PM-LOGON
Manual

www.siemens.com

SIEMENS

SIEMENS

Table of contents

SIEMENS

1 Introduction

1.1 Description

By using PM-LOGON, users from an active directory can login into e.g. SIMATIC Logon with an RFID card. The PM-LOGON Configurator application is used to associate active directory accounts to RFID-cards. To setup this association the unique id of the RFID card and the password of the user that is to be used for the login are stored in encrypted format within the user management. The PM-LOGON Runtime application then retrieves the associated user and password by using the unique id of the card presented to the reading device and uses these credentials to perform the login operation into SIMATIC Logon, the WinCC Web Navigator Client application or the TIA Runtime Advanced.

1.2 Licensing

Each installation of the PM-LOGON Configurator requires a separate license. The number of licensed users that can login via RFID card is independently defined from the PM-LOGON Configurator license by so called User Packages. Existing Client Packages already purchased with PM-LOGON V1.x can still be used with PM-LOGON V2.
The PM-LOGON Runtime can be operated on any number of suitable devices without a separate license.
Furthermore, a license is required for each instance of PM-LOGON Server.

2 Installation

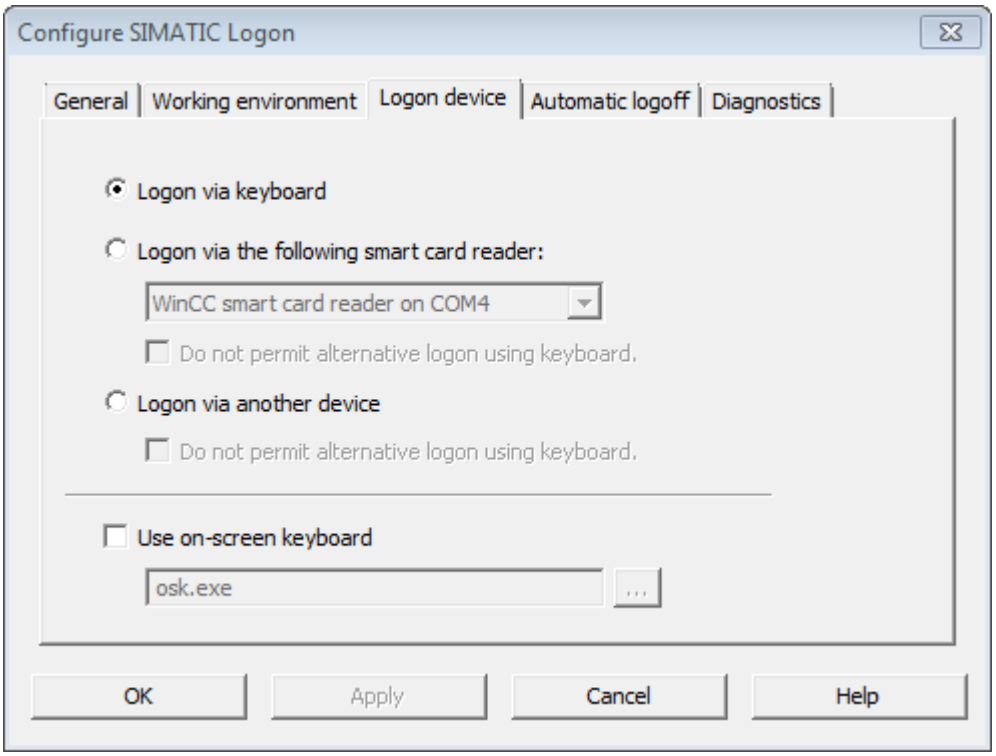
2.1 Installation prerequisites

SIMATIC Logon 1.5/1.6
SIMATIC RF1040R/RF1060R/RF1070R or
Admitto card reader (USB) in the operation mode “active send” or
OmniKey USB Smart Card Reader (e.g. OMNIKEY 5021 CL)
Teratron PC-Loc Reader
Euchner EKS USB Reader
Windows 7 32/64 bit SP1 or later or Windows Server 2008 32/64 bit or later

Please also note the current product information from PM-LOGON.

2.2 Configuration of SIMATIC LOGON

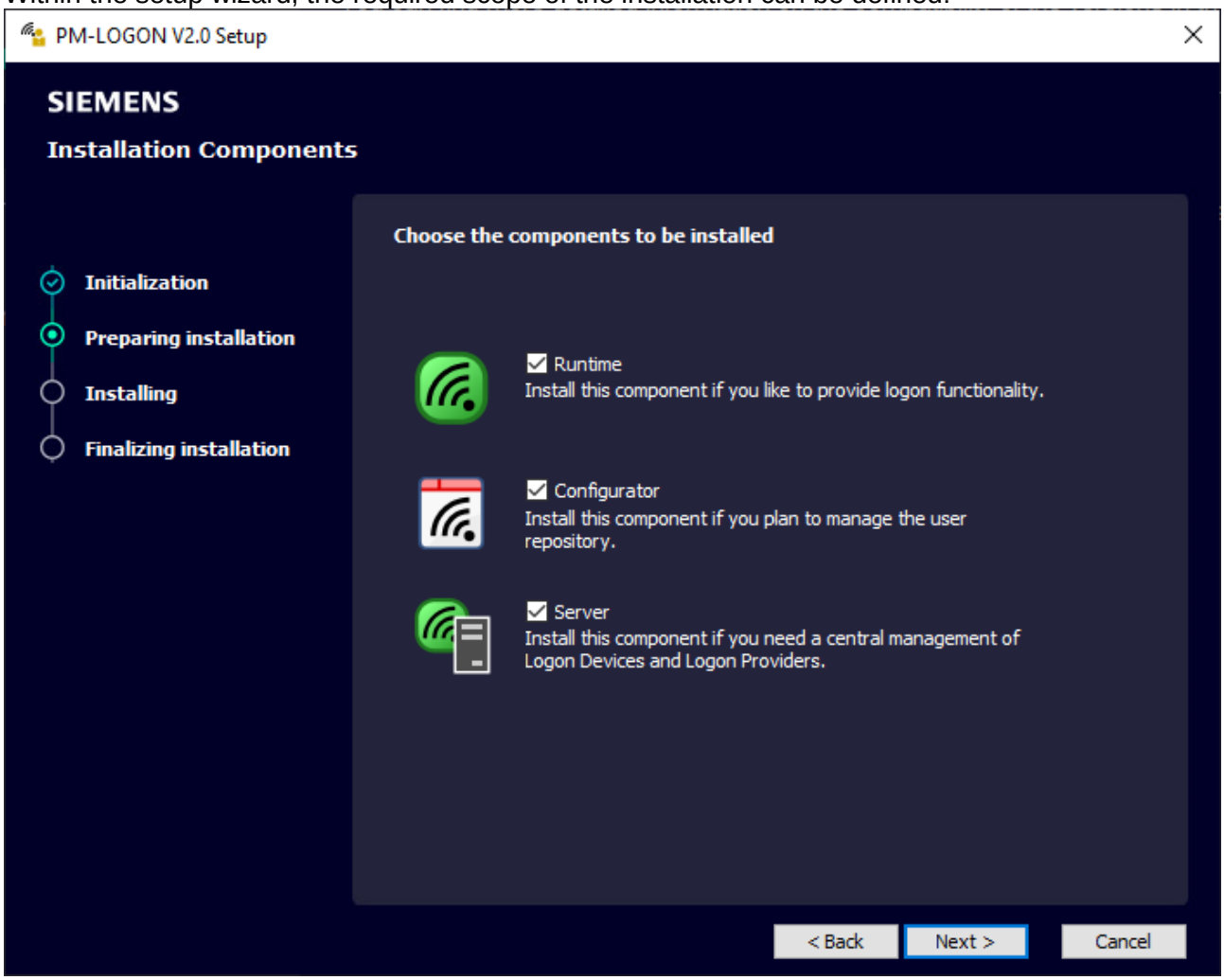
Please make sure, that in SIMATIC LOGON configuration "Logon via keyboard" is set as logon device.



2.3 Installation

The setup application “PM-LOGON Setup.exe” is located on the installation media in the folder “V2”:

Within the setup wizard, the required scope of the installation can be defined:



Runtime installs the PM-LOGON Runtime – This is the application that is required for the login process. Furthermore, the runtime can be used as a relaying gateway for providing login credentials over its integrated web service for other runtimes, running on remote comfort panels.

Configurator installs the application PM-LOGON Configurator, which organizes the association of operator logins and the corresponding RFID cards.

Server installs PM-LOGON Server.

2.4 PMSecurityService

During the installation of PM-LOGON the service "PMSecurityService" is also installed. During the installation of the service, a user named "PMSecurityService" is automatically installed and assigned to the service as the execution account. The user is created with a randomly generated password and associated to the local administrators group.
If the machine is a member of a domain, the group policies may need to be adjusted so that the "PMSecurityService" user remains in the local administrators group.

Important notice:
A change of the service execution account of the PMSecurityService or a change of the password of the execution account may cause that the data stored in the user repository can no longer be read!

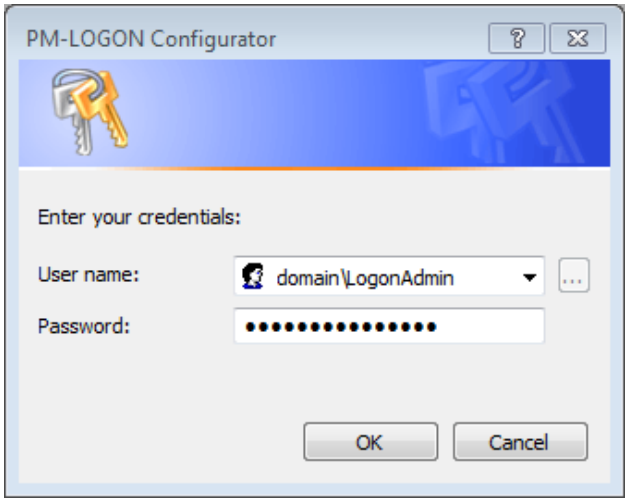
3 PM-LOGON Configurator

3.1 Introduction

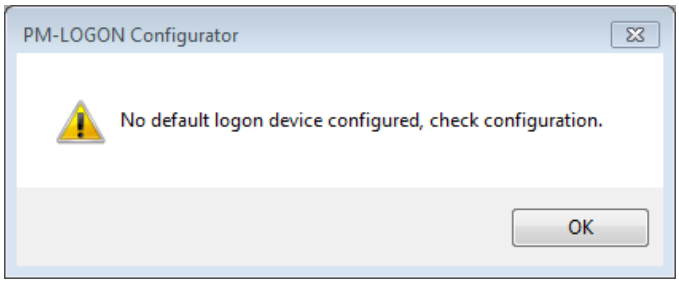
The PM-LOGON Configurator application is used to associate active directory users to RFID-cards. The user accounts must be already present in the active directory. Each installation of the Configurator requires a separate license. If the PM-LOGON Configurator is used without a valid license it switches into a test mode where it allows associating only one user account to an RFID card in order to test the compatibility of readers, cards, login method etc.

3.2 Configuration

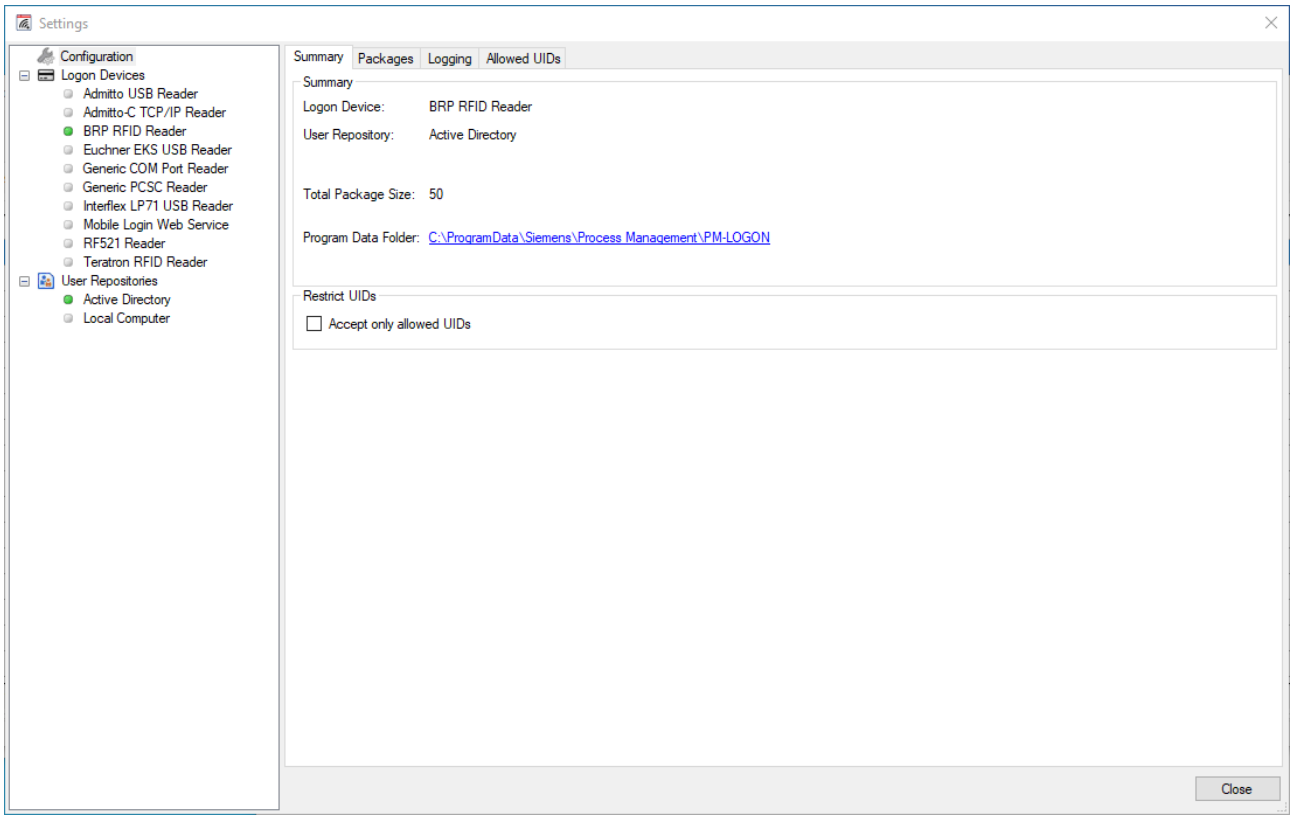
You can start the application PM-LOGON Configurator with the corresponding link that has been created from the setup process in the start menu. After launching the application you will be asked to login. For this login any user that is either locally or within the domain defined as a member of the “Logon_Administrator” group may be used. When a domain account is used, the name of the domain user needs to be prefixed with the domain name (“<domain>\<user>").The most recent user that has been logged in is stored as a default and is used to pre-fill the user name when the application is started the next time.



When started for the first time, a warning message will be displayed that no login device has been configured yet.



Open the configuration of PM-LOGON Configurator by using the menu item File->Configuration. The settings dialog of PM-LOGON Configurator will be displayed.



The tree view on the left side allows you to navigate over the different configuration sections.

The element labeled “Configuration” opens the general configuration settings of PM-LOGON Configurator.

The summary page displays the logon device and the user repository that is currently being used by PM-LOGON Configurator.

The link allows you to navigate to the path in the file system where the configuration data is stored.

The page with the title “Packages” allows you to manage the User Packages that define the number of users that can log in via an RFID card.

The “Logging” page allows you to activate the writing of diagnostic trace information into log files if needed.

The "Allowed UIDs" page allows you to maintain the list of allowed UIDs for the Configurator. This list determines the UIDs, that are allowed to be assigned to a user within the Configurator.

The element “Logon Devices” navigates to an overview of all currently supported login devices. Underneath this element the configuration sections for the individual login devices are located.

The element “User Repositories” navigates to the configuration section for the supported user management systems. Underneath this element the configuration sections for the individual user management repositories are located.

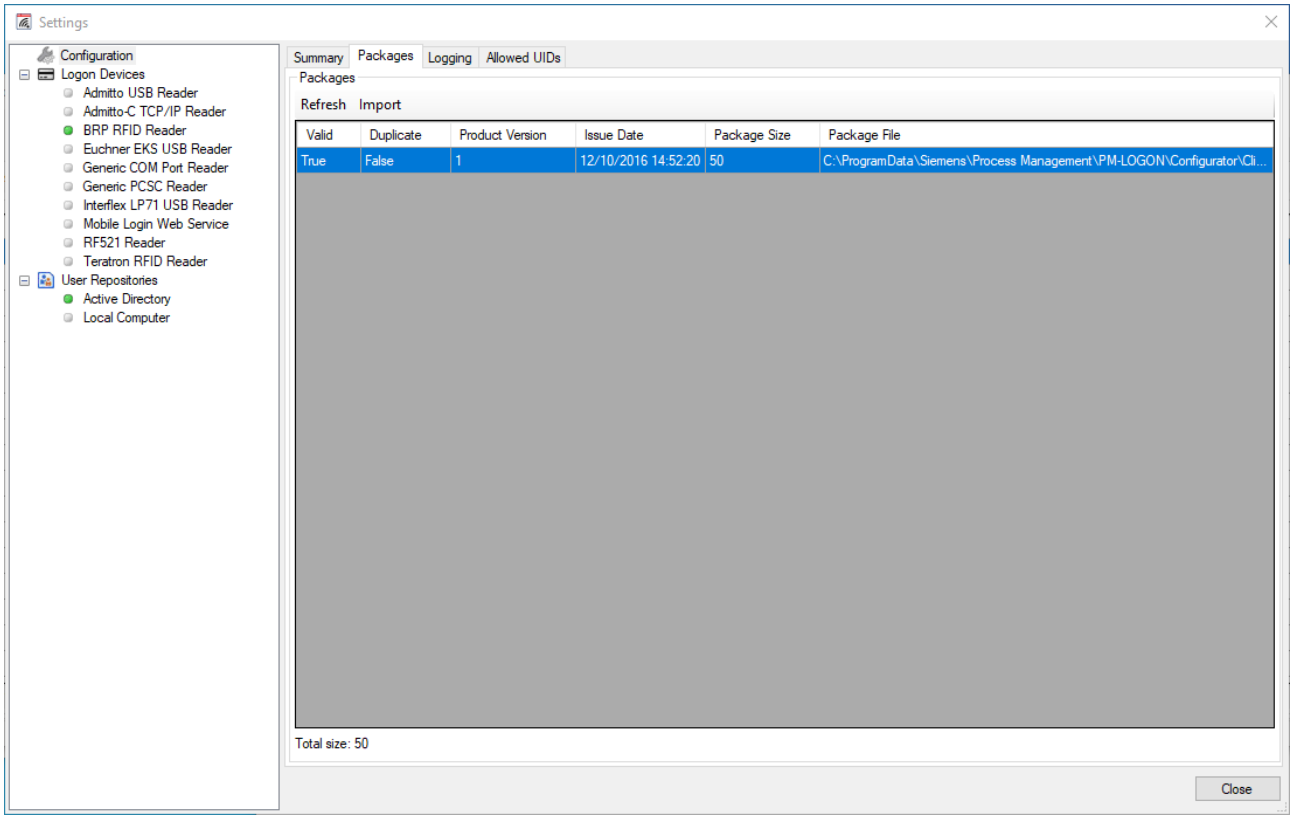
PM-LOGON has a plug-in concept that allows the system to be expanded in order to support additional reading devices and user repositories.

