

► PIT User Authentication Service

Readme

Version 1.5.0 · 2026-05-22

PILZ
THE SPIRIT OF SAFETY



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.

All rights to this documentation are reserved by Pilz GmbH & Co. KG. Copies may be made for the user's internal purposes. Suggestions and comments for improving this documentation will be gratefully received.

CECE[®], CHRE[®], CMSE[®], INDUSTRIAL PI[®], Leansafe[®], MYZEL[®], PAS4000[®], PAScal[®], PASconfig[®], Pilz[®], PIT[®], PMCprimo[®], PMCprotego[®], PM Ctendo[®], PMD[®], PMI[®], PNOZ[®], Primo[®], PSEN[®], PSS[®], PVIS[®], SafetyBUS p[®], SafetyEYE[®], SafetyNET p[®], THE SPIRIT OF SAFETY[®] are registered and protected trademarks of Pilz GmbH & Co. KG in some countries.



SD means Secure Digital

1	Introduction	5
1.1	Terminology	5
1.2	Notices	6
2	Overview	6
2.1	System components	7
2.2	System Requirements	7
3	Security	8
3.1	Implemented Security Measures	9
3.2	Required Security Measures	9
3.2.1	Network topology examples	10
4	Installation	10
4.1	Windows Installation	12
4.1.1	Windows Installer	12
4.1.2	Installer command line options	12
4.1.3	Run as Windows service	13
4.1.4	Service control	13
4.1.5	Run in manual mode	14
4.2	Linux Installation	14
4.2.1	Extract the tar.gz archive	14
4.2.2	Run as Linux service (daemon)	14
4.2.3	Service control	15
4.2.4	Revolution Pi firmware version	15
4.2.5	Run in manual mode	15
4.2.6	Wibu CodeMeter	16
4.3	Replace the Java Runtime	16
4.3.1	Daemon mode	16
4.3.2	Manual mode	18
5	Configuration	18
5.1	Basic Settings	19
5.1.1	Configuration file location	19
5.1.2	Configuration file format	19
5.2	HTTPS Setup	20
5.3	Web Interface	20
6	Getting Started	20
6.1	First-time setup checklist	21
7	Uninstall PIT User Authentication Service	21
7.1	Uninstall on Windows	22
7.1.1	Windows Installer / Windows service	22
7.1.2	Uninstall CodeMeter Runtime	22
7.2	Uninstall on Linux	22
7.2.1	Linux daemon	22
7.2.2	Uninstall CodeMeter Runtime	23
7.3	Manual Cleanup	23
7.3.1	Remaining files	23
7.3.2	ZIP / tar.gz archive	23
8	License Information	23
9	Appendix	24
9.1	Windows Environment Variables	25

9.2	Windows Firewall Settings for Network Scan.....	25
10	Changelog.....	25
10.1	Version 1.5.0	27
10.2	Version 1.4.1	27
10.3	Version 1.4.0	27
10.4	Version 1.3.0	27
10.5	Version 1.2.0	28
10.6	Version 1.1.2	28
10.7	Version 1.1.1	28
10.8	Version 1.1.0	28
10.9	Version 1.0.0	28

1 Introduction

About this document

This document provides the information required to install, configure, and operate PIT User Authentication Service (UAS). It covers all steps from system requirements through initial configuration to uninstallation.



For detailed information on the web interface, device management, data management, and the REST API, refer to the online help, which is accessible through the UAS web interface after installation.

Validity

This document applies to PIT User Authentication Service V1.5.x.

Target audience

This document is intended for system administrators and integrators who install and configure UAS in industrial environments. It assumes familiarity with the target operating system (Windows or Linux) and basic network administration concepts.

- ▶ [Terminology](#)  5 — Definitions of product names and abbreviations used in this document
- ▶ [Notices](#)  6 — Explanation of notice types used throughout this document

1.1 Terminology

The following terms and abbreviations are used throughout this document.

Term	Definition
PITreader	Pilz RFID transponder reader device for industrial user authentication. Includes variants such as PITreader S.
PIT gatebox (PIT gb RLLE)	PITreader variant integrated into a gate box enclosure.
PIT Transponder Manager (PTM)	Pilz software tool for managing users, transponders, permissions, and time restrictions.
PIT User Authentication Service (UAS)	Service that synchronizes user and transponder data from PIT Transponder Manager to PITreader devices.
Transponder	RFID key fob or card that is read by a PITreader device for user authentication.
CodeMeter	Wibu-Systems license management runtime, required for UAS licensing with more than 3 managed devices.
PKCS12	File format (.p12) for storing SSL/TLS certificates and their corresponding private keys in a single encrypted container.
mDNS	Multicast DNS — network protocol used by UAS to discover PITreader devices on the local network.
Security ID	Unique hexadecimal identifier of a transponder, used for block list and permission list entries.

1.2 Notices

This document uses the following notice types to highlight important information.



INFORMATION

Supplementary information, application advice, and useful tips.



NOTICE

Important information to prevent data loss, configuration errors, or security risks. Follow these instructions carefully.

2 Overview

PIT User Authentication Service (UAS) is a service that connects PITreader devices (including PIT gatebox variants such as PIT gb RLLE) to the management of users and transponders in the software tool PIT Transponder Manager (PTM).

