigt.

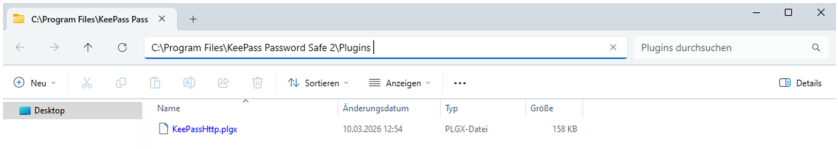


3. Wählen Sie in der Menüleiste ***Tools*** -> ***Plugins***.

   Das Menü “Plugins“ wird angezeigt.



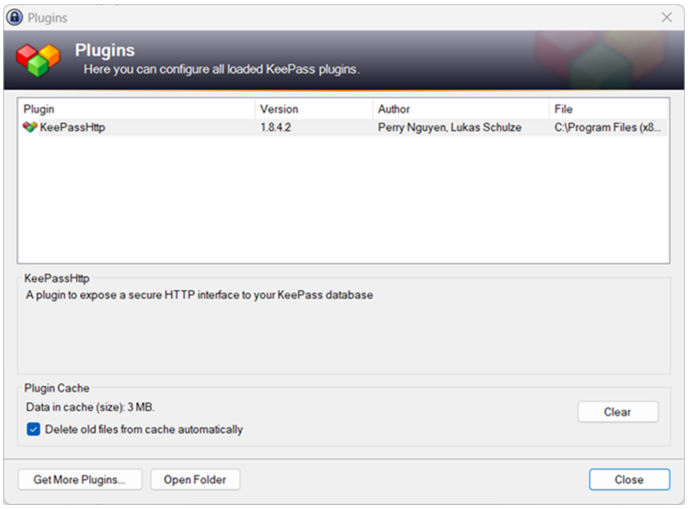
4. Klicken Sie auf ***Verzeichnis öffnen.***
5. Öffnen Sie das Verzeichnis in dem sich die heruntergeladene Datei "KeePassHttp.plgx" befindet.
6. Kopieren Sie die Datei "KeePassHttp.plgx" in das Menü "Plugins" und fügen Sie es in den Installations-Ordner (C:\Program Files\KeePass Password Safe 2\Plugins) für die KeePass Plugins hinzu.



7. Klicken Sie auf ***Schließen***.

   Das Menü "Plugins" wird geschlossen.
8. Beenden Sie KeePass 2 und starten Sie KeePass 2 erneut.

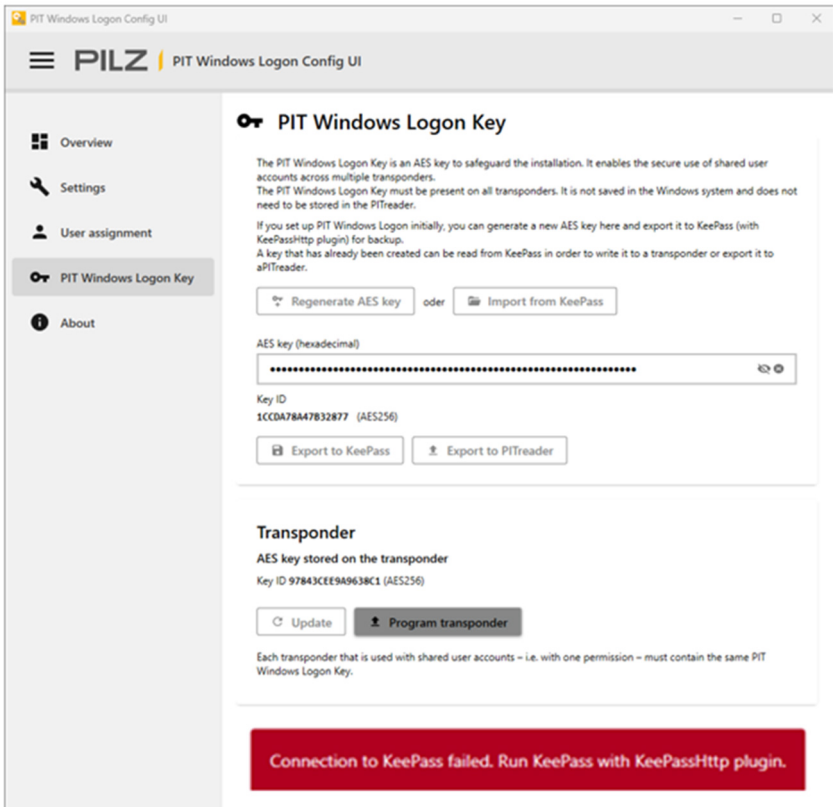
   Nach dem Neustart ist das KeePassHttp-Plugin installiert. Das KeePassHttp-Plugin “ KeePassHttp“ wird im Menü "Plugins" angezeigt.