3.2.1 Import of User Packages

The licensed number of users that can log in by using a RFID card and managed with “PM-LOGON Configurator “ is defined by the number of users defined by the installed User Packages. User Packages are digitally signed xml files. In order to activate a User Package you have to import it into the PM-LOGON Configurator. In order to do this, navigate to the “Configuration” element and open the page with the tile “Packages”.

To import a User Package click on the button labeled “Import”, which opens a file selection dialog. Select the User Package file to import and open it. After the package has been successfully imported it will be displayed in the list of installed packages. Also the number of totally available users will be updated accordingly at the bottom of the page.

The User Packages that you have ordered together with your PM-LOGON package are delivered to you by email.



Description of the displayed columns:

- Valid:
  Indicates that the User Package has been recognized as a valid license file and the signature has been successfully validated.

- Duplicate:
  Indicates if the packages has been already imported by using another file name.

- Product Version:
  Product version of PM-LOGON this User Package is applicable to.

- Issue Date:
  Issuing date of the package.

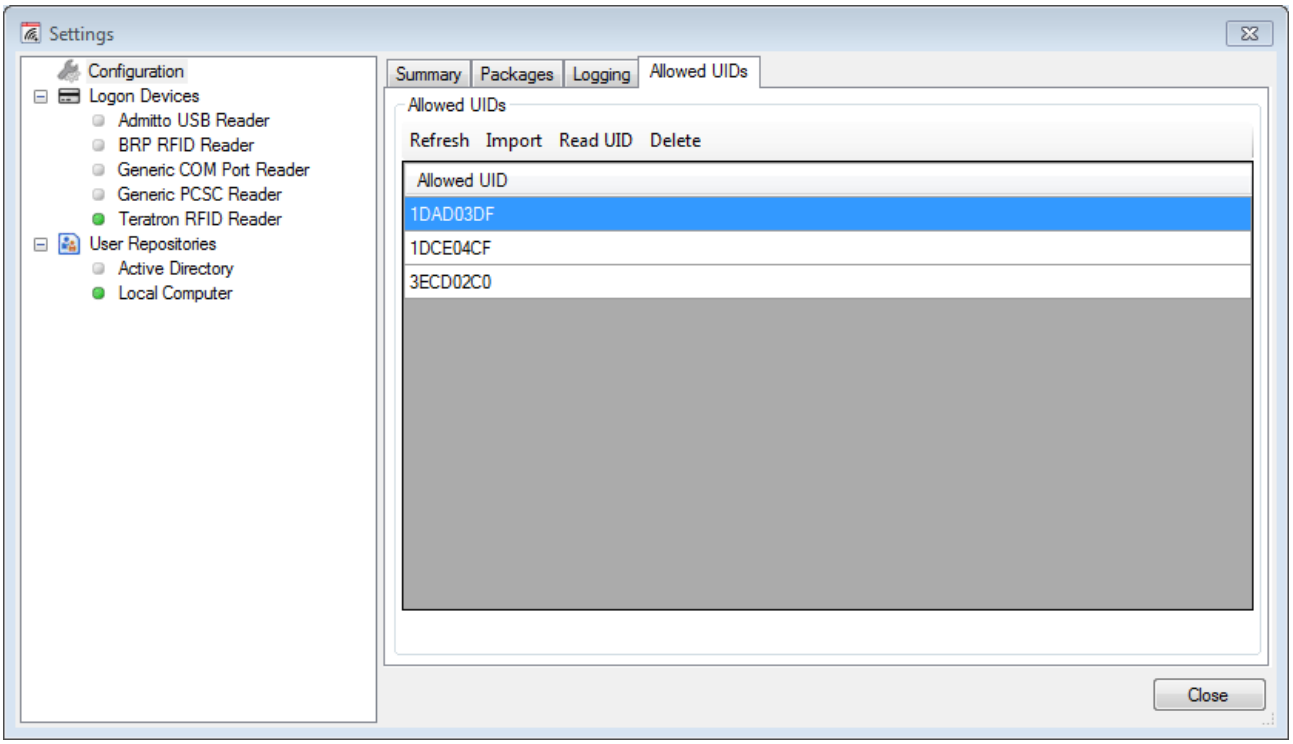
- Package Size:
  Number of users licensed by this package.

- Package File:
  File location of the package file.

Underneath the list of installed packages the total number of users licensed by all installed packages is displayed.

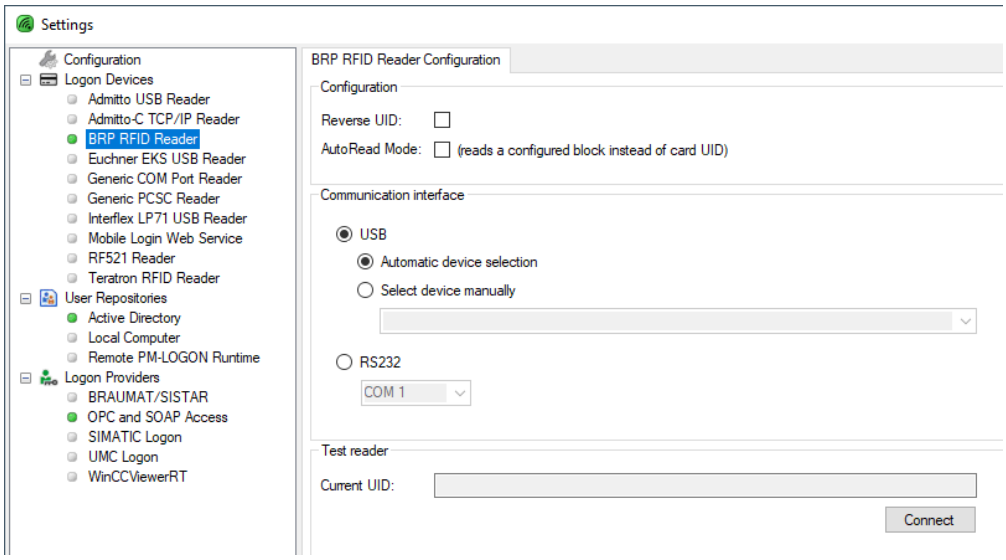
3.2.2 Maintaining the list of allowed UIDs

The list of allowed UIDs determines, which UIDs are allowed to be assigned to a user within the Configurator if activated on the summary page.
To import a list of UIDs click on the Import button and select a text file, containing a single UID per line.
A single UID read by a attached card reader can be added by clicking the button Read UID.
Delete UIDs from the list by selecting one ore multiple lines and clicking the Delete button.



3.2.3 Configuration of the SIMATIC RF1040R/RF1060R/RF1070R RFID card reader

The element labeled “BRP RFID Reader” allows the configuration of a connected SIMATIC RF1040R/RF1060R/RF1070R card reader device.



The setting “Reverse UID” instructs PM-LOGON to reverse the byte ordering of the unique id that has been read from the device. This might be required if the reader is used together with other reading devices that sometimes transmit the unique id of the card in reversed byte ordering. If this cannot be configured on the other reading device, it can be compensated here by activating this checkbox.

If the option “AutoRead Mode” is activated the reader doesn’t read the card UID but automatically reads a configured memory block depending on the card type. For this it is necessary that the reader is prepared with an “AutoRead” configuration.

In the section "Communication interface" it is possible to select the interface through which PM-LOGON communicates with the connected reader.

- USB (RF1040R/RF1060R/RF1070R):
  In most cases the setting "Automatic device selection" is sufficient. If the automatic device selection fails, the hardware ID of the reader can be specified here.
- RS232 (RF1040R/RF1070R):
  The virtual COM port, which is generated by the driver of the reader in the system, must be set. The correct port can be determined via the Windows Device Manager in the section "Ports (COM & LPT)".

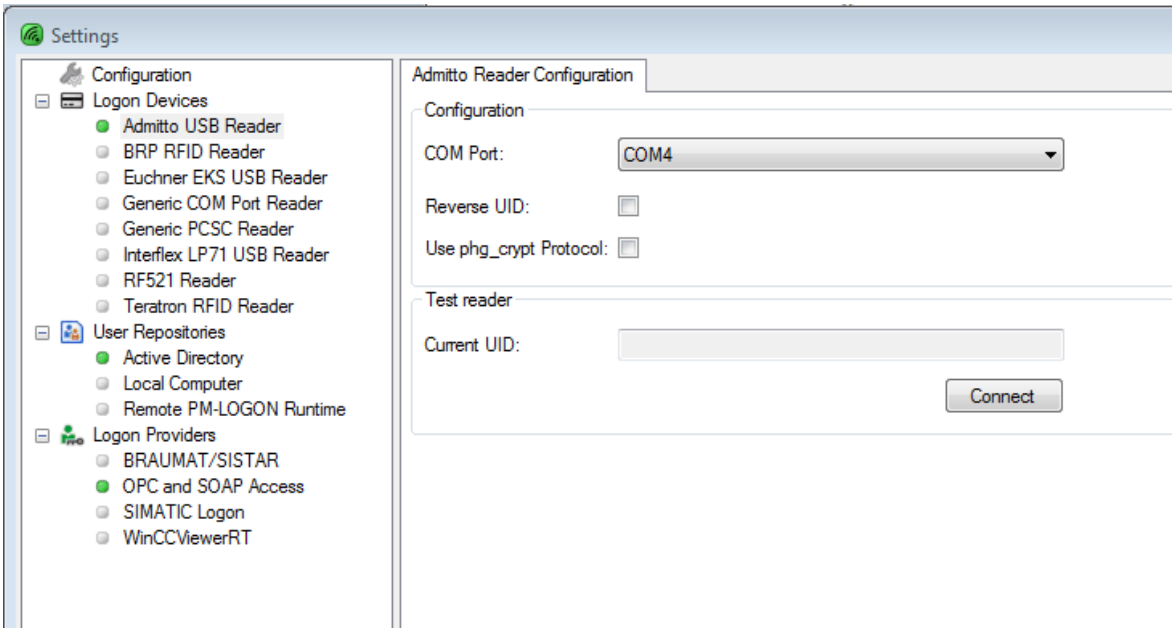
The elements in the section “Test Reader” can be used to test the reader for correct operation. In order to start the test, click the button “Connect” to establish a connection to the reading device. If the device is functioning correctly the unique id of the card will be displayed in the field “Current UID” when you bring the card into the detection range of the reader.

The initial connection attempt to the device might fail but this can be safely ignored.

In order to use the reader it must be selected as the standard device by selecting the command “Set as default”from the context menu. The context menu is opened by right clicking on the element.

3.2.4 Configuration of the Admitto USB reader

The element labeled “Admitto USB Reader” allows the configuration of a connected Admitto USB card reader device.



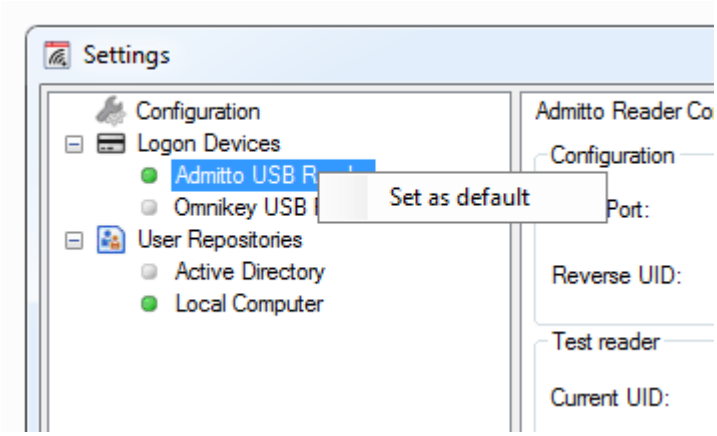
The communication with the Admitto USB reader is established over a virtual COM port. This COM port is only present when the device is connected to the PC. Therefore, make sure that the device is connected and the appropriate COM port is selected. The virtual COM port that is created by the device driver of the Admitto USB reader can be determined in the device manager of the Windows operating system.

The setting “Reverse UID” instructs PM-LOGON to reverse the byte ordering of the unique id that has been read from the device. This might be required if the reader is used together with other reading devices that sometimes transmit the unique id of the card in reversed byte ordering. If this cannot be configured on the other reading device, it can be compensated here by activating this checkbox.

If the Admitto USB reader is equipped with a Firmware that supports the phg_crypt protocol, the setting "Use phg_crypt Protocol" enables PM-LOGON to communicate with the Admitto USB reader using this specific protocol.

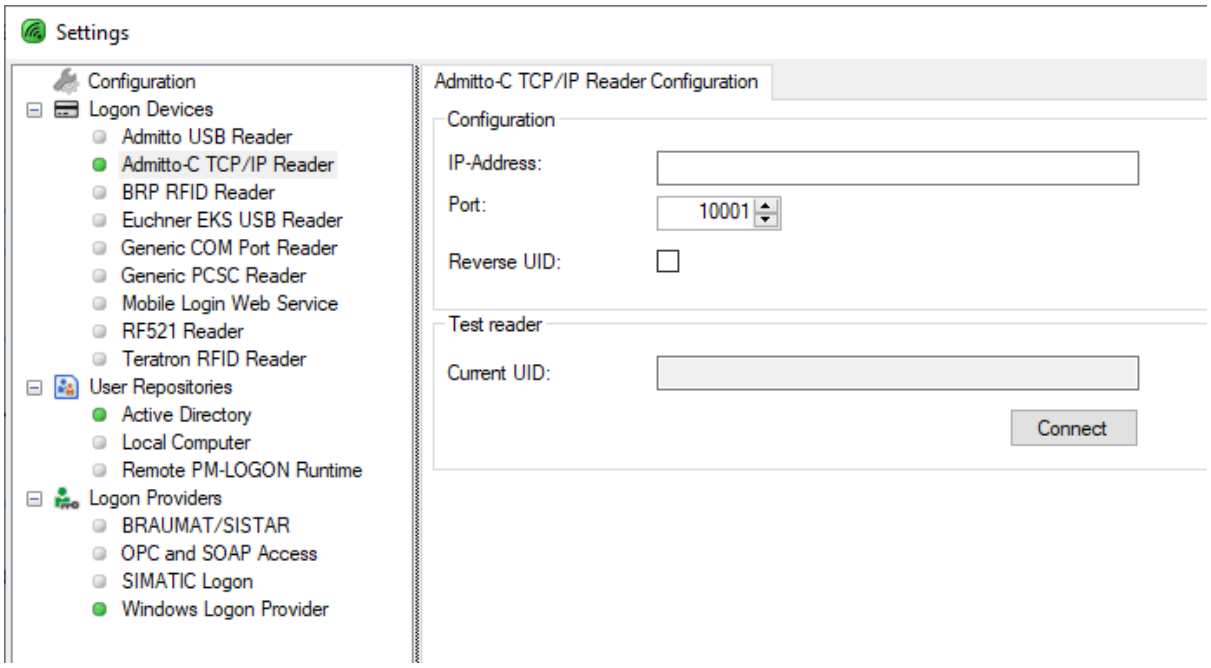
The elements in the section “Test Reader” can be used to test the reader for correct operation. In order to start the test click the button “Connect” to establish a connection to the reading device. If the device is functioning correctly the unique id of the card will be displayed in the field “Current UID” when you bring the card into the detection range of the reader.

In order to use the reader it must be selected as the standard device by selecting the command “Set as default” from the context menu. The context menu is opened by right clicking on the element.


Settings
Configuration
Logon Devices
Admitto USB R
Omnikey USB
User Repositories
Active Directory
Local Computer
Set as default
Admitto Reader Co
Configuration
Port:
Reverse UID:
Test reader
Current UID:

3.2.5 Configuration of the Admitto-C TCP/IP reader

The element labeled “Admitto-C TCP/IP Reader” allows the configuration of a connected Admitto-C TCP/IP card reader device.