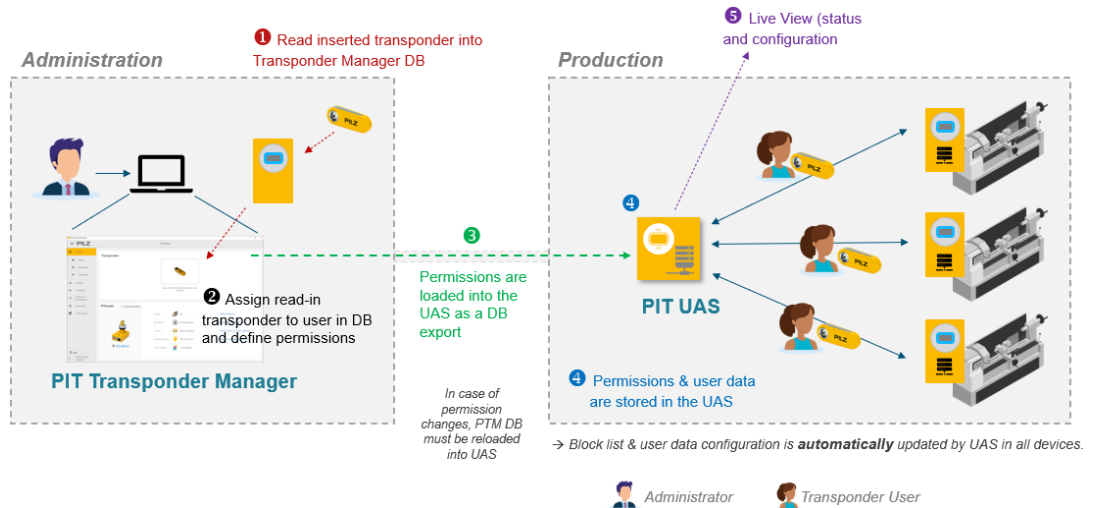


Figure 1: UAS workflow

UAS automates the repetitive tasks of updating permissions and data on transponders and distributing data to PITreader devices. This includes:

- ▶ Permissions
- ▶ Start and end dates (time limitations)
- ▶ User data and user data configuration
- ▶ Block list

2.1 System components

Component	Role
PIT Transponder Manager (PTM)	Central management of users, transponders, and permissions. Exports configuration data for UAS.
PIT User Authentication Service (UAS)	Runs as a background service. Reads PTM export data and synchronizes it to all configured PITreader devices. Provides a web interface for configuration and monitoring.
PITreader	RFID transponder reader device. Receives configuration and user data from UAS via its REST API.
Web browser	Used to access the UAS web interface for configuration and monitoring.
CodeMeter Runtime	Wibu-Systems license management. Required when managing more than 3 PITreader devices.

2.2 System Requirements

Operating system

Platform	Supported versions
Windows	Windows 10 / Windows 11, Windows Server 2016 or later
Linux	Debian-based distributions (including Raspberry Pi OS “Buster” or later)

PITreader firmware

Feature	Minimum firmware version
Basic device management	1.5.x
Permission list, external authentication, allow external override	2.0
Fingerprint verification code (PIN)	2.1.0
Network discovery (mDNS)	2.2
Firmware downgrade via UAS	2.2

Network

- ▶ TCP/IP network connection between UAS host and PITreader devices
- ▶ PITreader devices must be reachable on their configured HTTPS port (default: 443)
- ▶ The UAS web interface is available on the configured HTTP port (default: 8080) and/or HTTPS port (default: 8443)

Web browser

A modern web browser is required to access the UAS web interface (e.g. Google Chrome, Mozilla Firefox, Microsoft Edge).

Licensing

- ▶ Wibu-Systems CodeMeter Runtime is required for license management
- ▶ For dongle-based licensing: a compatible USB port and a Pilz PASkey USB dongle

3 Security

To secure plants, systems, machines, and networks against cyber threats, it is necessary to implement and continuously maintain an overall industrial security concept that is state of the art.

Perform a risk assessment in accordance with VDI/VDE 2182 or IEC 62443-3-2 and plan the security measures with care. If necessary, seek advice from Pilz Customer Support.

- ▶ [Implemented measures](#) [📖 9] — Security functions provided by UAS
- ▶ [Required measures](#) [📖 9] — Security measures that must be implemented by the operator

3.1 Implemented Security Measures

PIT User Authentication Service (UAS) provides the following security functions:

- ▶ HTTPS-secured communication between PITreader devices and UAS
- ▶ Configurable HTTPS for the web and REST interface
- ▶ Username and password authentication for the web interface



NOTICE

The default username and password must be changed immediately during commissioning.

Refer to the online help for details on configuring these security features.

3.2 Required Security Measures

The following security measures must be implemented by the operator of PIT User Authentication Service (UAS):

- ▶ Before installation, compare the installation package with the checksum on the download page to detect manipulations.
- ▶ Protect the installation directory of UAS against unauthorized access, to prevent manipulation of libraries and program code.
- ▶ The export file generated in PIT Transponder Manager contains all permissions and data assigned to transponders and users. Protect this file against unauthorized changes and manipulation.
- ▶ Follow the instructions in the PITreader user manual for secure deployment and usage of PITreader devices.
- ▶ For the web-based configuration interface of UAS:
 - Configure HTTPS for the communication between a client and the web interface. Refer to [HTTPS setup](#) [📖 20] for more information.
 - The web interface requires a username and password to prevent unauthorized access. The initial configuration provides a default username and password that must be changed immediately during commissioning.
 - Alternatively, ensure that UAS is only accessible from the local computer (default behavior) and that access to that computer is limited to authorized users. If UAS is deployed on a headless system and must be accessible over the network, deploy a firewall to limit accessibility of the web interface to authorized users.
- ▶ Protect the configuration computer that accesses UAS from attacks by a firewall or other suitable measures. Use a virus scanner on this computer and update it regularly.
- ▶ Protect the configuration computer and the system hosting UAS from unauthorized use by assigning passwords and taking further measures if required. The user logged on to the configuration computer should not have administrator rights.
- ▶ Ensure that the product is separated by a router (layer 3 switch or firewall) from the company network.