10.2 Datenbank in KeePass 2 anlegen

Damit der PIT Windows Logon Key exportiert werden kann, muss eine KeePass-Datenbank angelegt sein.

Ist keine KeePass-Datenbank vorhanden, wird folgende Fehlermeldung in einem roten Rahmen angezeigt – auch wenn das KeePassHttp-Plugin installiert ist:
Connection to KeePass failed. Run KeePass with KeePassHTTP plugin



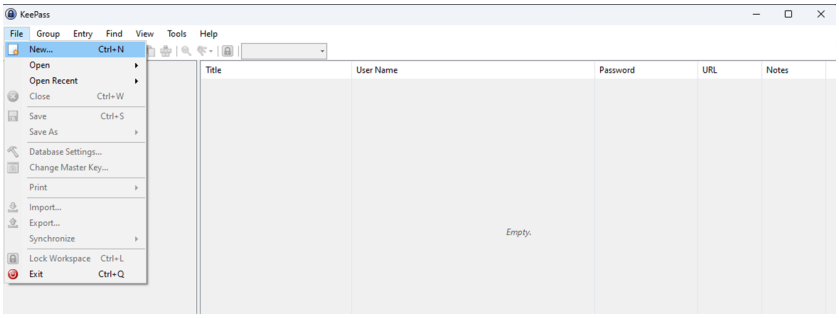
Voraussetzungen

- KeePass 2 und KeePassHttp-Plugin sind installiert, siehe KeePassHttp-Plugin installieren [📖 41].
- Der PC ist eingeschaltet.
- Sie verfügen über Administratorrechte auf dem Windows-PC.

Vorgehensweise

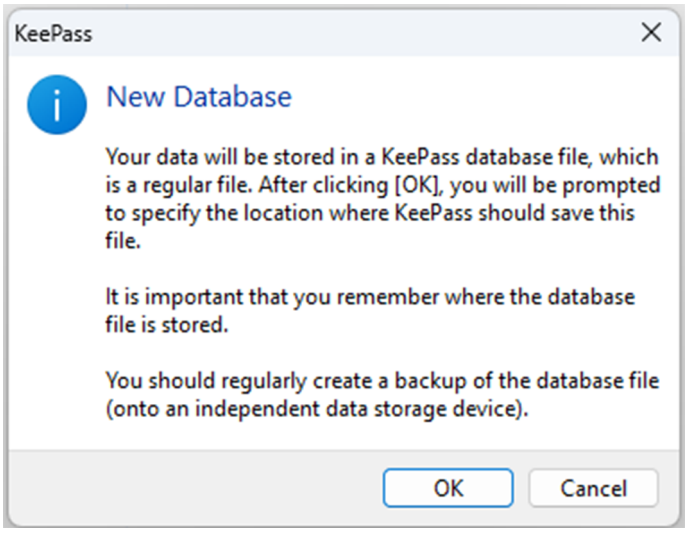
1. Starten Sie das Programm "KeePass 2".

   Das Programm wird angezeigt.



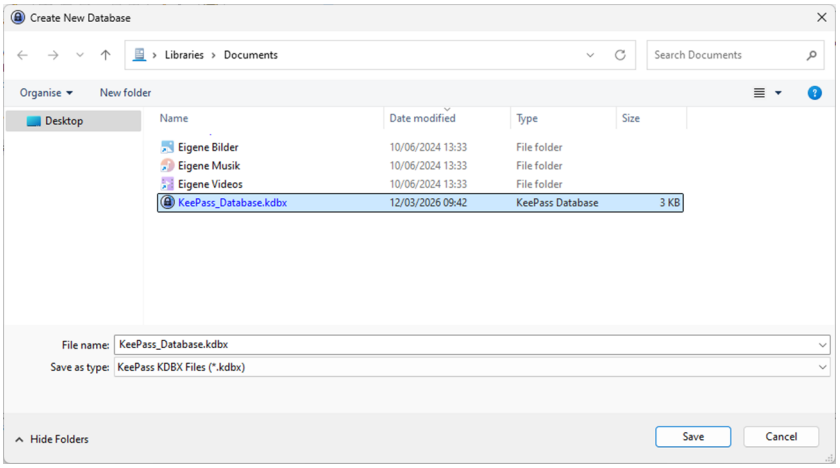
2. Wählen Sie in der Menüleiste ***Datei*** und anschließend ***Neu.***

   Das Fenster "KeePass" mit Hinweisen zur Datenbank wird angezeigt.