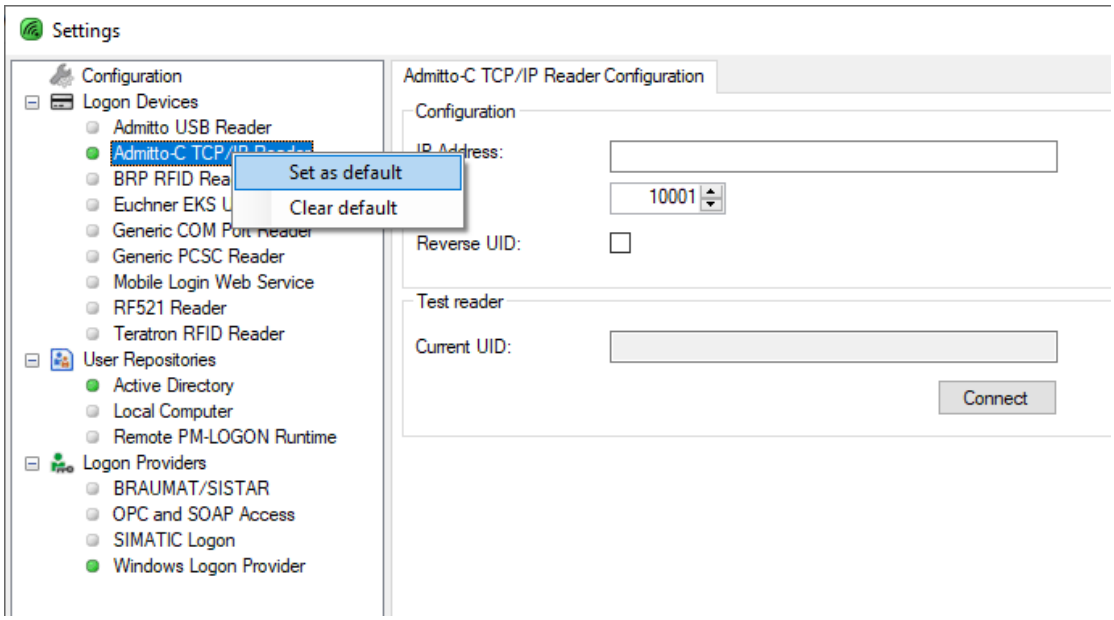


The communication with the Admitto-C TCP/IP reader is established over a TCP connection. Establishing a connection is only possible if the reader is connected to a network, over which the computer can reach the reader. This must be done by using an ethernet cable and the designated connector on the reader. Also, make sure the reader is powered over an USB-cable. Before the connection can be established, you must enter the reader’s IP-Address in the field “IP-Address” and the port, which is configured in the readers own configuration, in the field “Port”. You can get this information about the reader with the tool “Device Installer” from Lantronix. The reader itself is configured with the port 10001 by default.

The setting “Reverse UID” instructs PM-LOGON to reverse the byte ordering of the unique id that has been read from the device. This might be required if the reader is used together with other reading devices that sometimes transmit the unique id of the card in reversed byte ordering. If this cannot be configured on the other reading device, it can be compensated here by activating this checkbox.

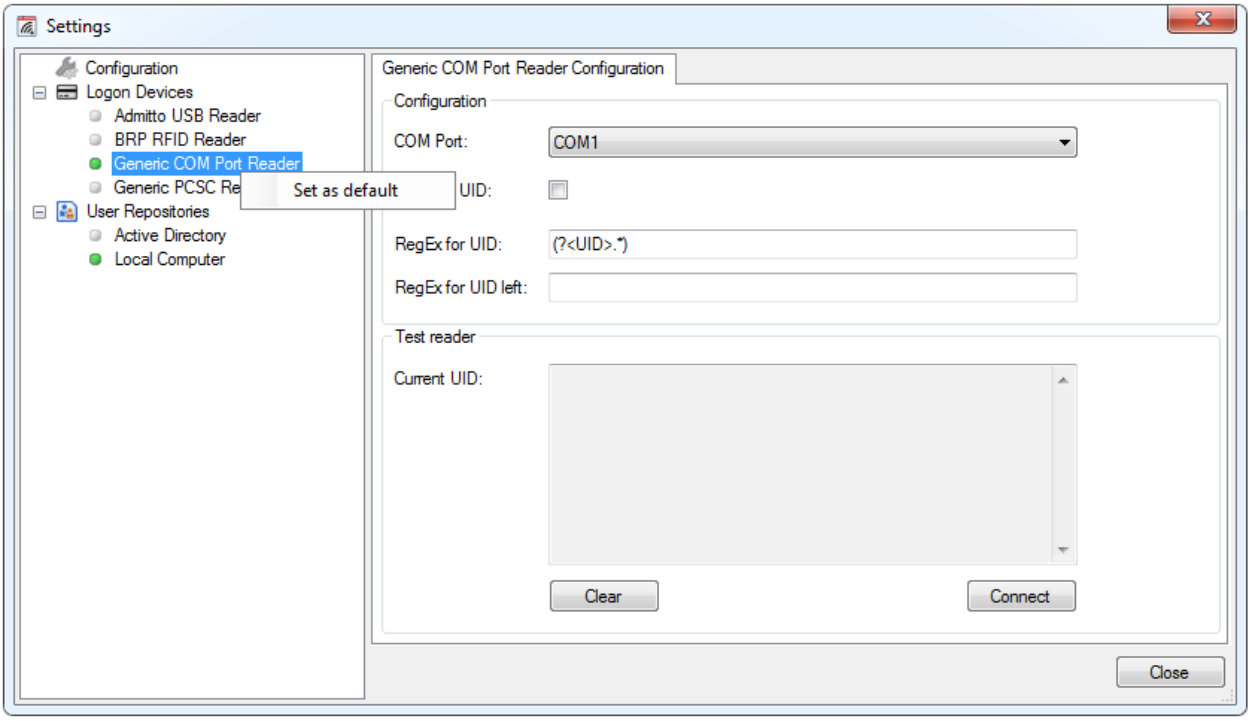
The elements in the section “Test Reader” can be used to test the reader for correct operation. In order to start the test, click the button “Connect” to establish a connection to the reading device. If the device is functioning correctly the unique id of the card will be displayed in the field “Current UID” when you bring the card into the detection range of the reader.

In order to use the reader, it must be selected as the standard device by selecting the command “Set as default” from the context menu. The context menu is opened by right clicking on the element.



3.2.6 Configuration of a generic COM port reader

There are various reading devices available that establish a communication channel to the PC by creating a virtual COM port from the device driver. For such devices the element “Generic COM Port Reader” can be used.
A precondition for this configuration type is that the reading device is actively sending the serial number (unique id) of the card as soon as it is brought into the detection range of the reader.



Select the serial (COM) port the reader has been connected to. Virtual COM ports that are generated by the device driver can be determined by using the device manager of the Windows operating system.

The setting “Reverse UID” instructs PM-LOGON to reverse the byte ordering of the unique id that has been read from the device. This might be required if the reader is used together with other reading devices that sometimes transmit the unique id of the card in reversed byte ordering. If this cannot be configured on the other reading device, it can be compensated here by activating this checkbox.

The reader delivers a data stream at the serial port connection when a card is detected and removed. To interpret the data sent from the device in order to filter out the unique id of the card, a regular expression is used. A description how regular expressions can be built in order to filter data from continuous text streams can be found under the following URL:

https://msdn.microsoft.com/de-de/library/hs600312(v=vs.110).aspx

In order to filter out the unique card id of the data stream sent when the card enters the detection range of the reader a regular expression must be entered into “RegEx for UID”. Optionally the reader might also send a data stream when the card leaves the detection range. The data that is expected to be sent on this event needs to be entered into the field “RegEx for UID left”.

In order to precisely match the unique id of the card contained in the data sent from the reader a so called “Named Matched Subexpression” with the name “UID” is used. That means that the data stream might contain additional control characters like e.g. STX and ETX which are not part of the unique card id. In this way it is possible to separate the data that is expected when the card enters the reader field and which part of this data represents the unique id.

A detailed description of “Named Matched Subexpressions” can e.g. be found under the URL:

https://msdn.microsoft.com/de-de/library/bs2twtah(v=vs.110).aspx#named_matched_subexpression

In the example above, everything that is sent from the reader is treated as the unique id.

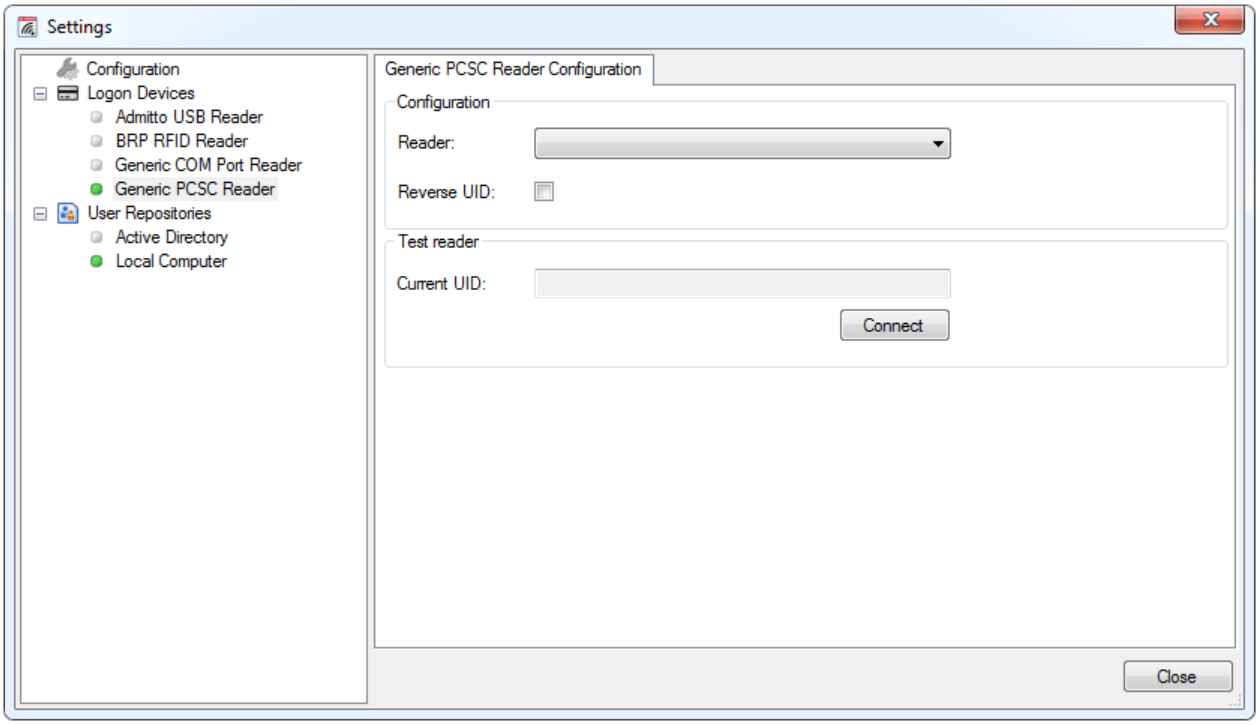
If you want to test the regular expressions you have been creating you may also test them under e.g. https://regex101.com/.
Make sure, no control characters (e.g. CR LF) are included in the result of the match.

The elements in the section “Test Reader” can be used to test the reader for correct operation. In order to start the test click the button “Connect” to establish a connection to the reading device. If the device is functioning correctly the unique id of the card will be displayed in the field “Current UID” when you bring the card into the detection range of the reader.

In order to use the reader it must be selected as the standard device by selecting the command “Set as default” from the context menu. The context menu is opened by right clicking on the element.

3.2.7 Configuration of a generic PCSC card reader

The element labeled “Generic PCSC Reader” allows the configuration of a connected PCSC card reader device (e.g. Omnikey).



Please select the appropriate reader from the list of detected compatible reading devices.

The setting “Reverse UID” instructs PM-LOGON to reverse the byte ordering of the unique id that has been read from the device. This might be required if the reader is used together with other reading devices that sometimes transmit the unique id of the card in reversed byte ordering. If this cannot be configured on the other reading device, it can be compensated here by activating this checkbox.

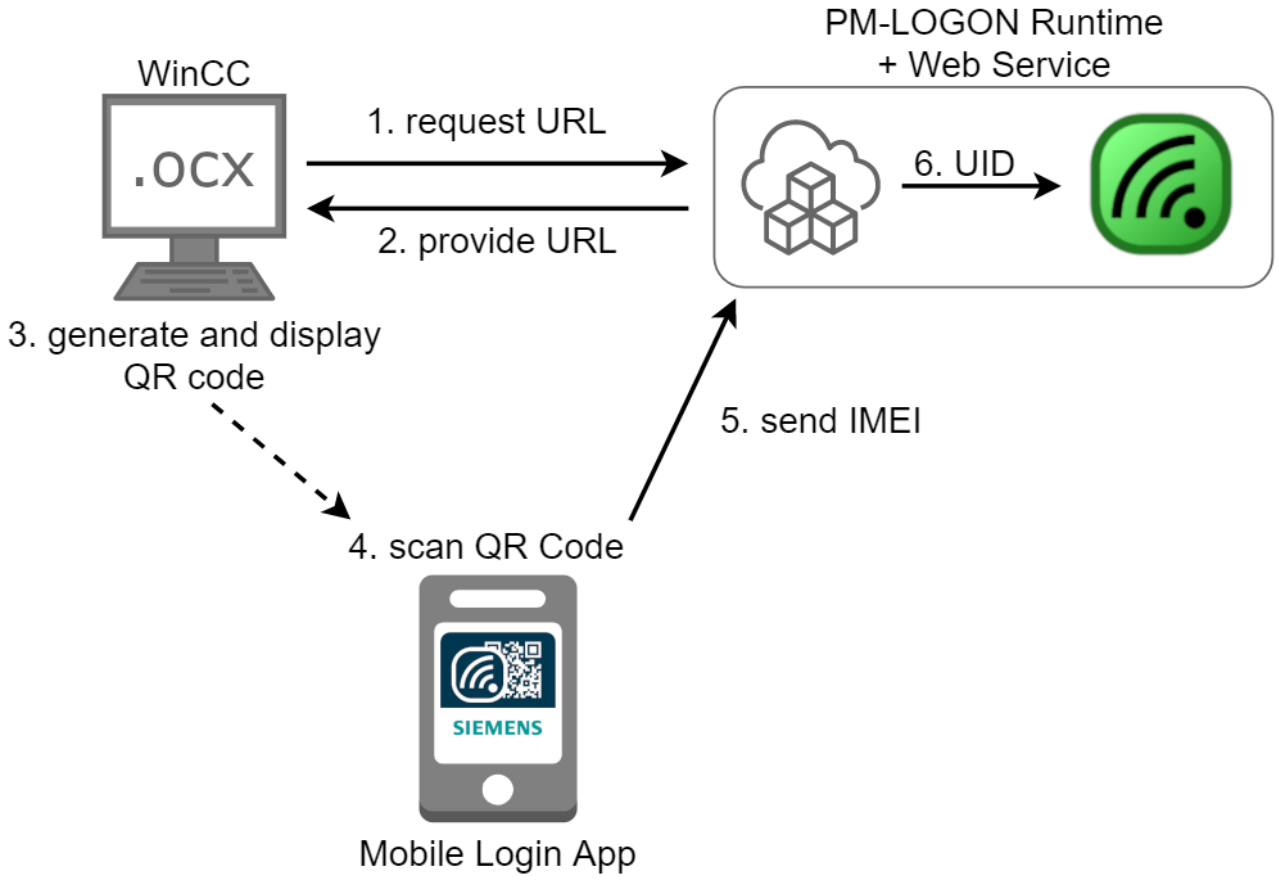
The elements in the section “Test Reader” can be used to test the reader for correct operation. In order to start the test click the button “Connect” to establish a connection to the reading device. If the device is functioning correctly the unique id of the card will be displayed in the field “Current UID” when you bring the card into the detection range of the reader.

In order to use the reader it must be selected as the standard device by selecting the command “Set as default” from the context menu. The context menu is opened by right clicking on the element.

3.2.8 Mobile Login

PM-LOGON Mobile Login enables a user to log in to WinCC via a mobile device. The user is authenticated via the IMEI of his mobile device, which serves as UID. Three components are required for this: The Mobile Login QR-Generator ActiveX Control in a WinCC image, the Mobile Login App on the user's mobile device and the Mobile Login Web Service in the PM-LOGON Runtime. In addition, a logon provider that enables logon to WinCC must be used, e.g. SIMATIC-Logon (see chapter 4.3.15). Mobile Login cannot be used together with Windows Logon Provider.

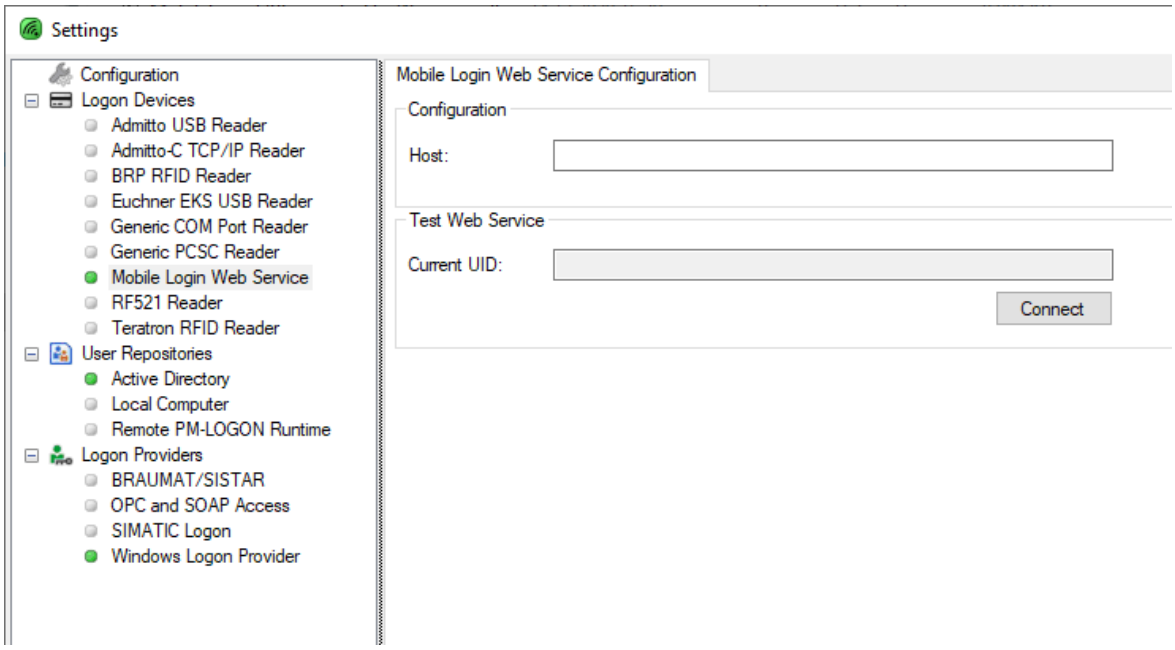
The authentication process is as follows:



1. By clicking the login button, the QR-Generator sends a request to the web service.
2. The web service responds with a URL, via which the Mobile Login App can reach the web service.
3. The QR-Generator generates and displays the QR code.
4. The user scans the QR code with the Mobile Login App on his device.
5. The Mobile Login App sends a request to the web service and passes the IMEI of the device.
6. The web service receives the request and passes the IMEI as UID to the PM-LOGON Runtime.