- ▶ Assign only safe passwords. When assigning passwords, observe the following:
 - The password should have at least 12 characters.
 - The password should contain upper- and lower-case characters, as well as special characters and numbers.
 - The password should not be available in dictionaries.
 - The password should not be made up of standard variants, repetitions, or keyboard patterns (e.g. not 1234abcd).
 - Use a password manager for management of complex passwords.
 - Change passwords of user accounts on the system regularly and instruct users to change their passwords.
 - Make users aware of the responsible use of their login credentials.
- ▶ Install firmware or software updates that Pilz provides for the product as soon as possible.
- ▶ Log data may contain personal data. Only store exported logs on a storage medium that is adequately protected.

3.2.1 Network topology examples

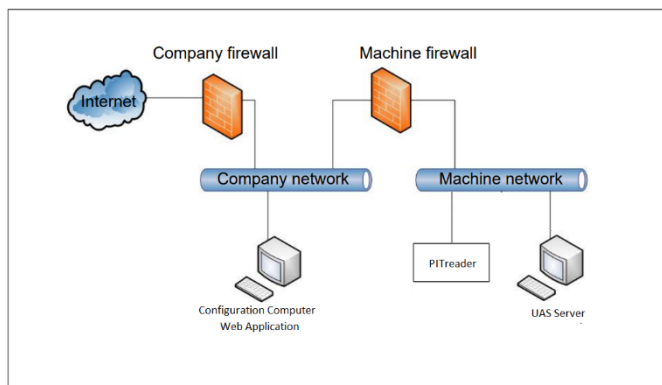


Figure 2: Example 1: UAS inside the firewall

Fig.: Example 1 — UAS located inside the firewall, on the same network as the PITreader devices.

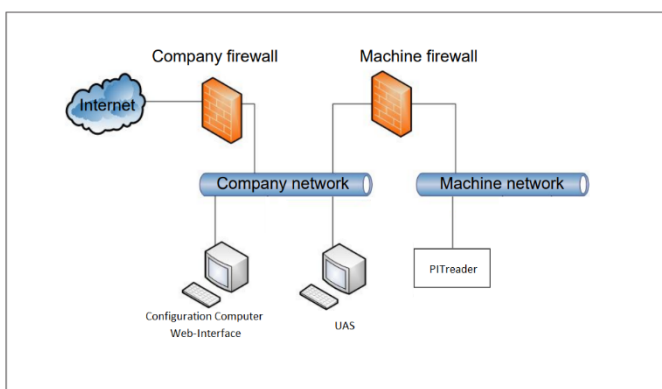


Figure 3: Example 2: UAS outside the firewall

Fig.: Example 2 — UAS located outside the firewall, separated from the PITreader devices.

Fig.: UAS network interfaces and connections.

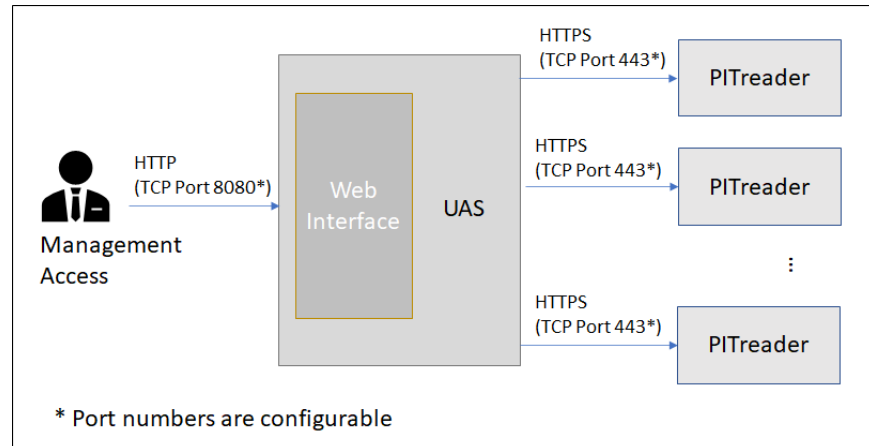


Figure 4: UAS network interfaces and connections

4 Installation

PIT User Authentication Service (UAS) is available for Windows and Linux platforms. Choose the installation method that matches your target system.



NOTICE

Before installation, compare the installation package with the checksum published on the download page to detect potential manipulations.



INFORMATION

Existing configuration data is preserved during an update installation. However, it is recommended to create a backup of the database before upgrading.

- ▶ [Windows \[12\]](#) — Windows Installer, silent installation, Windows service
- ▶ [Linux \[14\]](#) — tar.gz extraction, systemd service, Revolution Pi, CodeMeter
- ▶ [Java Runtime \[16\]](#) — Replace the bundled JRE (Linux only)

4.1 Windows Installation

4.1.1 Windows Installer

Windows users can install PIT User Authentication Service (UAS) via the provided installer. The installer automatically detects previous installations and performs an update.

Existing configuration data is preserved during an update installation. However, it is recommended to create a backup of the database before upgrading.



INFORMATION

Starting with version 1.5.0 of UAS, the installer will set special file system permissions on the default configuration data directory (located in %ProgramData%) that only permit access to the members of the local administrator group, the local service user and the operating system. All other users will not be able to access this directory unless corresponding permissions are manually granted by an admin user. During an upgrade installation from a previous version these new permissions will also be applied to an existing data directory. After the permissions were initially changed by the installer, they will not be changed during subsequent update installations, to allow permanent custom modifications if required.