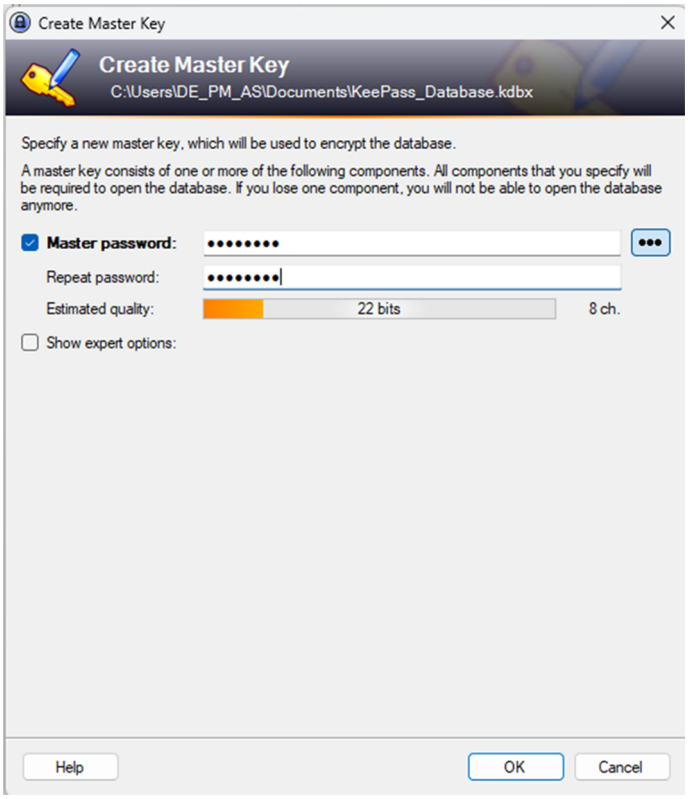
3. Klicken Sie auf ***OK***.

   Das Fenster „Neue Datenbank erstellen“ erscheint.



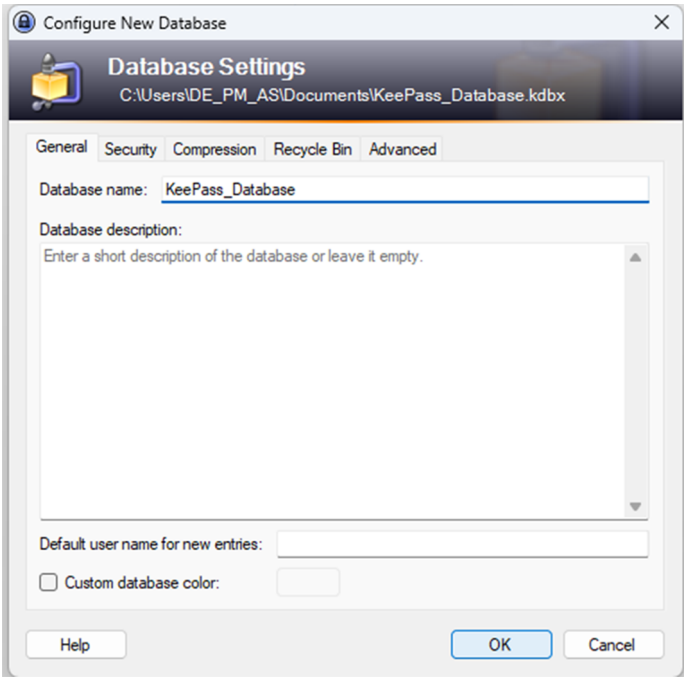
4. Wählen Sie einen geeigneten Speicherort und vergeben Sie einen eindeutigen Namen für die Datenbank, z. B. "KeePass_Database".
5. Klicken Sie auf ***Speichern***.

   Das Fenster „Hauptschlüssel erstellen“ erscheint.