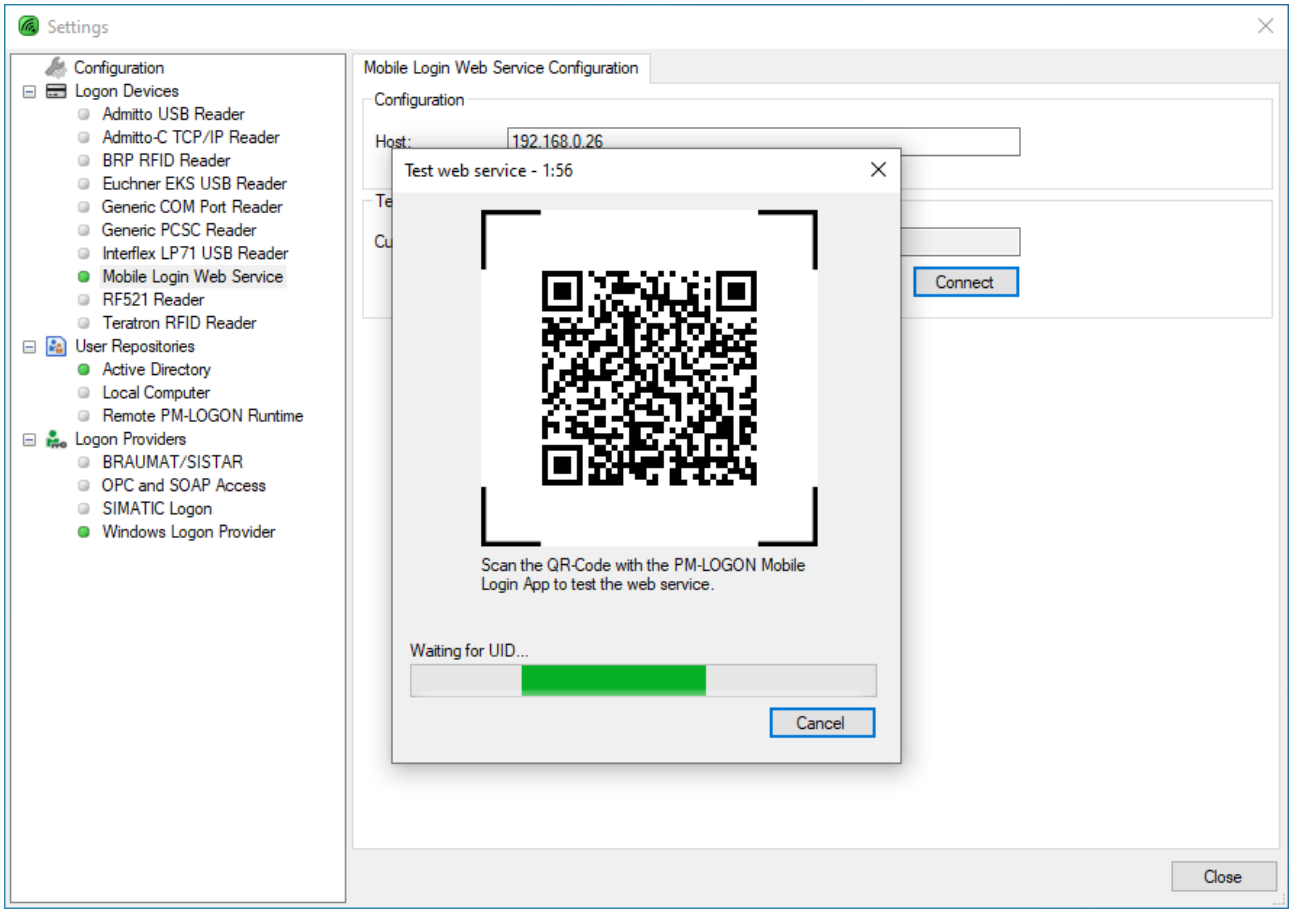
3.2.8.1 Configuration of the Mobile Login Web Service

The element labeled “Mobile Login Web Service” allows the configuration of the Mobile Login Web Service.

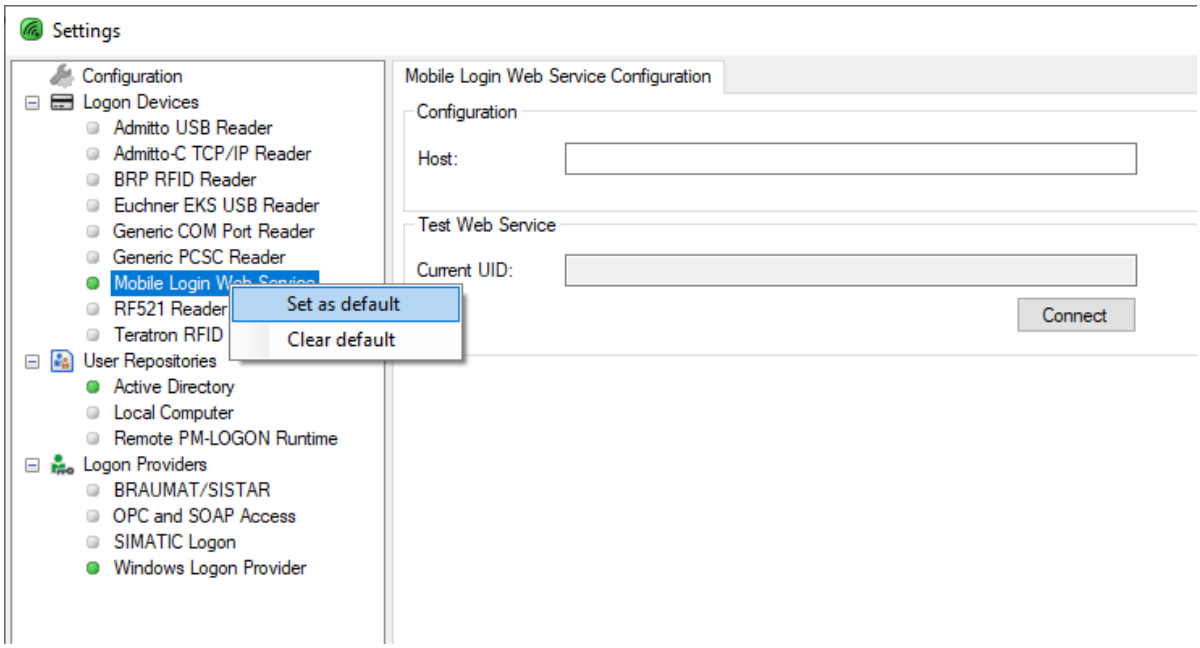


In the “Host” field, you must enter the IP-Address of the computer, over which the Mobile Login App can reach the computer. The port of the Mobile Login Web Service is fixed and cannot be specified here.

The elements in the section “Test Web Service” can be used to test the Mobile Login Web Service for correct operation. To start the test, click the button “Connect” to start the web service. If you scan the shown QR-Code with the Mobile Login App on a mobile device, the unique id of the card will be displayed in the field “Current UID”.

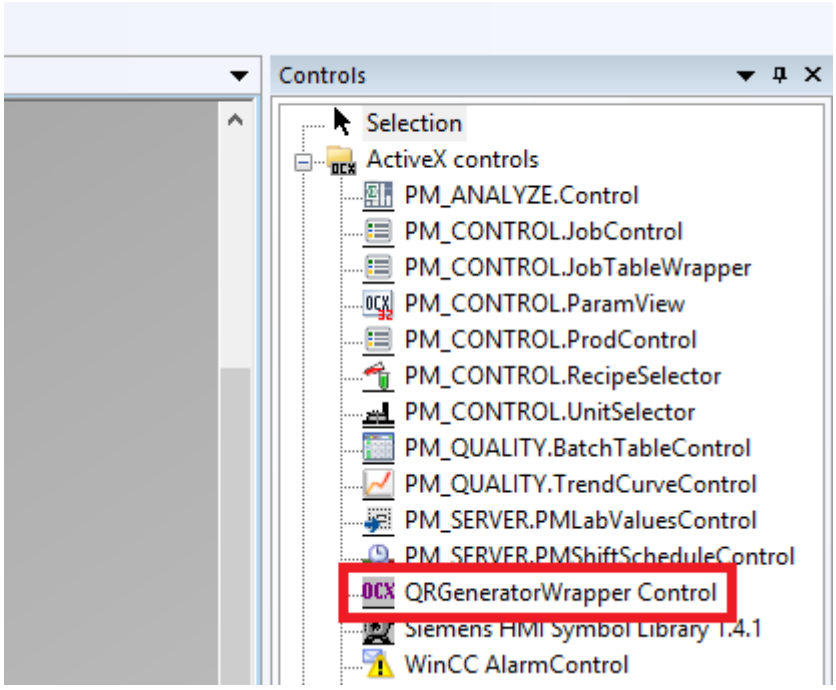


To get the web service started, it must be selected as the standard login method by selecting the command “Set as default” from the context menu. The context menu is opened by right clicking on the element.

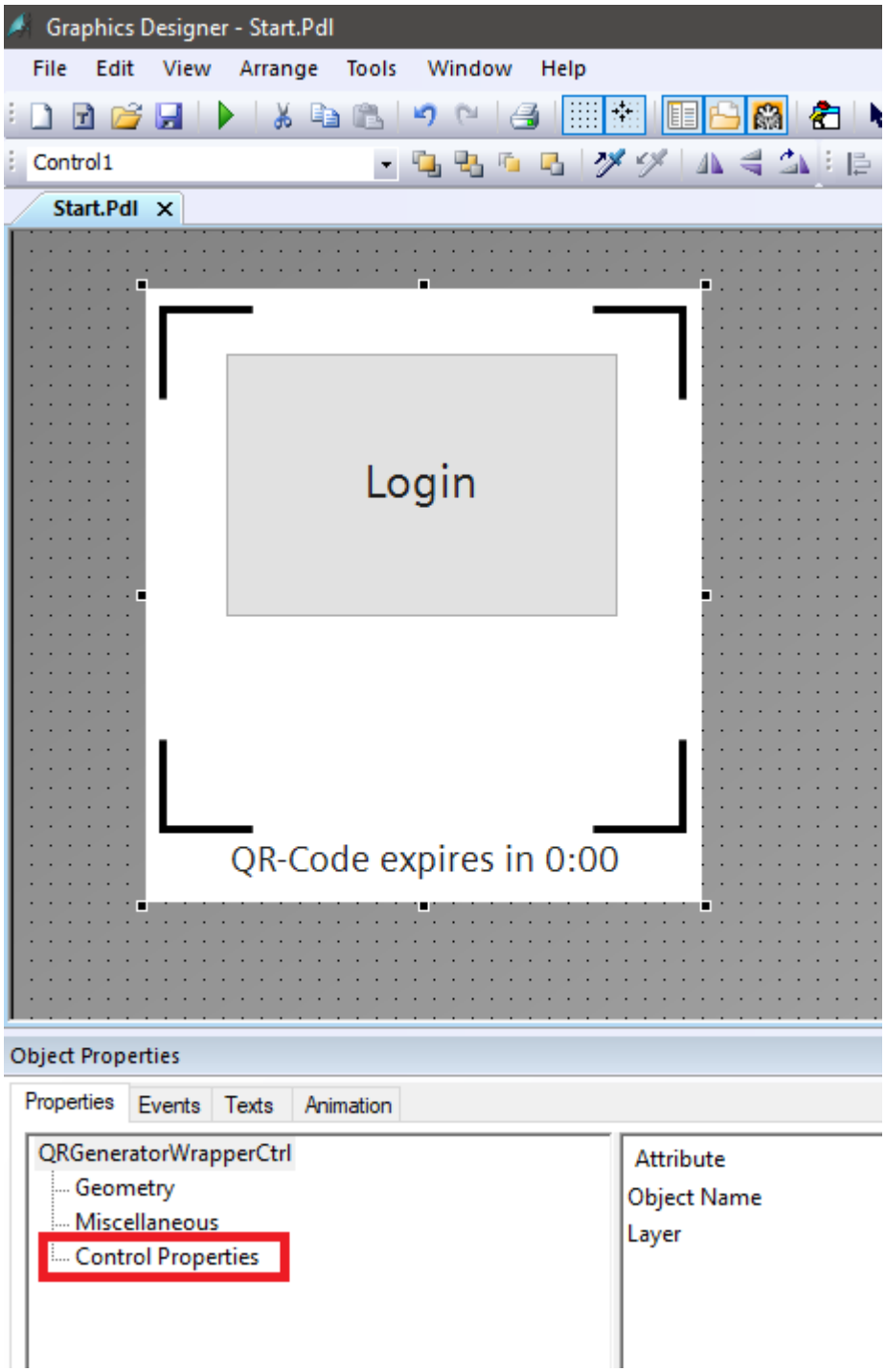


3.2.8.2 Configuration of the Mobile Login QR-Generator ActiveX Control

The Mobile Login QR-Generator ActiveX Control is installed during the installation of PM-LOGON and can be integrated into a WinCC picture in the WinCC Graphics Designer.

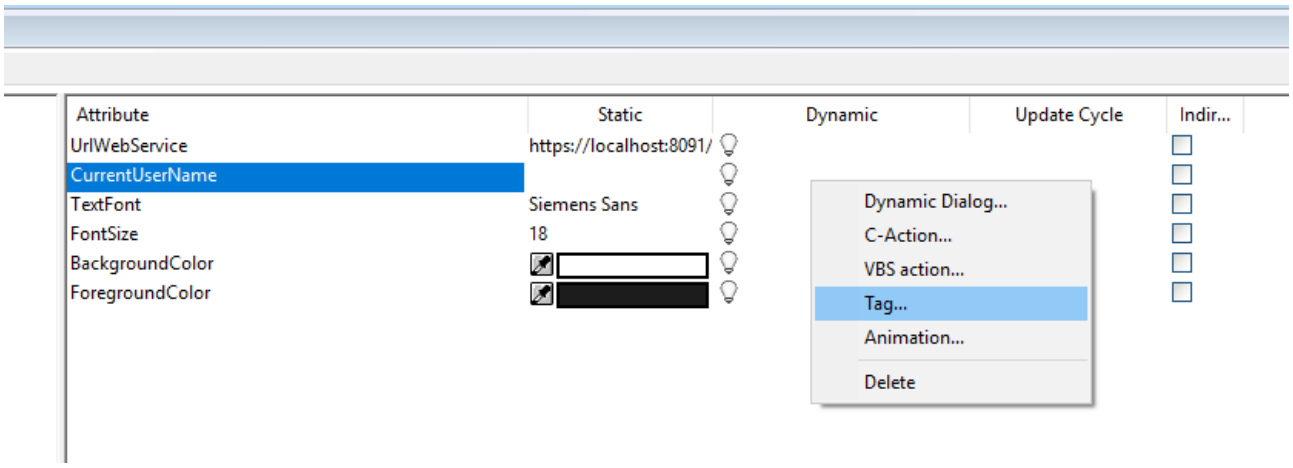


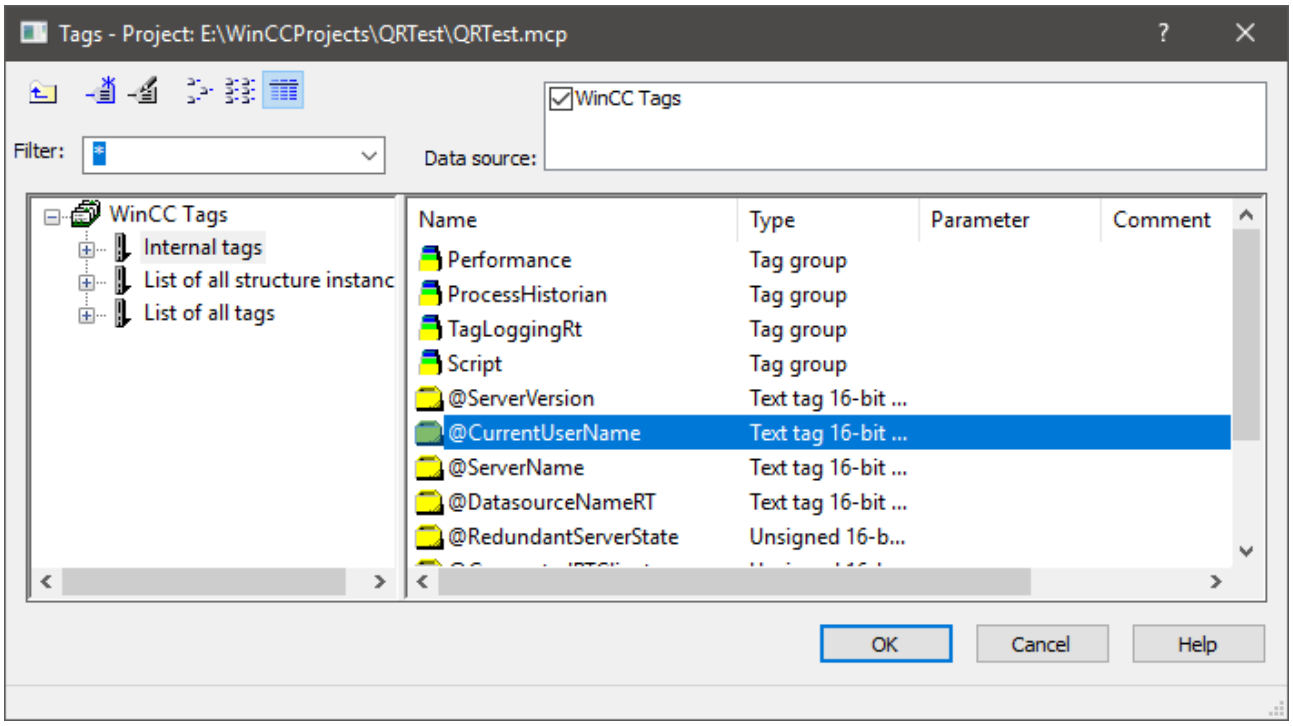
If the control is selected, the properties of the control can be displayed and configured by clicking on "Control Properties".