4.1.2 Installer command line options

▶ Silent installation

To install UAS silently, add `/silent` to the command line:

```
PIT-UAS-Setup.exe /silent
```

▶ Disable option to install as Windows service

The installer lets the user select if UAS shall be installed as Windows service. This option can be disabled in the installer by adding `/nosvcinst` to the command line.

```
PIT-UAS-Setup.exe /nosvcinst
```

4.1.3 Run as Windows service

During installation, UAS is registered as a Windows service unless you disable the corresponding option.

The Windows installation provides a control panel that allows installing/uninstalling UAS as a Windows service, and starting/stopping UAS manually. A link to the control panel is added to the Windows Start menu by the installer. Alternatively, start `uas.exe` from the `services` folder in the installation directory.

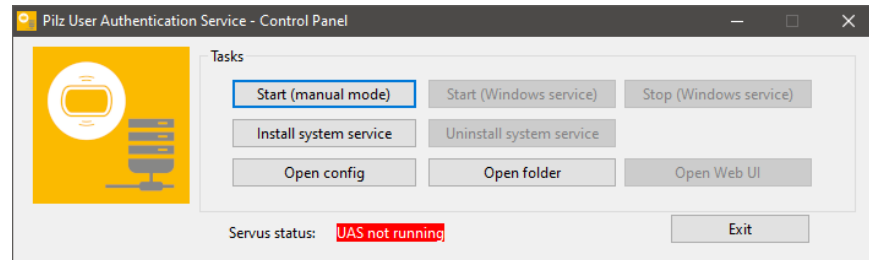


Figure 5: UAS Windows control panel

To register UAS as a Windows service after installation, use the corresponding control panel function or run `service install` from the UAS installation directory.

4.1.4 Service control

You can start and stop the service via the control panel or through the **Services** section of the Windows Computer Management console.

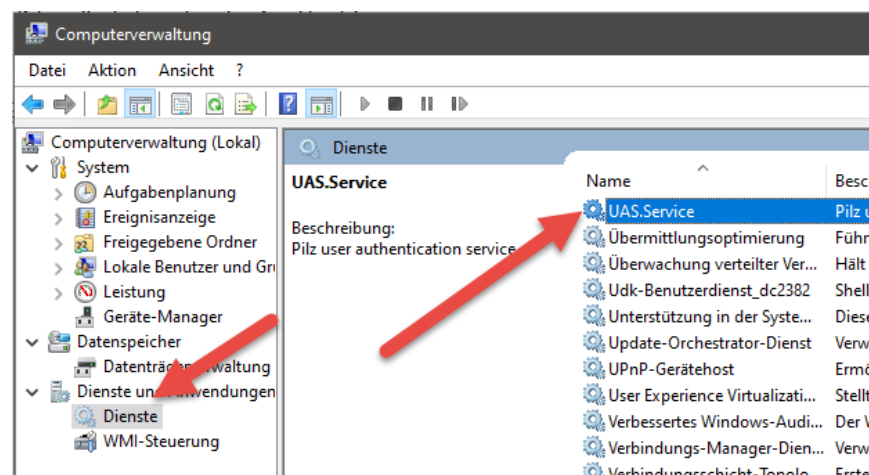


Figure 6: UAS in Windows Services

Alternatively, use the service command line tool located in the UAS installation directory:

Command	Description
<code>service start</code>	Starts the UAS service.
<code>service stop</code>	Stops the UAS service.
<code>service install</code>	Installs UAS as a Windows service.
<code>service uninstall</code>	Removes UAS from Windows services.

Operation modes Depending on the local permissions of the user who starts the service control panel, available functionality is slightly different.

If a user who is **member of the local administrator group** starts the control panel

- ▶ all functions are available
- ▶ the `%ProgramData%` directory is used for searching the configuration file

If a user who is **not** member of the local administrator group starts the control panel

- ▶ all functions related to the control of Windows services are disabled
- ▶ the `%LocalAppData%` directory is used for searching the configuration file
- ▶ if the configuration directory in `%LocalAppData%` does not exist, it will be created and initialized with default settings

Refer to section [configuration file location](#) [19] for additional information.

4.1.5 Run in manual mode

UAS can also run without being registered as a Windows service. To start UAS in manual mode, use the UAS control panel or execute `UAS.Service.cmd` from the UAS installation directory.

To stop UAS in manual mode, press [Enter] or [Ctrl+C] in the corresponding console window.

4.2 Linux Installation

4.2.1 Extract the tar.gz archive

To extract the tar.gz file, enter:

```
$ tar -xvf PIT-UAS-linux-x.y.z.tar.gz -C /home/username/
```

A directory `/home/username/PIT-UAS-linux-x.y.z` will be created. Replace `username` with your actual username or extract the service to a different folder.

4.2.2 Run as Linux service (daemon)

PIT User Authentication Service (UAS) can run as a Linux background service integrated into systemd. You need root privileges to install, uninstall, and control the service.

To install UAS as a service, run the following command with root access:

```
$ sudo /home/username/PIT-UAS-linux-x.y.z/setup_service.sh
↪ --install
```

After the installation process is complete, the service starts automatically as `uas`. The directory `/home/username/PIT-UAS-linux-x.y.z` can now be safely removed.

Existing configuration data is preserved during an update installation. However, it is recommended to create a backup of the database before upgrading.