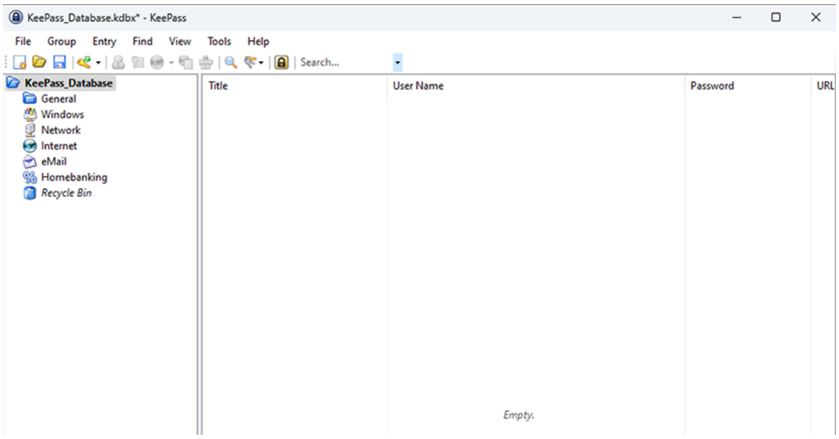
6. Erstellen Sie das Hauptpasswort für die Datenbank.
7. Klicken Sie auf ***OK***.

   Das Menü "neue Datenbank konfigurieren" erscheint.



8. Konfigurieren Sie bei Bedarf die Datenbank.
9. Klicken Sie auf ***OK***.

Die neu angelegte, leere KeePass-Datenbank wird angezeigt, z. B. "KeePass_Database.kdbx* - KeePass".



10.3 PIT Windows Logon Key von PIT Windows Logon exportieren

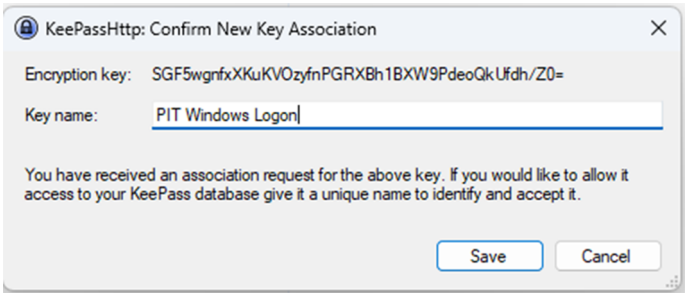
Voraussetzungen

- KeePass 2 mit KeePassHttp-Plugin sind installiert, KeePassHttp-Plugin installieren [📖 41].
- Eine KeePass-Datenbank ist angelegt, Datenbank in KeePass 2 anlegen [📖 43].
- Sie verfügen über Administratorrechte auf dem Windows-PC.
- KeePass 2 ist gestartet.

Vorgehensweise

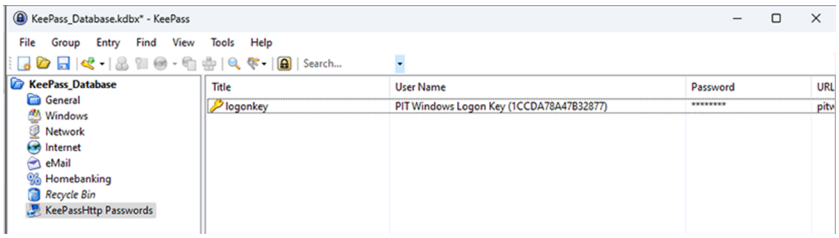
1. Exportieren Sie den PIT Windows Logon Key aus PIT Windows Logon, PIT Windows Logon Key generieren und verwalten [📖 30].

   Wenn Sie den PIT Windows Logon Key zum ersten Mal exportieren, erscheint das Fenster "KeePassHttp. Confirm New Key Association".



2. Geben Sie einen geeigneten Namen für die Verbindung zwischen KeePass 2 und PIT Windows Logon Config UI ein.
3. Klicken Sie auf ***Sichern***.

   Der PIT Windows Logon Key wird angelegt und in der KeePass-Datenbank gespeichert.


KeePass_Database.kdbx* - KeePass
File Group Entry Find View Tools Help
Search...
KeePass_Database
General
Windows
Network
Internet
eMail
Homebanking
Recycle Bin
KeePassHttp Passwords
Title
User Name
Password
URL
logonkey
PIT Windows Logon Key (1CCDA78A47B32877)
****

11 Lizenzierung

Die Software PIT Windows Logon steht auf der Pilz-Webseite zum Download bereit. Sie können die Software installieren und einrichten, auch wenn keine Lizenz aktiviert ist.