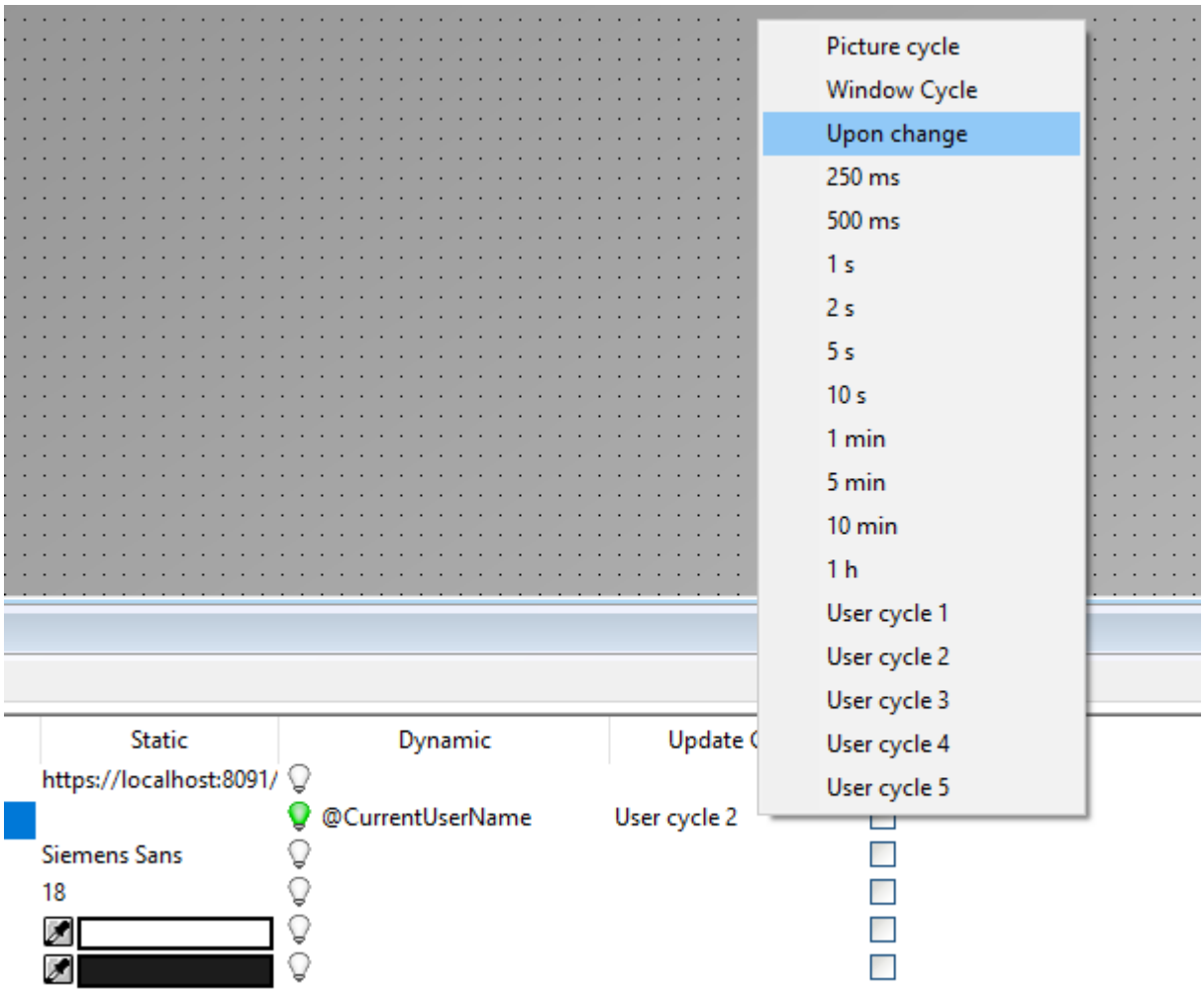


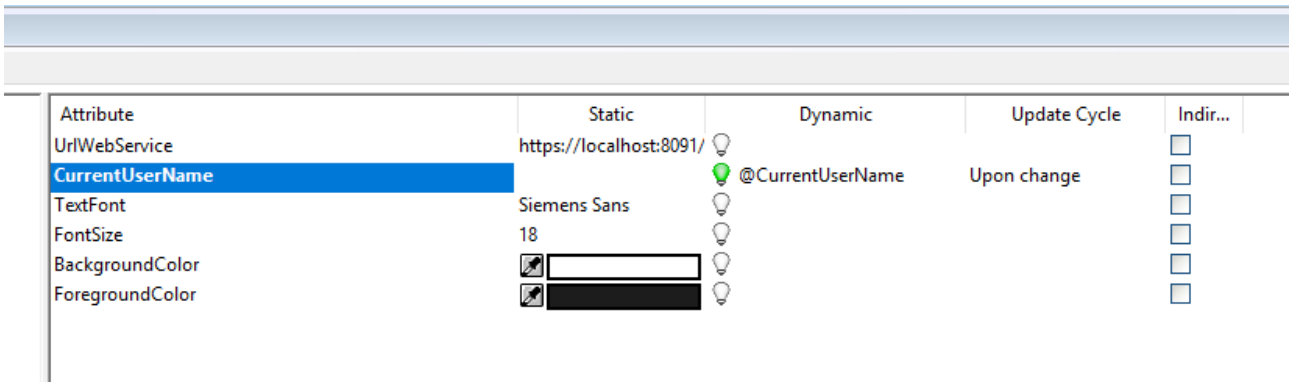
UrlWebService: Here the URL must be entered, over which the control can reach the web service in the runtime.

CurrentUserName: If the logged in user changes, the control should display the login button again. For this purpose, this property must be linked to the internal tag "@Current User" by right-clicking in the column "Dynamic" at "CurrentUserName". For update cycle, "Upon Change" must be selected by right-clicking in the column “Update Cycle”, so that the control is notified when the tag changes.









TextFont: Here you can specify a font for the control.

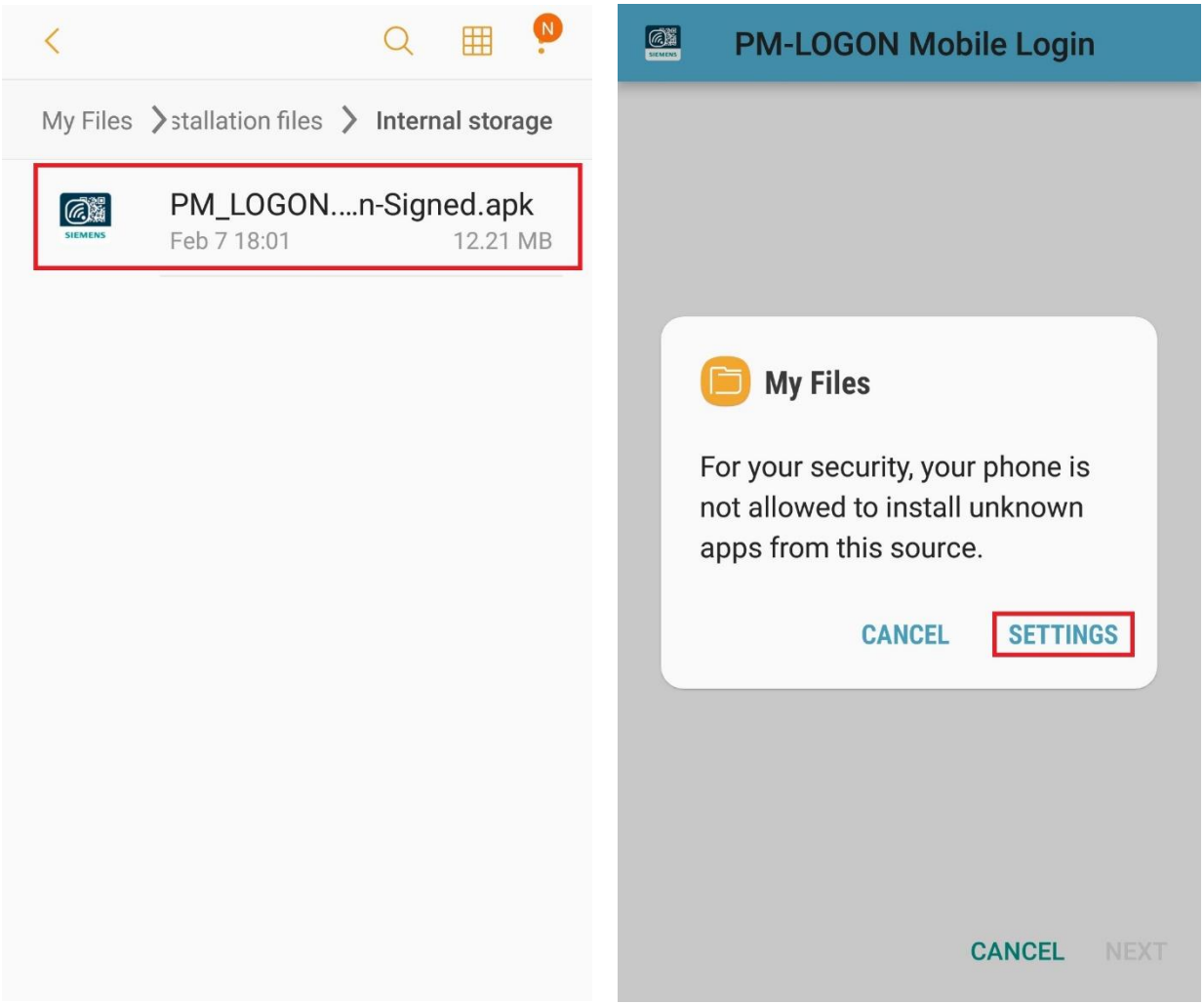
FontSize: Here the font size can be adjusted.

Background/ForegroundColor: Here you can change the foreground and background color of the control.

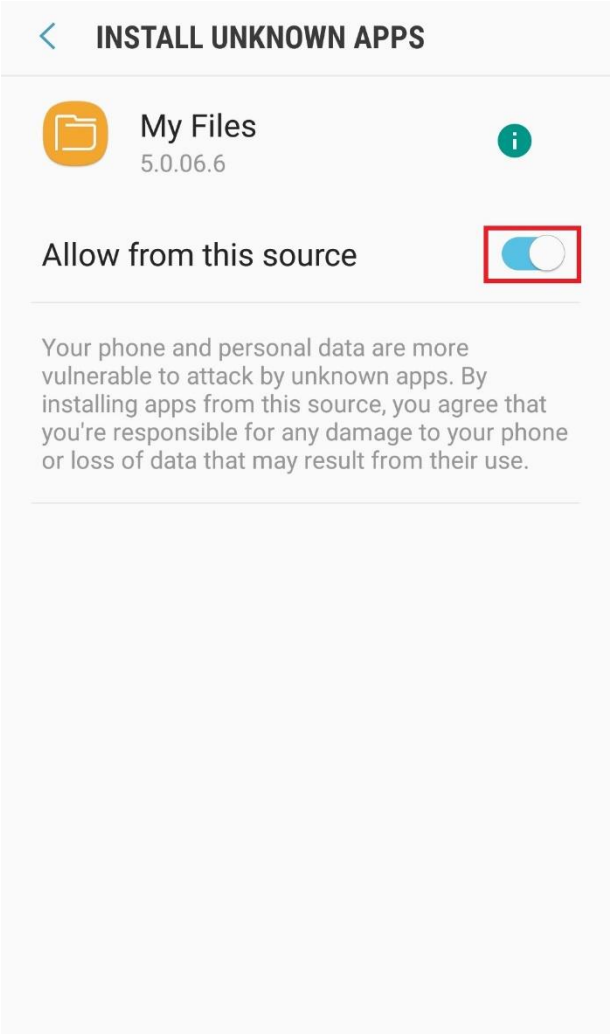
3.2.8.3 Installation of the Mobile Login App

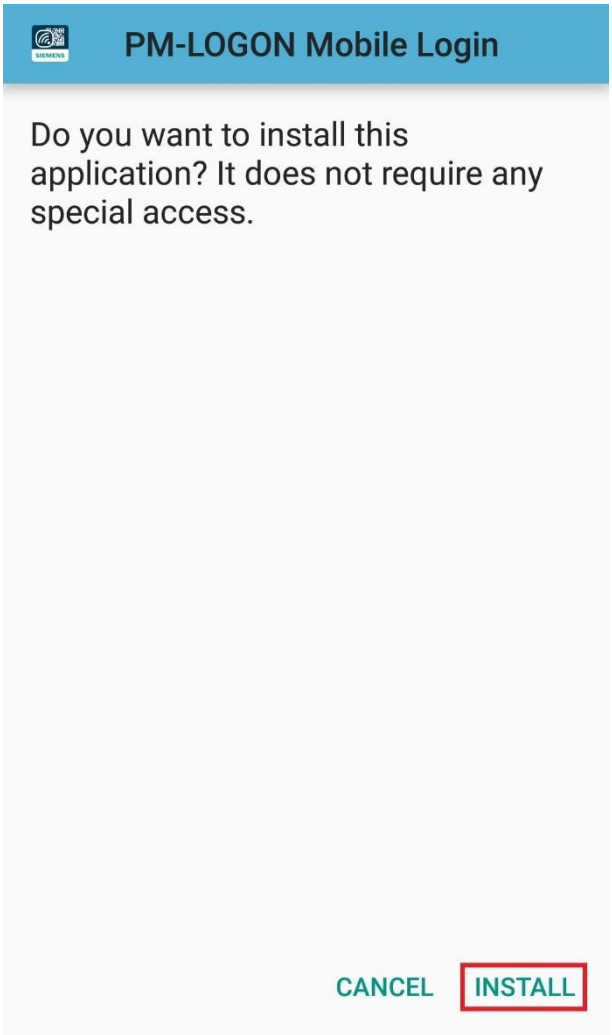
In order to login an user via the Mobile Login Web Service, the user has to have the Mobile Login App installed on his mobile device.

The .apk installation file is stored on the installation media under ".\V2\Android\PM_LOGON.MobileLogin-Signed.apk". The installation file can be moved to the mobile device's storage over an USB-Connection.

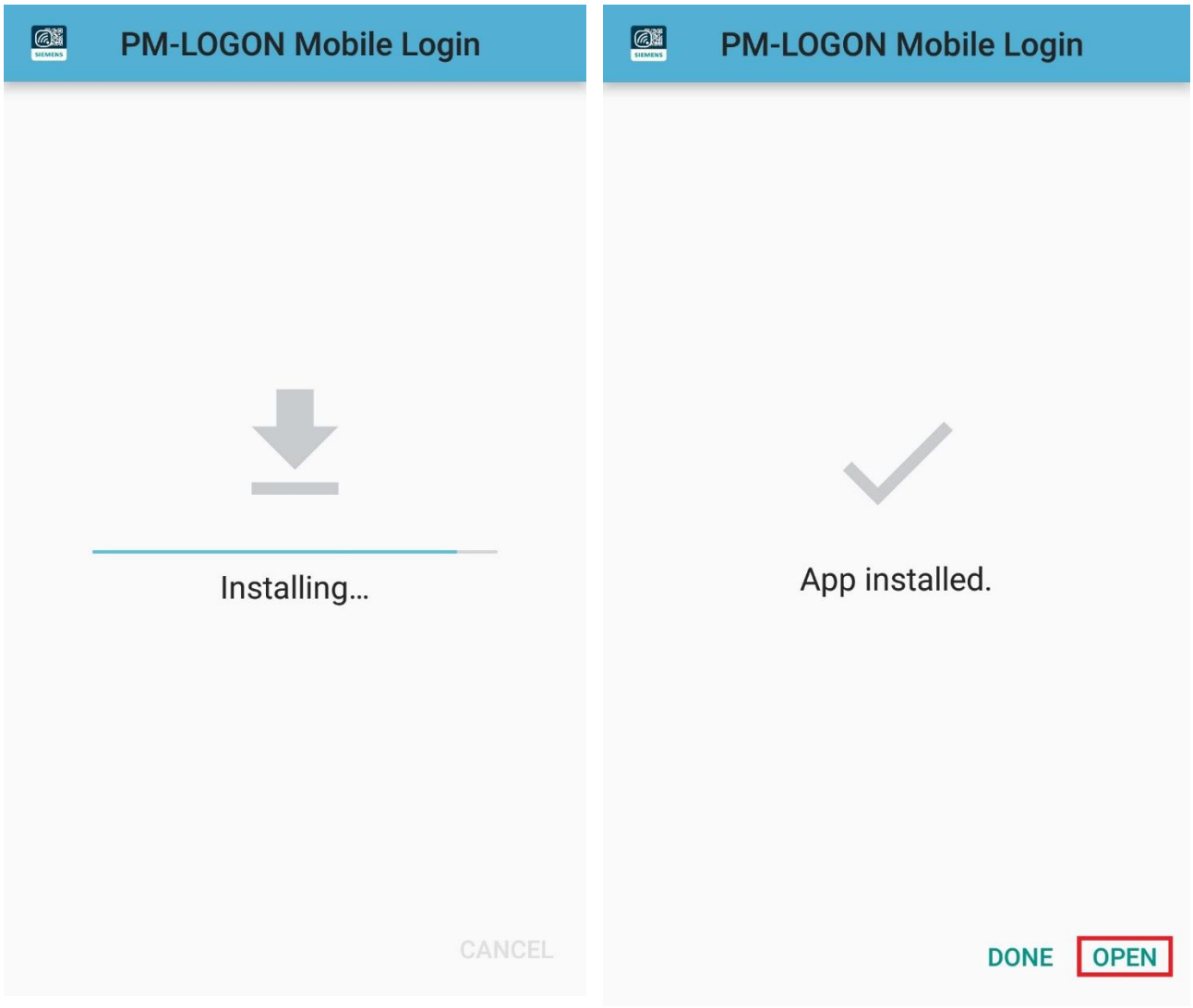


Before installing an .apk file manually, installing apps from unknown sources must be allowed.