Service installation directories and files

Directory / File	Description
<code>/opt/Pilz/</code> <code>PITUserAuthenticationService</code>	Installation directory of the service
<code>/etc/Pilz/</code> <code>PITUserAuthenticationService/</code> <code>service.config</code>	Service configuration file
<code>/etc/systemd/system/uas.service</code>	Unit file for systemd
<code>/var/opt/Pilz/</code> <code>PITUserAuthenticationService/lib</code>	Path to the database file

Directory / File	Description
/var/log/Pilz/ PITUserAuthenticationService	Log files

4.2.3 Service control

The service can be controlled using standard systemd tools:

Command	Description
\$ sudo systemctl start uas.service	Starts the UAS service.
\$ sudo systemctl stop uas.service	Stops the UAS service.
\$ sudo systemctl status uas.service	Displays the status of the UAS service.
\$ sudo systemctl enable uas.service	Enables the UAS service to start during boot.
\$ sudo systemctl disable uas.service	Disables the UAS service from starting during boot.
\$ sudo journalctl -u uas.service	Displays system messages for the UAS service.

To remove the service, run:

```
$ sudo
↪ /opt/Pilz/PITUserAuthenticationService/bin/setup_service.sh
↪ --uninstall
```

4.2.4 Revolution Pi firmware version

The Revolution Pi firmware version must be at least “buster” or higher.

See <https://revolutionpi.com/de/support/downloads> for firmware downloads.

4.2.5 Run in manual mode

If a UAS service is already running, it must first be stopped.

1. You can start the UAS service from console by executing (for debugging purposes):

```
$ sudo -u uas
↪ /opt/Pilz/PITUserAuthenticationService/lib/jre/bin/java
↪ -Xmx1G -jar
↪ /opt/Pilz/PITUserAuthenticationService/lib/UAS.Main.jar
```

2. Alternatively, UAS can be started without being registered as a service by executing `UAS.Service.sh` from the installation directory (quick test).

To stop UAS in manual mode, press [Enter] or [Ctrl+C] in the corresponding console window.

4.2.6 Wibu CodeMeter

When installing UAS as a service, Wibu CodeMeter is also installed if it is not already present. CodeMeter is not uninstalled when uninstalling the UAS service — it must be removed manually.



INFORMATION

To access the CodeMeter WebAdmin remotely, set `RemoteRead` to 2 in the file `/etc/wibu/CodeMeter/Server.ini`.



NOTICE

Deactivate the license before uninstalling the service. Otherwise, the license will be lost. See [Uninstall \[22\]](#) for details.

4.3 Replace the Java Runtime

PIT User Authentication Service (UAS) is delivered with its own Java Runtime Environment (JRE). In some cases it may be necessary to replace it, for example:

- ▶ The delivered JRE does not match your system architecture.
- ▶ You need to update the JRE for security or compatibility reasons.

The replacement procedure depends on whether UAS runs as a daemon or in manual mode.

4.3.1 Daemon mode

When UAS runs as a systemd service, choose one of the following three methods.

Method 1: Symbolic link

1. Stop the daemon:

```
$ sudo systemctl stop uas.service
```

2. Remove the existing JRE directory:

```
$ sudo rm -rf /opt/Pilz/PITUserAuthenticationService/lib/jre
```

3. Install the new JRE to any directory, e.g. `/opt/jdk-17.0.14+7-jre`.

4. Create a symbolic link from the UAS JRE path to the new JRE:

```
$ cd /opt/Pilz/PITUserAuthenticationService/
$ sudo ln -s /opt/jdk-17.0.14+7-jre lib/jre
```

5. Start the daemon:

```
$ sudo systemctl start uas.service
```



INFORMATION

When you uninstall the daemon, only the symbolic link is deleted, not the JRE files behind it.

Method 2: Modify the service file

1. Stop the daemon:

```
$ sudo systemctl stop uas.service
```

2. Install the new JRE to any directory, e.g. /opt/jdk-17.0.14+7-jre.

3. Edit the systemd unit file:

```
$ sudo vi /etc/systemd/system/uas.service
```

4. Change the JAVA_HOME line to point to the new JRE:

```
Environment="JAVA_HOME=/opt/jdk-17.0.14+7-jre"
```

5. Reload the systemd configuration and start the daemon:

```
$ sudo systemctl daemon-reload
$ sudo systemctl start uas.service
```

**INFORMATION**

Changes to the service file are lost when you uninstall the daemon with `./setup_service.sh --uninstall --clean`.

Method 3: Replace files in the JRE directory

1. Stop the daemon:

```
$ sudo systemctl stop uas.service
```

2. Install the new JRE to any directory, e.g. /opt/jdk-17.0.14+7-jre.

3. Delete the contents of the existing JRE directory:

```
$ cd /opt/Pilz/PITUserAuthenticationService
$ sudo rm -rf lib/jre/legal lib/jre/bin lib/jre/release
↪ lib/jre/conf lib/jre/NOTICE lib/jre/lib
```

4. Copy the new JRE files into the directory and set ownership:

```
$ cd /opt/Pilz/PITUserAuthenticationService
$ sudo cp -r /opt/jdk-17.0.14+7-jre/* lib/jre
$ sudo chown root:uas -R lib/jre
```

5. Start the daemon:

```
$ sudo systemctl start uas.service
```

**INFORMATION**

The replaced files are lost when you uninstall the daemon with `./setup_service.sh --uninstall --clean`.

4.3.2 Manual mode

When UAS runs in manual mode (not as a daemon), choose one of the following three methods. All commands are executed from the UAS installation directory.