Für die Anmeldung an einem Windows-PC mit einem Transponder benötigen Sie jedoch eine aktivierte Lizenz.

Die Lizenzen werden in Lizenzcontainern verwaltet. Die Verwaltung erfolgt über die Software CodeMeter der Firma WIBU SYSTEMS. CodeMeter ist im Download-Paket von PIT Windows Logon enthalten und muss zusätzlich installiert werden. Nach der Installation erscheint das CodeMeter-Icon  in der Windows-Statusleiste.

11.1 Lizenz erwerben

Für jede Installation von PIT Windows Logon benötigen Sie eine eigene Lizenz. Das gilt für jedes Windows-System, auf dem eine Anmeldung erfolgen soll. Sie können Lizenzen im Pilz eShop oder über andere Vertriebswege erwerben.

Nach dem Kauf erhalten Sie einen Produktschein mit einem Lizenz-Ticket.
Damit die Software die Lizenz erkennt müssen Sie das Lizenz-Ticket über CodeMeter in den Lizenzcontainer importieren.

11.2 Lizenz aktivieren

Die Lizenz muss auf dem PC verfügbar sein, auf dem PIT Windows Logon verwendet wird. Dazu muss die Lizenz auf diesem PC aktiviert werden. Nach der Aktivierung ist die Lizenz an diesen PC gebunden. Bei Bedarf können Sie die Lizenz später auf einen anderen PC übertragen.

Zum Aktivieren der Lizenz gehen Sie so vor wie es bei Pilz Produkten üblich ist.

12 PIT Windows Logon deinstallieren

Bei der Deinstallation von PIT Windows Logon werden alle Einstellungen, Benutzerzuordnungen und gespeicherten Zugangsdaten vom Windows-PC gelöscht.

Voraussetzungen

- Sie verfügen über Administratorrechte auf dem Windows-PC.

Vorgehensweise

- Zum Deinstallieren von PIT Windows Logon, verwenden Sie die in Windows üblichen Deinstallationsfunktionen.

13 Bestelldaten

Produkttyp	Merkmale	Artikel-Nr.
PIT Windows Logon Licence 1	PIT Windows Logon Lizenz für 1 Aktivierung	402356

Support

Technische Unterstützung von Pilz erhalten Sie rund um die Uhr.

Amerika
Brasilien
+55 11 97569-2804
Kanada
+1 888 315 7459
Mexiko
+52 55 5572 1300
USA (toll-free)
+1 877-PILZUSA (745-9872)

Asien
China
+86 400-088-3566
Japan
+81 45 471-2281
Südkorea
+82 31 778 3390

Australien und Ozeanien
Australien
+61 3 95600621
Neuseeland
+64 9 6345350

Europa
Belgien, Luxemburg
+32 9 3217570
Deutschland
+49 711 3409-444
Frankreich
+33 3 88104003
Großbritannien
+44 1536 460866
Irland
+353 21 4804983
Italien, Malta
+39 0362 1826711
Niederlande
+31 347 320477
Österreich
+43 1 7986263-444
Schweiz
+41 62 88979-32
Skandinavien
+45 74436332
Spanien
+34 938497433
Türkiye
+90 216 5775552

Unsere internationale Hotline erreichen Sie unter:
+49 711 3409-222
support@pilz.com

Meldung von Security-Schwachstellen oder Security-Vorfällen
Wenn Sie eine Security-Schwachstelle oder einen Security-Vorfall im Zusammenhang mit einem Pilz Produkt melden möchten, wenden Sie sich bitte an unser **Pilz Product Security Incident Response Team (PSIRT).** Sie erreichen uns unter: www.pilz.com/psirt

Pilz entwickelt umweltfreundliche Produkte unter Verwendung ökologischer Werkstoffe und energiesparender Techniken. In ökologisch gestalteten Gebäuden wird umweltbewusst und energiesparend produziert und gearbeitet. So bietet Pilz Ihnen Nachhaltigkeit mit der Sicherheit, energieeffiziente Produkte und umweltfreundliche Lösungen zu erhalten.

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

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

Wir sind international vertreten. Nähere Informationen entnehmen Sie bitte unserer Homepage www.pilz.com oder nehmen Sie Kontakt mit unserem Stammhaus auf.

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

PILZ
THE SPIRIT OF SAFETY