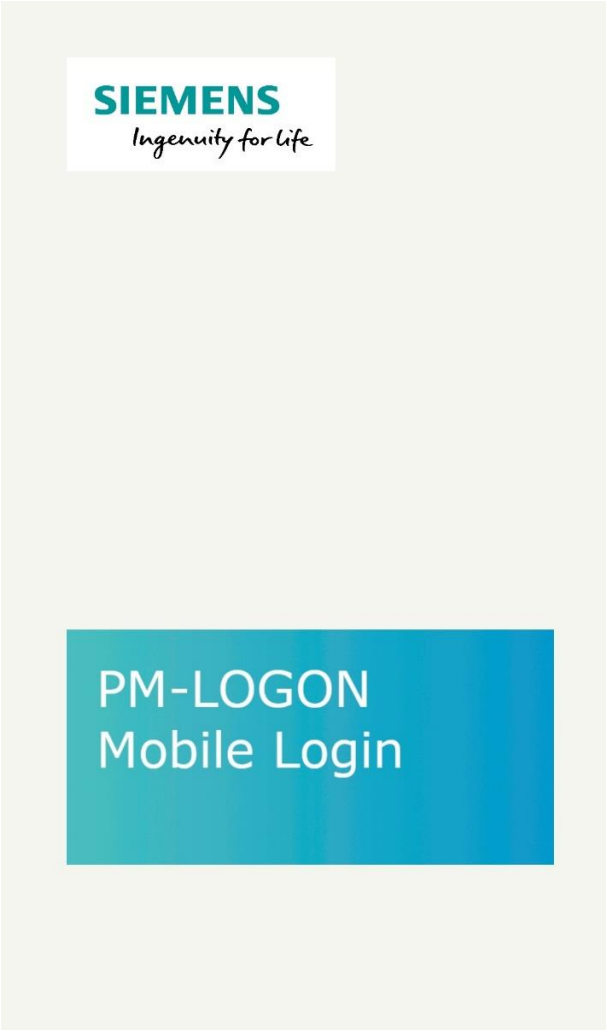




Afterwards, the app can be installed.

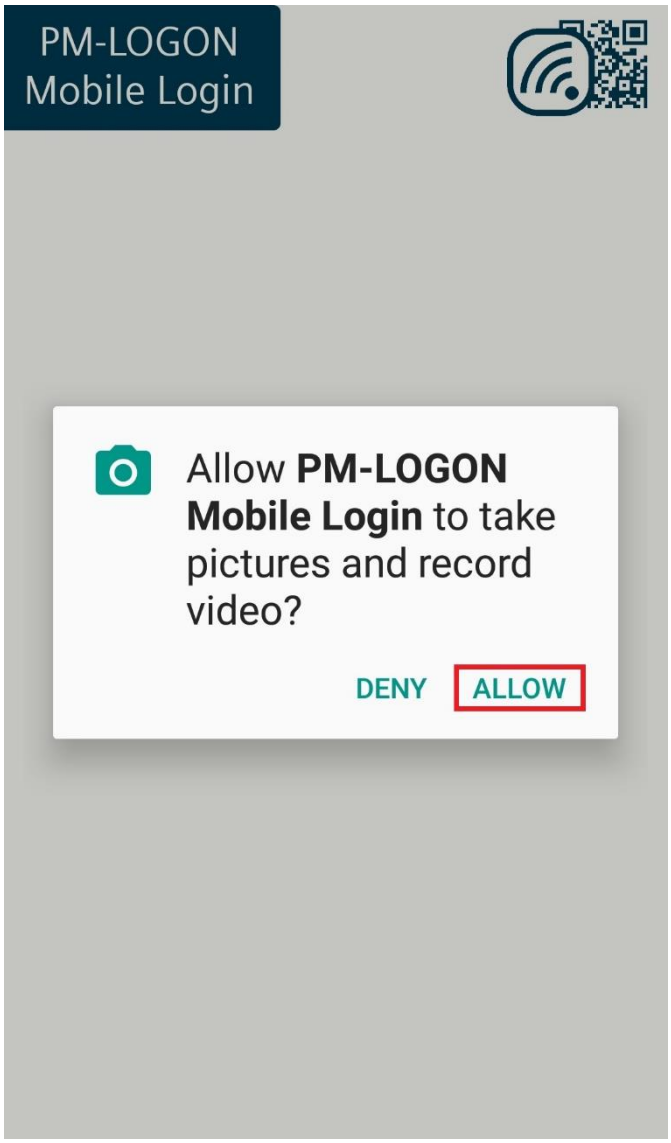


After installing, the app can be opened. If PM-LOGON shows a QR-Code for authentication, it can be scanned by the Mobile Login App by pressing the button “Scan QR-Code”.


SIEMENS
Ingenuity for life
PM-LOGON
Mobile Login

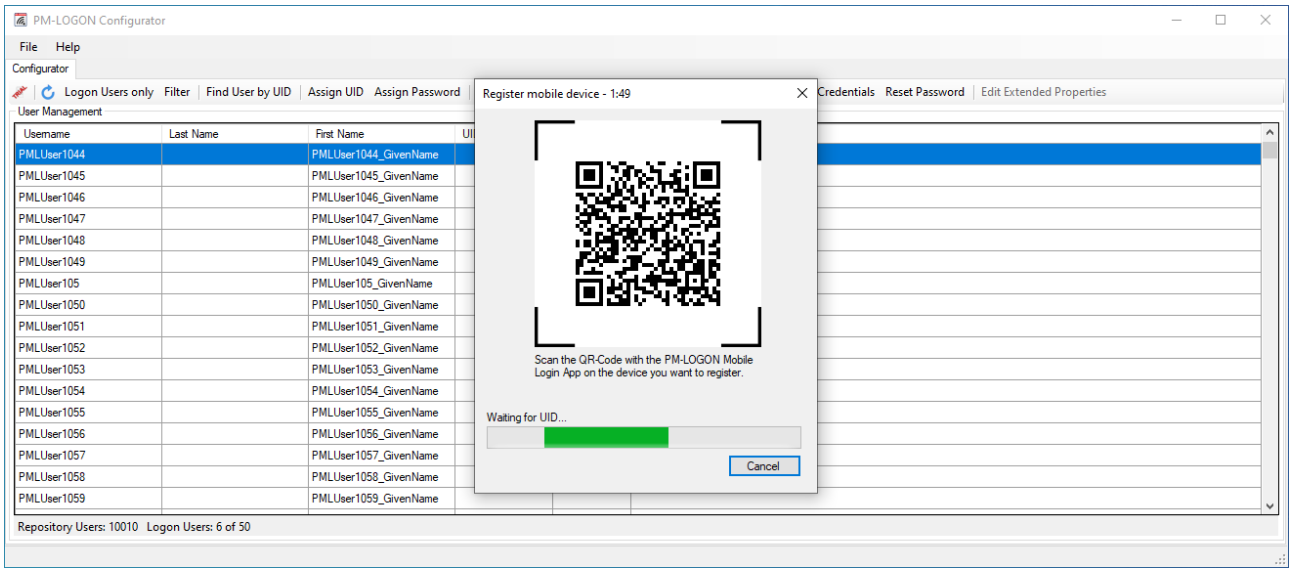

PM-LOGON
Mobile Login
SCAN QR-CODE

Before scanning a QR-Code for the first time, the app must have been granted privileges to take pictures and record video.



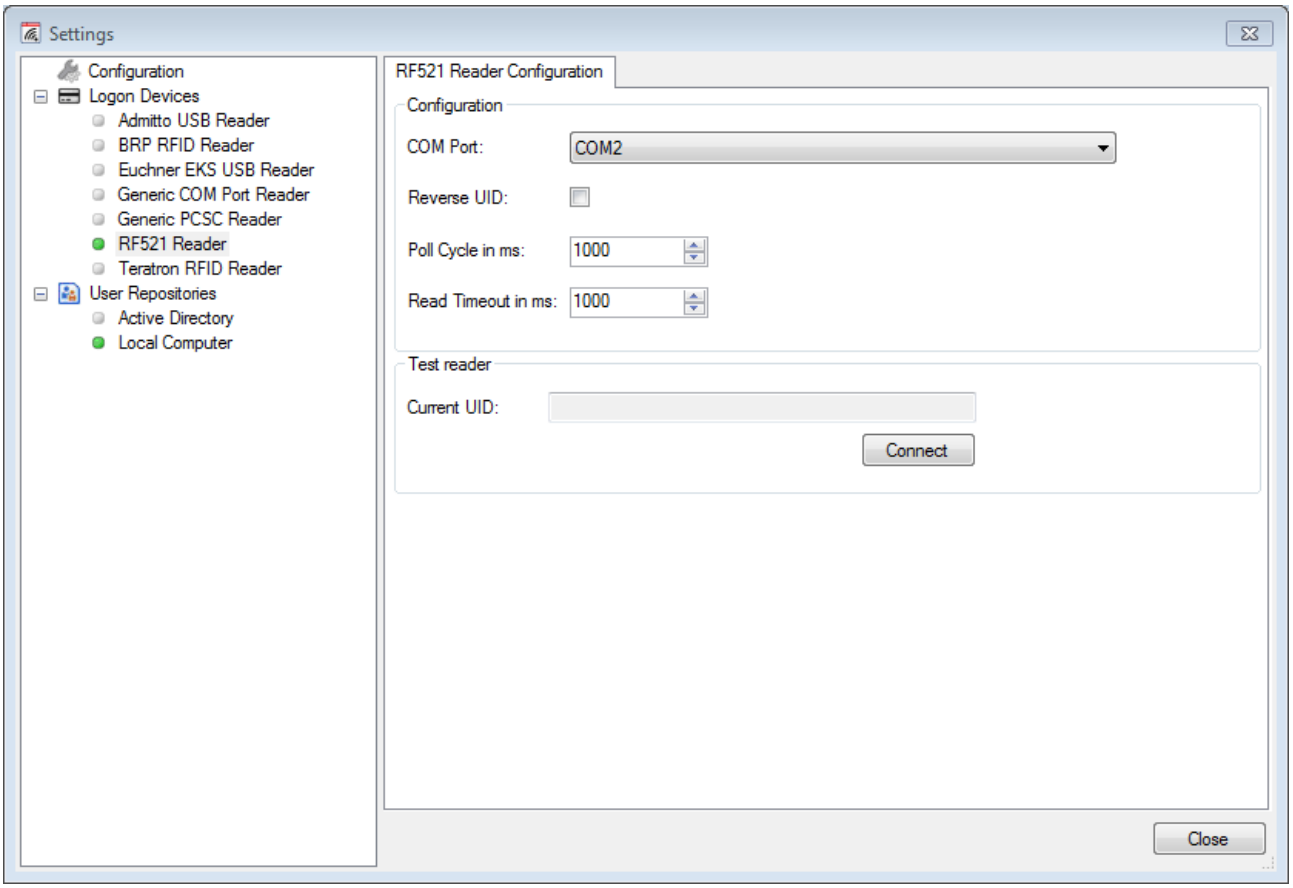
3.2.8.4 Assigning a mobile device to a user

In order to be able to log in via Mobile Login, the IMEI of the mobile device must be assigned to the user in the PM-LOGON Configurator. If the Mobile Login web service is selected as the logon device in the Configurator, clicking on "Assign UID" opens a new window with a QR code. If the user scans this QR code with the Mobile Login app on a device, the IMEI of this device is entered as the user's UID.



3.2.9 Configuration of a RF521 reader

The menu item "RF521 Reader" is used to configure a connected RF521 reader.



The RF521 reader is addressed via a virtual COM port; this COM port is only available if the device is connected to the PC. Therefore make sure that the device is connected and select the appropriate port. The virtual COM port generated by the driver of the RF521 reader can be determined via the Windows Device Manager.

Via the setting "Reverse UID" the Unique ID (UID) of the read RFID transponder transmitted by the reader can be reversed byte by byte. This may be necessary if other readers are in use which may transmit the UID in reverse byte order and this cannot be set on the reader itself.

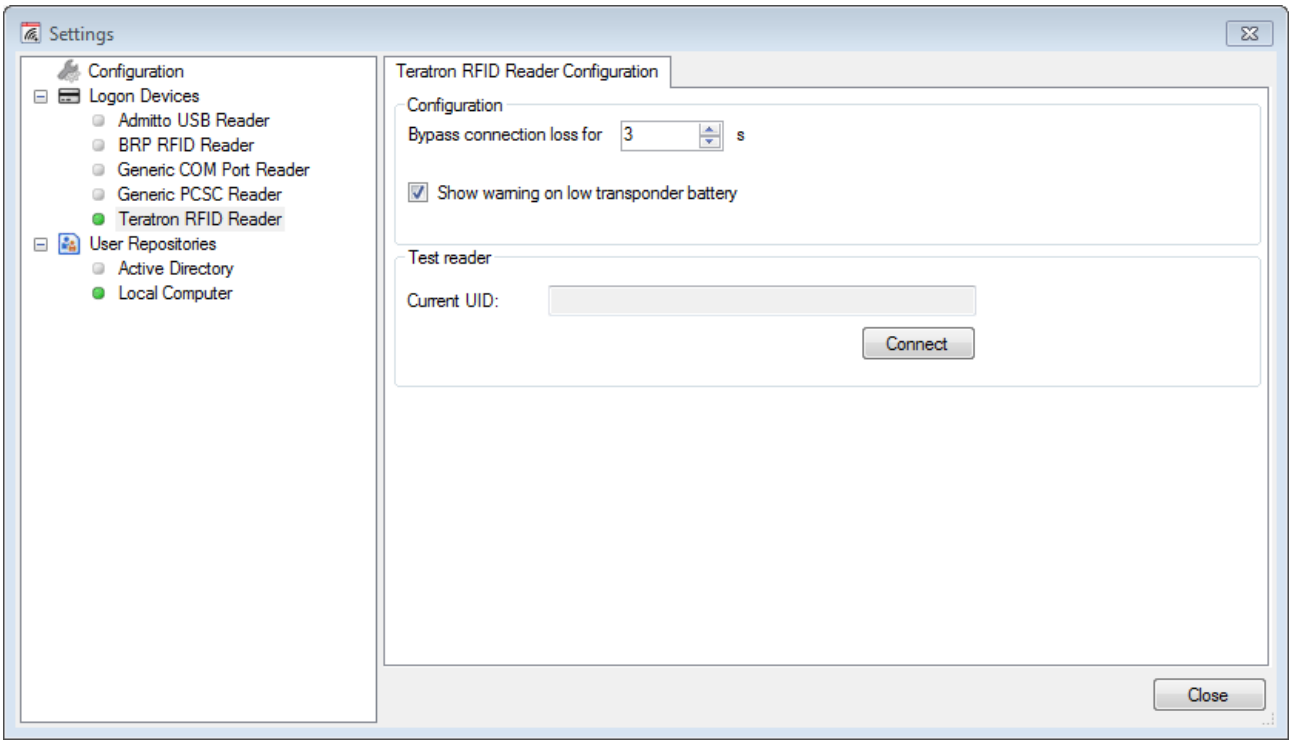
The setting "Poll Cycle in ms" defines the cycle in milliseconds in which the reader is queried.

In the section "Test Reader" the reader can be tested for correct function. To do this, press the "Connect" button to connect to the reader. If the device is functioning correctly the unique id of the card will be displayed in the field “Current UID” when you bring the card into the detection range of the reader.

To use the RF521 reader in PM-LOGON, you must now define it as the standard logon device. To do this, right-click the element "RF521 Reader" under "Logon Devices" in the tree structure and click on the entry "Set as default".

3.2.10 Configuration of a Teratron RFID reader

The element labeled "Teratron RFID Reader" allows the configuration of a connected Teratron RFID reader.
The Teratron PC-Loc driver for Siemens has to be installed first.