Method 1: Symbolic link

1. Remove the existing JRE directory:

```
$ sudo rm -rf jre
```

2. Install the new JRE to any directory, e.g. /opt/jdk-17.0.14+7-jre.
3. Create a symbolic link:

```
$ sudo ln -s /opt/jdk-17.0.14+7-jre jre
```

4. Start UAS:

```
$ ./UAS.Service.sh
```

Method 2: Set JAVA_HOME

1. Remove the existing JRE directory:

```
$ sudo rm -rf jre
```

2. Install the new JRE to any directory, e.g. /opt/jdk-17.0.14+7-jre.
3. Set the JAVA_HOME environment variable and start UAS:

```
$ export JAVA_HOME=/opt/jdk-17.0.14+7-jre  
$ ./UAS.Service.sh
```

Method 3: Replace files in the JRE directory

1. Install the new JRE to any directory, e.g. /opt/jdk-17.0.14+7-jre.
2. Delete the contents of the existing JRE directory and copy the new files:

```
$ cd jre  
$ sudo rm -rf *  
$ cp -r /opt/jdk-17.0.14+7-jre/* .
```

3. Start UAS:

```
$ ./UAS.Service.sh
```

5 Configuration

PIT User Authentication Service (UAS) uses two layers of configuration:

1. **Configuration file** (`service.config`) — Contains basic settings that must be defined before UAS starts, such as web server address and HTTPS settings.
2. **Web interface** — Provides runtime configuration and monitoring after UAS is running.

This section covers the initial configuration file settings required to start UAS. For all other configuration options, refer to the online help accessible through the UAS web interface after installation.

- ▶ [Basic settings](#) [19] — Configuration file location and format
- ▶ [HTTPS setup](#) [20] — Enable HTTPS for the web interface
- ▶ [Web interface](#) [20] — Default URL and credentials

5.1 Basic Settings

While most of the configuration can be done via the integrated web interface, some settings must be provided **before UAS starts**. These settings are stored in a configuration file.

5.1.1 Configuration file location

The configuration file to use is determined in the following order:

1. **Command line parameter** — specify with `-cfg` or `--configFile`
2. **Default location** (see below)
3. **Current working directory**
4. **UAS application path**

Default location — Windows:

```
%ProgramData%\Pilz\PITUserAuthenticationService\service.config
```

When UAS is started via the [service control panel](#) [13] as **non-admin user** in manual mode, a data directory in the current user profile folder is created and used:

```
%LocalAppData%\Pilz\PITUserAuthenticationService\service.config
```



INFORMATION

`%ProgramData%` and `%LocalAppData%` are Windows environment variables. See [Windows environment variables](#) [25] for more information.

Default location — Linux:

```
/etc/Pilz/PITUserAuthenticationService/service.config
```

5.1.2 Configuration file format

Each line of the file represents a key/value combination in the format `key=value`. Lines with a leading `#` are treated as comments. Empty lines are ignored.

Example:

```
## Config file for UAS
dbtype=SQLITE
webserver.ip=192.168.0.1
webserver.port=8080
```

**NOTICE**

Do not change any settings in this file other than those described in the online help, as this may prevent UAS from working as expected.

The default configuration works for most installations. Refer to the online help for a complete list of all configuration parameters, including database location, log directory, web server IP/port, HTTPS, audit logs, and time synchronisation settings.

5.2 HTTPS Setup

Encrypted HTTPS communication based on SSL/TLS certificates is available for the PIT User Authentication Service (UAS) web server. To enable HTTPS, set the following parameters in the configuration file:

- ▶ `webserver.https_enabled` — set to `true`
- ▶ `webserver.https_port` — HTTPS port (default: 8443)
- ▶ `webserver.https_redirect` — redirect HTTP to HTTPS (default: `true`)
- ▶ `webserver.ssl.key-store` — path to the PKCS12 key-store file
- ▶ `webserver.ssl.key-store-password` — key-store password
- ▶ `webserver.ssl.key-store-keyAlias` — certificate alias in the key-store

The certificate and private key must be stored in a PKCS12 container file (.p12). Refer to the online help for instructions on creating or importing SSL certificates.

**NOTICE**

Protect the PKCS12 key-store file with a strong password and prevent access to both the key-store and the configuration file (which contains the password) by unauthorized users.

5.3 Web Interface

PIT User Authentication Service (UAS) provides a web interface for configuration and monitoring. By default, it is available at:

`http://localhost:8080`

The default username is `admin`, the default password is `pilz`.

**NOTICE**

Change the default password immediately after the first login.

Refer to the online help within the web interface for all configuration and operational functions.

6 Getting Started

This checklist guides you through the initial setup of PIT User Authentication Service after installation.

6.1 First-time setup checklist

1. **Configure the service configuration file** Edit the `service.config` file to set the database path and other basic parameters if the defaults do not suit your environment. See Configuration for details.
2. **Register and start the service** Register UAS as a system service and start it. See Windows Installation or Linux Installation for platform-specific instructions.
3. **Change the default password** Open the UAS web interface in your browser (default: `http://localhost:8080`). Log in with the default credentials (`admin / pilz`) and change the password immediately.
4. **Configure HTTPS (recommended)** Set up SSL/TLS for the web interface to secure communication. See HTTPS Setup for the required parameters and the online help for SSL certificate instructions.
5. **Configure PITreader devices** Set the required authentication mode and device group on each PITreader device via its own web interface. Refer to the online help for the required settings.
6. **Import PTM data** Export the PTM data from PIT Transponder Manager and upload it via the UAS web interface, or register a MYZEL connection to synchronise data automatically. Refer to the online help for details.
7. **Add PITreader devices to UAS** Use the web interface to register your PITreader devices with UAS. Refer to the online help for the step-by-step wizard.
8. **Activate your license (if more than 3 devices)** If you manage more than 3 PITreader devices, activate a license. Refer to the online help for activation options.

After completing these steps, UAS will automatically synchronise PTM data with all connected PITreader devices.

7 Uninstall PIT User Authentication Service

Preparation



NOTICE

If you have installed a file-based license for PIT User Authentication Service (UAS), transfer this license back to the license depot **before** uninstalling UAS and/or the CodeMeter Runtime. This ensures that the license information stored on your platform is not lost, which would make it impossible to return or reuse the license on another device.

Refer to the corresponding licensing sections in the online help of the web interface, or to the CodeMeter help provided with the CodeMeter Runtime installation, for information on how to return a license.

Next steps

- ▶ [Uninstall on Windows](#) [📖 22]
- ▶ [Uninstall on Linux](#) [📖 22]
- ▶ [Manual cleanup of remaining files](#) [📖 23]

7.1 Uninstall on Windows

7.1.1 Windows Installer / Windows service

If you used the UAS Installer for Windows, open **Programs and Features** from the Windows Control Panel.

In the list of installed software, select **PIT User Authentication Service** and click the uninstall button. The uninstaller will remove the UAS Windows service and delete the files from the installation directory.

The uninstall routine does not remove the configuration file, database, or additionally generated files such as log files. See [Manual cleanup](#) [📖 23] for instructions on how to remove additional data that may have been stored in different locations.

7.1.2 Uninstall CodeMeter Runtime



NOTICE

Read the preparation notes in [Uninstall](#) [📖 22] before uninstalling CodeMeter Runtime.

You can uninstall the CodeMeter Runtime if no other software on the system requires it. Select **CodeMeter Runtime Kit** in the program list and click the uninstall button.

7.2 Uninstall on Linux

7.2.1 Linux daemon

To uninstall the UAS daemon, run the following command from the UAS directory:

```
$ ./setup_service.sh --uninstall
```

This removes the UAS daemon from the system and deletes the UAS files.

To also delete the UAS configuration file and database file, add the `--clean` parameter:

```
$ ./setup_service.sh --uninstall --clean
```


See [Manual cleanup](#) [📖 23] for instructions on how to remove additional data that may have been stored in different locations.

7.2.2 Uninstall CodeMeter Runtime



NOTICE

Read the preparation notes in [Uninstall](#) [📖 22] before uninstalling CodeMeter Runtime.

You can uninstall the CodeMeter Runtime if no other software on the system requires it.

Linux x86 / x86-64:

```
$ sudo dpkg --remove codemeter
$ sudo dpkg --purge codemeter      # also deletes CodeMeter
↪ configuration
```

Linux ARM64 / armhf (Revolution Pi):

```
$ sudo dpkg --remove codemeter-lite
$ sudo dpkg --purge codemeter-lite  # also deletes CodeMeter
↪ configuration
```

7.3 Manual Cleanup

After removing the UAS installation by following one of the platform-specific methods, some additional files may still reside on the system. Delete these files manually if required.

7.3.1 Remaining files

- ▶ **Configuration file** — See [Configuration file location](#) [📖 19] for possible locations of this file.
- ▶ **UAS database file** — Location defined by the `sqlite.path` configuration parameter.
- ▶ **Log files** — Location defined by the `log.dir` configuration parameter.
- ▶ **SSL key-store file** — Location defined by the `webserver.ssl.key-store` configuration parameter.
- ▶ **Cloud connection registration files** - Location defined by the `myzel.mqtt.path` configuration parameter.

Refer to [Basic settings](#) [📖 19] for details on these configuration parameters and their default values.

7.3.2 ZIP / tar.gz archive

If you did not use the Windows Installer or the service installation script for Linux, but only unpacked a UAS archive to a directory, simply delete the folder that contains the unpacked files.

8 License Information

Source code from third-party manufacturers or open source software has been used for some components of PIT User Authentication Service (UAS). The relevant license information can be found in the menu under “About PIT User Authentication Service” in the web interface.

The relevant LGPL source codes can be requested via opensource@pilz.de.

Your request should include the following:

1. The software name
2. The software version
3. Your name
4. Your company name (if applicable)
5. Your postal address
6. Your email address (if possible)

Pilz may charge a fee for the data medium and for sending.

The request for the source code must be received no later than 3 years after the receipt of the relevant GPL or LGPL licensed software. Irrespective of this period, Pilz will provide a complete, machine-readable copy of the source code as long as Pilz offers spare parts or technical support for this product.

Pilz permits the purchaser of this product to edit proprietary components from Pilz that are linked to open source components under the LGPL. Further, Pilz permits reverse engineering for debugging of the edited proprietary components. The results of reverse engineering must not be disclosed to any third party and the edited software must not be distributed to any third party.

9 Appendix

9.1 Windows Environment Variables

Windows environment variables are data values that are accessible by their name across application processes. When used in path references, the name of the variable must be enclosed in % characters to distinguish it from literal text.

Environment variables provide information that is referenced by a common name but varies from system to system or user to user. For example, the system drive and installation folder of the current Windows operating system is accessible via the variable %SYSTEMROOT%.

Using it in a path reference like %SYSTEMROOT%\Pilz\Sys would resolve to C:\Windows\Pilz\Sys on a typical Windows installation.

► %ProgramData%

%ProgramData% usually refers to the ProgramData subfolder on your Windows installation drive (e.g. C:\ProgramData).

It is intended to store data that is accessible for all users of a system.

► %LocalAppData%

%LocalAppData% refers to the AppData\Local subfolder in the current user profile directory (%UserProfile%; e.g. C:\Users\j.doe\AppData\Local).

It is intended to store application data that is only accessible for the respective user.