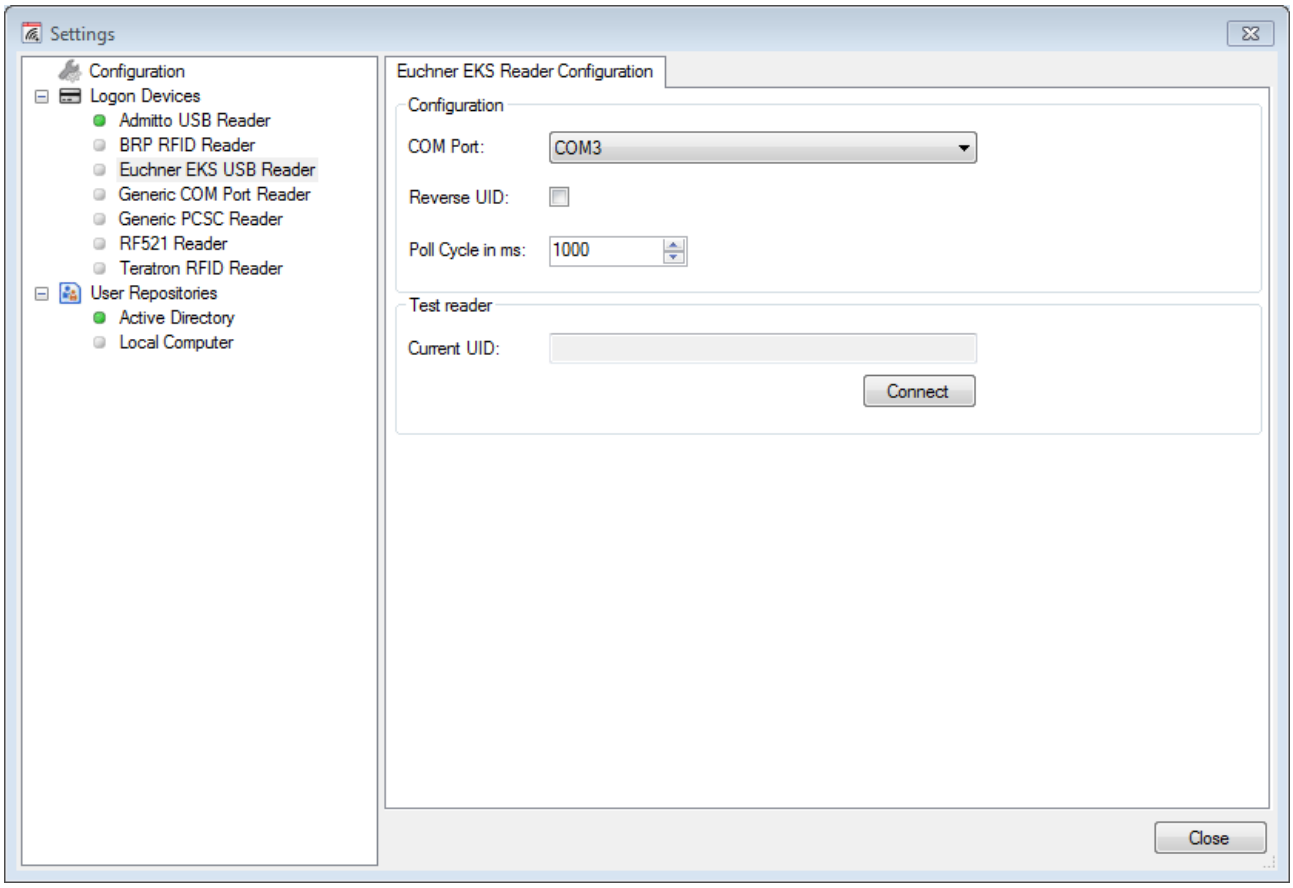
The setting "Bypass connection loss for" determines the time span, for which a connection loss between transponder an reader is bypassed by PM-LOGON.
This can be necessary if other electrical fields interfere with the field of the reader (e.g. mobile phones, power supplies).

The elements in the section “Test Reader” can be used to test the reader for correct operation. In order to start the test click the button “Connect” to establish a connection to the reading device. If the device is functioning correctly the unique id of the transponder will be displayed in the field “Current UID” when you bring the transponder into the detection range of the reader.

In order to use the reader it must be selected as the standard device by selecting the command “Set as default” from the context menu. The context menu is opened by right clicking on the element.

3.2.11 Configuration of an Euchner EKS USB Reader

The menu item "Euchner EKS USB Reader" is used to configure a connected Euchner EKS reader.



The Euchner EKS USB reader is addressed via a virtual COM port; this COM port is only available if the device is connected to the PC. Therefore make sure that the device is connected and select the appropriate port. The virtual COM port generated by the driver of the Euchner EKS reader can be determined via the Windows Device Manager.

Via the setting "Reverse UID" the Unique ID (UID) of the read EKS transponder transmitted by the reader can be reversed byte by byte. This may be necessary if other readers are in use which may transmit the UID in reverse byte order and this cannot be set on the reader itself.

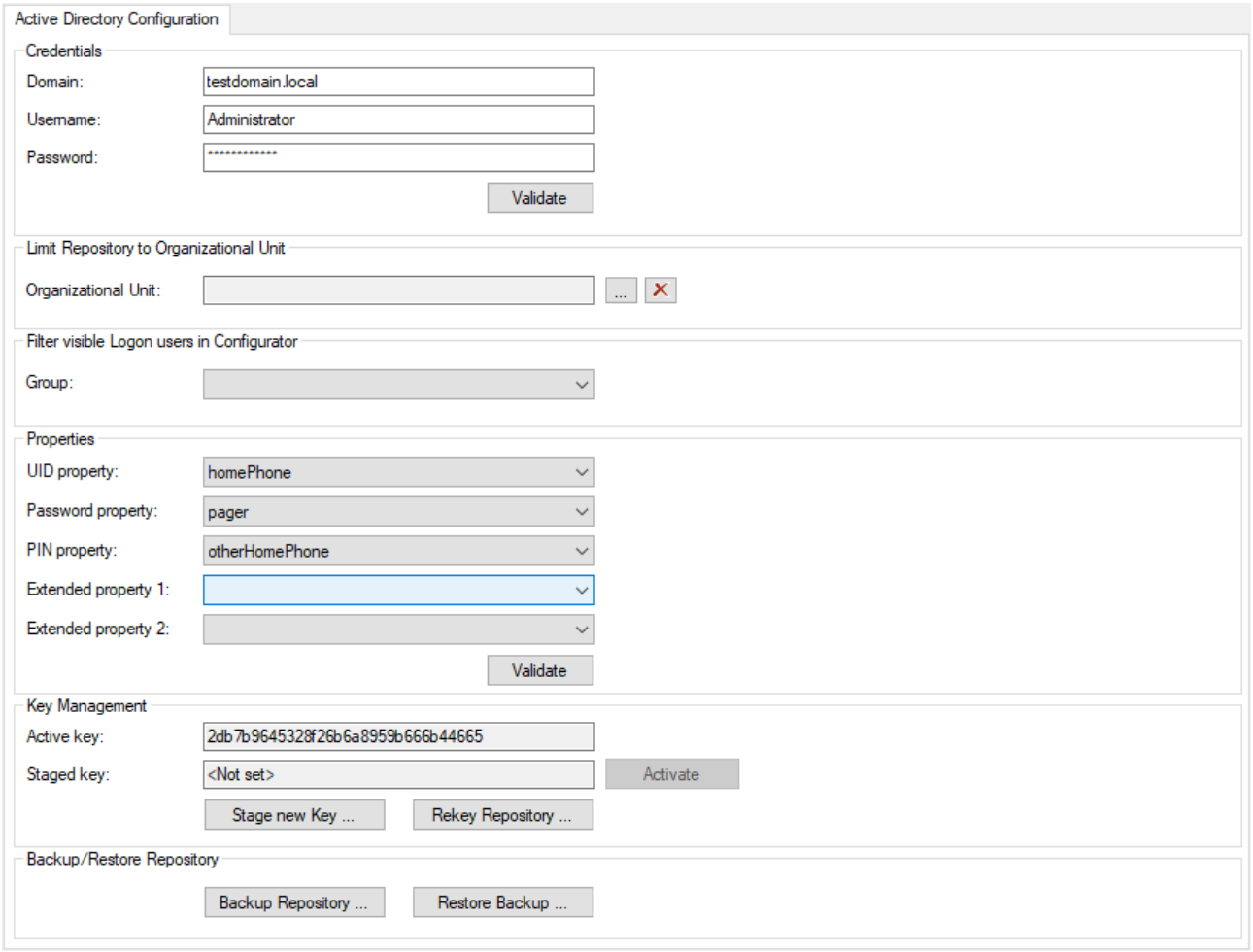
The setting "Poll Cycle in ms" defines the cycle in milliseconds in which the reader is queried.

In the section "Test Reader" the reader can be tested for correct function. To do this, press the "Connect" button to connect to the reader. If you then insert a Euchner Key into the reader, the UID is displayed in the "Current UID" field.

So that the Euchner EKS reader can be used, you must now define it as the standard logon device. To do this, right-click the element "Euchner EKS USB Reader" under "Logon Devices" in the tree structure and click on the entry "Set as default".

3.2.12 Configuration of an active directory

The settings for using active directory (i.e. a domain controller) are configured by using the element “Active Directory” within the section “User Repositories”.



The section “Credentials” is used to configure the credentials that are required for the domain:

- Domain:
  Name of the domain that is to be used as a user repository in PM-LOGON.

- Username / Password:
  Name and password of the user that is used by the PM-LOGON Configurator in order to assign RFID cards to domain accounts. The login that is used for this purpose must have the permission to read/write user attributes in the active directory of the domain and to change and to reset passwords.

By clicking the button labeled “Validate” the authentication credentials presented in the corresponding fields are verified against the domain.

In the section **"Limit Repository to Organizational Unit"** the user repository can be limited to one Organizational Unit (OU). Only users who are in this OU or in an OU below it are considered. This means that several user repositories (e.g. for different locations/companies) can be set up within the same domain.

The section **“Filter visible Logon users in Configurator”** can be used to filter the users read from the domain controller for members of a specific user group. This is especially useful for larger domains/OUs where only a dedicated group of users shall be configured for RFID card login.

The section **“Properties”** allows you to define the user attributes in the domain that will be used to store the **UID** of the card and also the encrypted **password** of the user. For this purpose either already existing attributes can be used or alternatively dedicated attributes can be created within the domain controller. The attribute have to be of type “Unicode String”.
In a redundant domain controller setup, make sure that the attributes that are used are marked as being relevant for replication.

The PIN attribute can be used to store an up to 8-digit PIN for the user. This PIN can then be used together with the Windows Logon Provider or transferred via the OPC
And SOAP Access Logon Provider e.g. to an OPC server.

The two attributes **Extended Property 1** and **Extended Property 2** can be used to store additional information about the user in the Active Directory, which can then be written to two linked variables in the Active Directory by PM-LOGON Runtime via the "OPC and SOAP Access" plug-in. The attributes used must also be of the type "DirectoryString".
These two attributes are optional and can be used independently of each other.

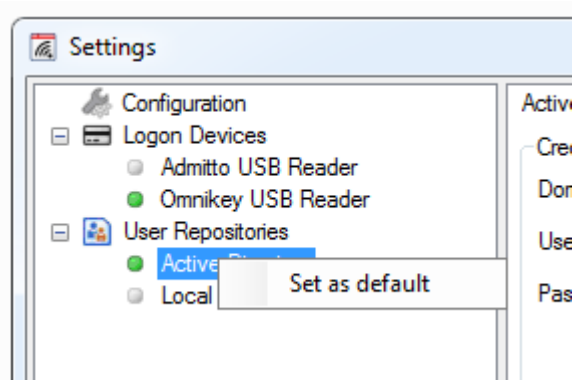
Clicking the button labeled “Validate” checks the selected attributes against the domain controller for validity.

Important:
Make sure that the attributes that are to be used from PM-LOGON are empty before being used for the first time. PM-LOGON cannot differentiate between e.g. a phone number and the unique id of a RFID transponder. Therefore every user with a non-empty UID attribute in the domain will be displayed as being a PM-LOGON user.
Furthermore the data that is eventually already present in the user id and password attributes will be encrypted upon startup of the PM-LOGON Configurator and will therefore not be usable for any other purpose afterwards!

In the section “Key Management”, you can create a user-defined key for encrypting the stored credentials.
For detailed information, please refer to chap. 7 - Key Management.

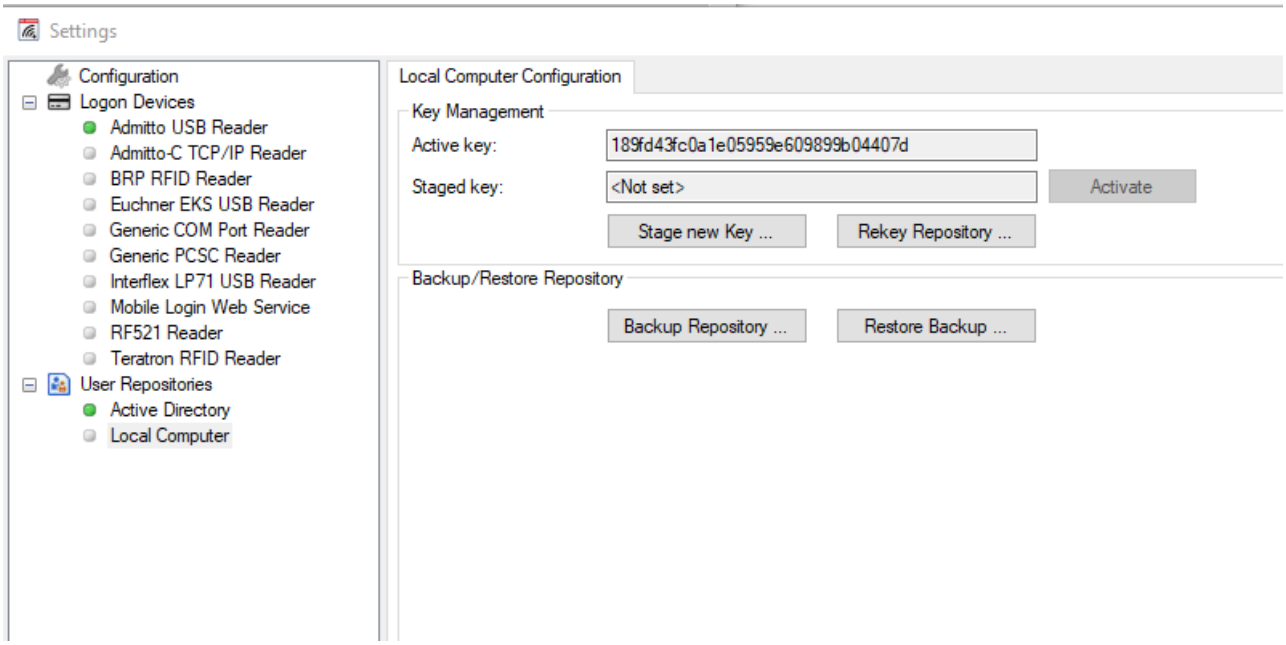
In the section "Backup/Restore Repository", you can back up the stored credentials of the user repositories or restore them from a backup.
Detailed information on this can be found in chap. 8 - Backup/Restore of a user repository.

To specify the Active Directory as the user repository to be used it has to be selected as the standard repository.
This can be done by selecting the command “Set as default” from the context menu. The context menu is opened by right clicking on the element.


Settings
Configuration
Logon Devices
Admitto USB Reader
Omnikey USB Reader
User Repositories
Local
Set as default

3.2.13 Configuration of the local user management

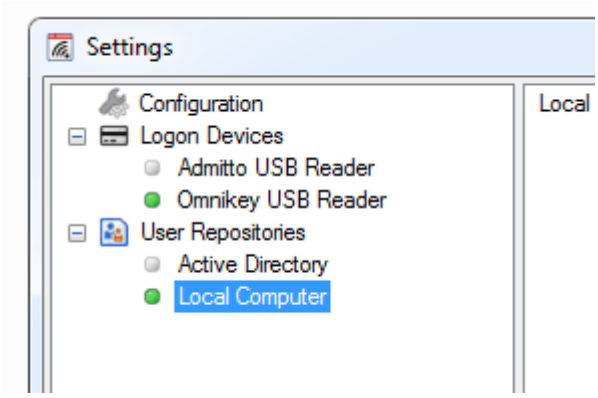
Instead of using active directory as a repository for user management, the user management of the local computer can be used as an alternative.