INFORMATION

In the default configuration, folders like ProgramData or AppData are hidden in Windows Explorer. To see them in the directory listing, enable the option to display hidden items in the Windows Explorer **View** menu. Alternatively, enter the environment variable (e.g. %ProgramData%) or the full path (e.g. %ProgramData%\Pilz\PITUserAuthenticationService) in the Explorer address bar and press Enter. This navigates directly to the corresponding directory without changing the display settings.

9.2 Windows Firewall Settings for Network Scan

During installation of the Windows version, the firewall rule “UAS Service” is created for mDNS queries used to detect PITreader devices on the network. This rule is removed during uninstallation of the software.

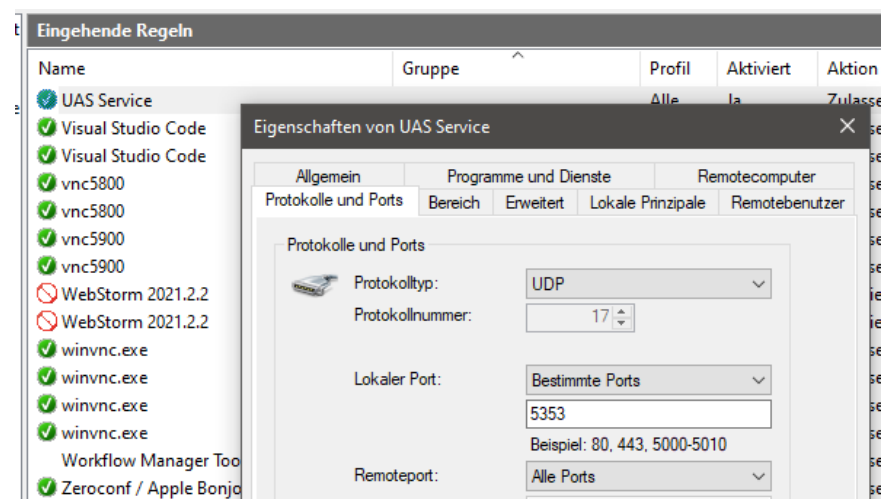


Figure 7: Windows firewall rule for UAS mDNS network scan

10 Changelog

10.1 Version 1.5.0

- Connection to MYZEL Lifecycle Platform (receiving PTM file updates)
- UAS Control Panel: Differentiation between admin and non-admin users
- Windows Installer: Limit permissions of default configuration data directory
- Restructured and improved online help
- Updated included software components
- Minor fixes and improvements
- Security-related component updates based on CVE program:
 - CVE-2025-15595 (Privilege escalation via DLL hijacking in Inno Setup v6.2.1 and earlier versions)
 - CVE-2026-22732 (Missing security headers vulnerability in spring-security-web v6.5.5)
 - CVE-2026-24880 (HTTP request/response smuggling vulnerability in tomcat-embed-core v11.0.14)

10.2 Version 1.4.1

- Fixed issue when importing PTM files from the cloud.
- Security-related component updates based on CVE program:
 - CVE-2024-12798 (RCE injection vulnerability in logback-core 1.5.6)
 - CVE-2025-55754 (Console manipulation vulnerability in tomcat-embed-core v10.1.39)
 - CVE-2025-12383 (MITM vulnerability in jersey-client v3.1.9)
 - CVE-2025-61795 (DoS vulnerability in tomcat-embed-core v10.1.39)
 - CVE-2025-31650 (DoS vulnerability in tomcat-embed-core v10.1.39)
 - CVE-2025-48988 (DoS vulnerability in tomcat-embed-core v10.1.39)

10.3 Version 1.4.0

- Upload firmware file for PITreader firmware update to UAS
- Upload and apply new firmware to PITreader devices managed by UAS
- Added export functionality for audit trail
- Improved compatibility when importing configuration data
- Switched to 64-bit JRE on Revolution Pi
- Updated included software components
- Minor fixes and improvements
- Security-related component updates based on CVE program:
 - CVE-2024-12798 (ACE vulnerability in logback-core 1.5.6)
 - CVE-2024-12801 (SSRF vulnerability in logback-core 1.5.6)
 - CVE-2024-57965 (Origin validation error vulnerability in axios 1.6.7)
 - CVE-2025-27152 (SSRF/credential leakage vulnerability in axios 1.6.7)
 - CVE-2025-27789 (ReDoS vulnerability in babel 7.23.9)

10.4 Version 1.3.0

- UAS can synchronize the real-time clock (RTC) between PITreader and PC
- UAS is compatible with PIT Transponder Manager export from the cloud
- Collect audit trail log data from all connected PITreader devices and display as summarized list in the web interface; data is stored persistently
- Upgraded included CodeMeter Runtime to version 8.00
- Updated all included software libraries and JREs
- Minor fixes and improvements

10.5 Version 1.2.0

- Scan network for PITreader devices (requires PITreader firmware version $\geq 2.0.0$)
- Fixed PIT Transponder Manager data import issues
- New wizard for adding PITreader devices to UAS
- Added support for fingerprint verification code when adding or editing a device (requires PITreader firmware version $\geq 2.1.0$)
- Add or edit devices using username and password to read the API token of an existing UAS user from PITreader, or create a UAS user on the PITreader (requires PITreader firmware version $\geq 2.0.0$)
- Updated all included software libraries
- Minor fixes and improvements

10.6 Version 1.1.2

- Upgraded included CodeMeter Runtime to version 7.60c
- Fixed bugs in Windows Installer

10.7 Version 1.1.1

- Support for PITreader firmware versions $\geq 2.1.0$
- Minor fixes and improvements

10.8 Version 1.1.0

- UAS licensing (support for more than 3 managed devices)
- Support for PITreader synchronization status surveillance (permissions and block list)
- Minor fixes and improvements

10.9 Version 1.0.0

- Initial release