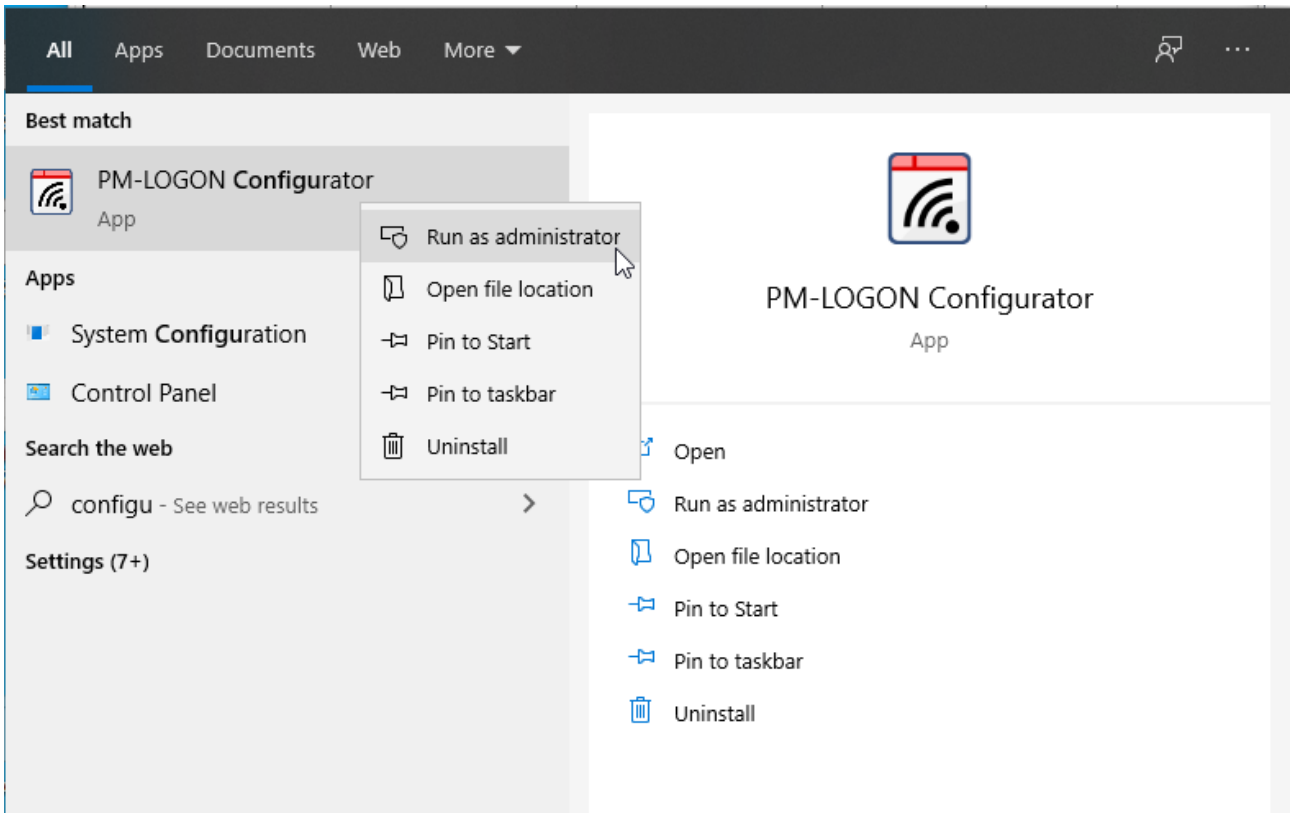
In the section “Key Management”, you can create a user-defined key for encrypting the stored credentials.
For detailed information, please refer to chap. 7 - Key Management.

In the section "Backup/Restore Repository", you can back up the stored credentials of the user repositories or restore them from a backup.
Detailed information on this can be found in chap. 8 - Backup/Restore of a user repository.

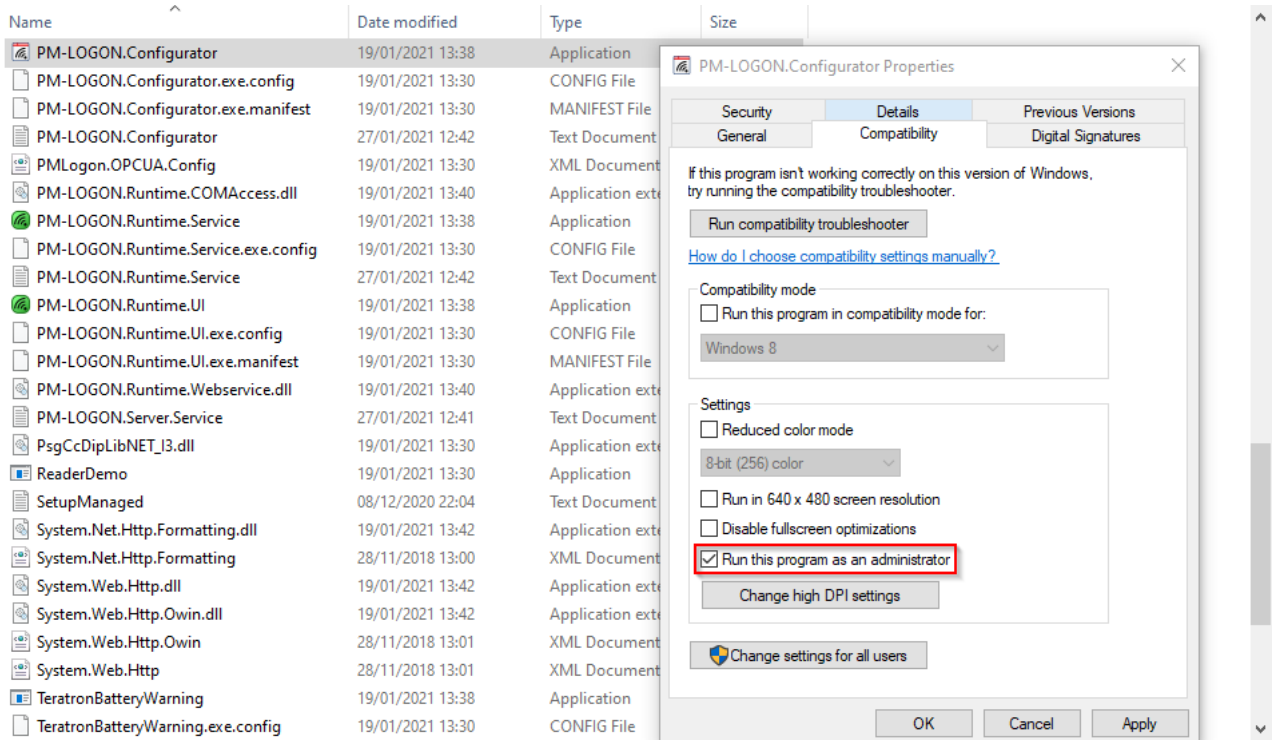
To specify the local user management as the user repository to be used it has to be selected as the standard repository.
This can be done by selecting the command “Set as default” from the context menu. The context menu is opened by right clicking on the element.



Please note that in the case when the local user management is used, the PM-LOGON Configurator must be started with administrative rights. This can be done by right clicking the program and selecting “Run as administrator” from the context menu. E.g. under Windows 10:

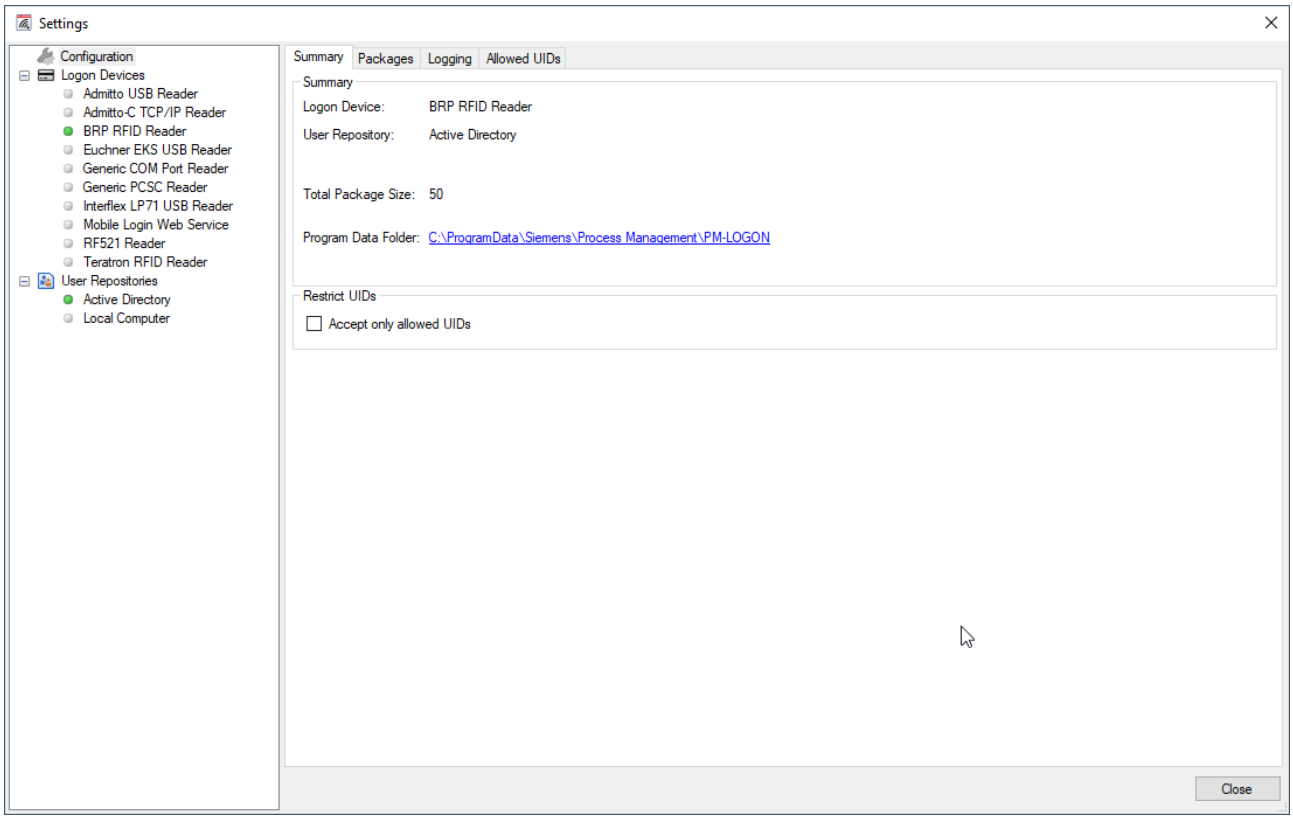

All
Apps
Documents
Web
More
Best match
PM-LOGON Configurator
App
Apps
System Configuration
Control Panel
Search the web
configu - See web results
Settings (7+)
Run as administrator
Open file location
Pin to Start
Pin to taskbar
Uninstall
PM-LOGON Configurator
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar
Uninstall

You can alternatively specify that the application shall always be started with administrative rights. For this purpose navigate to the installation folder (normally “C:\Program Files (x86)\Siemens\PM\PM-LOGON”) and edit the properties of the application:



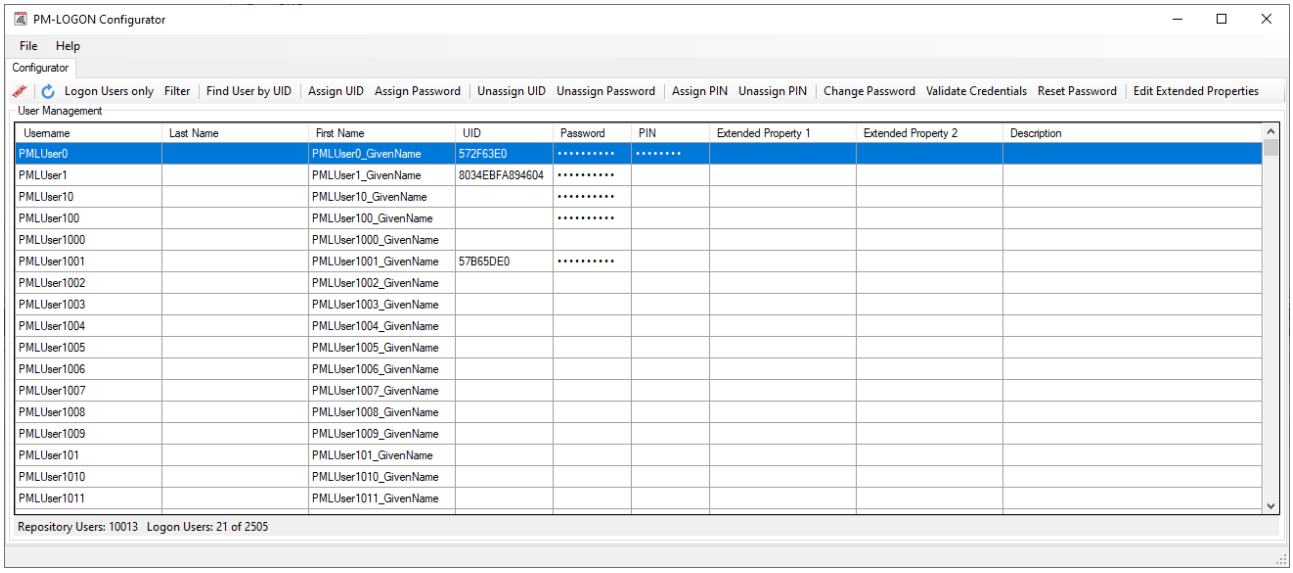
3.2.14 Checking the configuration

Select the summary page of the configuration. On the summary page you should now see the selected reading device and the user repository that is used.
The configuration of the PM-LOGON Configurator is now complete.



Click the “Close” button to leave the configuration dialog.

3.2.15 Operation



After the configuration has been completed, the list of users from the selected repository is displayed.

Operation:

- Assigning a RFID card to a user:
  Select the user from the list and click the button labeled “Assign UID”. After that, present the card of the user to the connected reading device.
  When the card has been recognized and the UID has been read it is assigned to the user and stored in the configured user repository.

  If the user has already been assigned a card or the presented card has been assigned to another user account a warning message will be displayed. You can decide if the configuration should be updated accordingly.

  If there has been no password assigned to the user yet, you can use the button “Assign Password”. The password entered here must match the current login password of the selected user account. After the password has been entered it will be validated against the configured user repository. If the credentials cannot be verified a warning message will be displayed.

  Entering the password here does not change the existing login password of the selected user account.

- Assign password:
  By clicking the “Assign Password” button, the current login password of the selected user account can be entered and then stored within the configured user repository.

- Change Password:
  By clicking the “Change Password” button, the current login password of the selected user account can be changed and in parallel be stored in the configured user repository used for PM-LOGON.

- Assign PIN:
  By clicking the “Change Password” button, an up to 8-digit numeric PIN can be stored for the user.
  If an Active Directory is used as the user repository, the PIN can only be edited if the corresponding attribute has been attached in the configuration of the Active Directory plug-in.

- Validate Credentials:
  With the button labeled “Validate Credentials” you can check if the credentials that have been stored in the user repository of PM-LOGON match the credentials of the selected user account.

- Remove the assignment of a RFID card from a user:
  The button “Unassign UID” removes the linkage between the selected user account and a RFID card.

- Remove password assignment:
  By clicking the button “Unassign Password” the credentials stored in the configured user repository of PM-LOGON are removed. This does **not** change the existing login password of the selected user account.

- Reset password:
  By clicking the button “Reset Password” the logon password of the selected user account as well as the credentials stored within the configured user repository of PM-LOGON can be reset.
  To reset the password, the credentials of a domain administrator must be provided here.

- Remove PIN:
  By clicking the Button “Unassign PIN” the stored PIN for the user can be removed.

- Edit Extended Properties:
  The "Edit Extended Properties" button can be used to store additional information related to the user. This information can only be edited if an Active Directory is used as the user repository and if corresponding attributes are attached in the configuration of the Active Directory plug-in.

Finding user accounts:

- By using the button “Find User by UID” the corresponding user account that has been assigned to a specific card at hand can be determined. Click the button and present the card to the reading device. Once the reader has detected the card and the unique id has been read, the corresponding logon that is associated with that card will be selected. If the card is not associated to any account, a warning message will be displayed.

- Displaying only PM-LOGON relevant users:
  With the button “Logon Users only” the displayed list of user accounts is filtered to show only users that have already been assigned to a RFID card.

- Filtering:
  By using the “Filter” button output to the list can be restricted to show only accounts matching additional criterions.

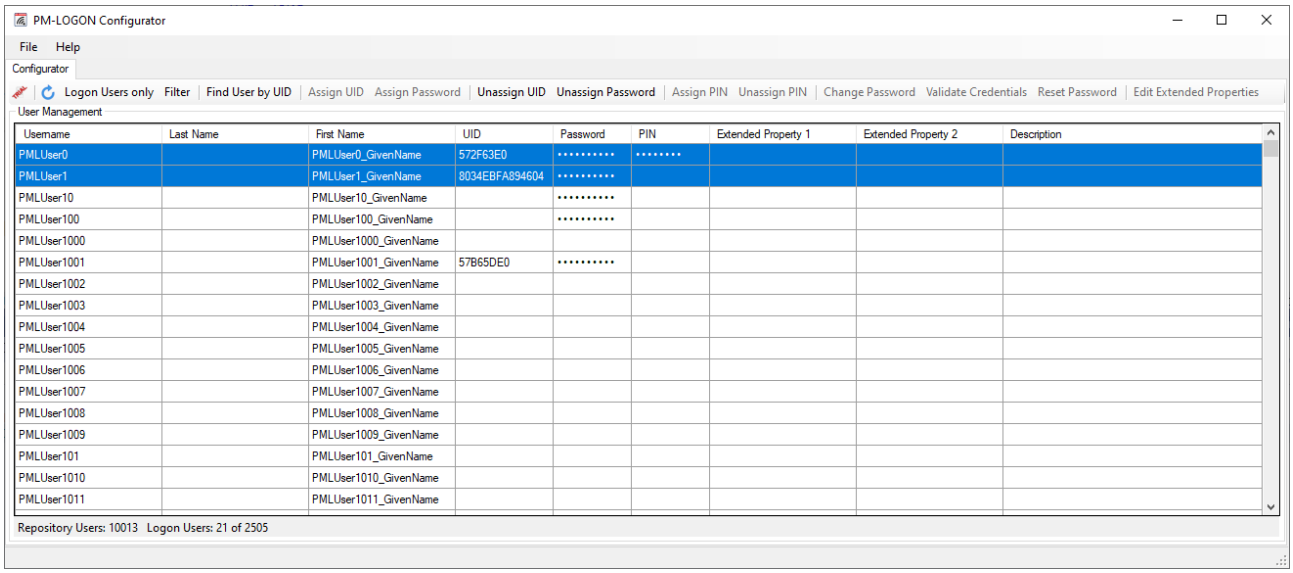
Please note:
When using the repository “Local Computer” administrative privileges are required to perform the following actions:

- Assign UID
- Unassign UID
- Assign Password
- Unassign Password
- Change Password
- Reset Password
- Rekeying
- Backup/Restore user repository

PM-LOGON Configurator has to be started from a user with administrative rights.

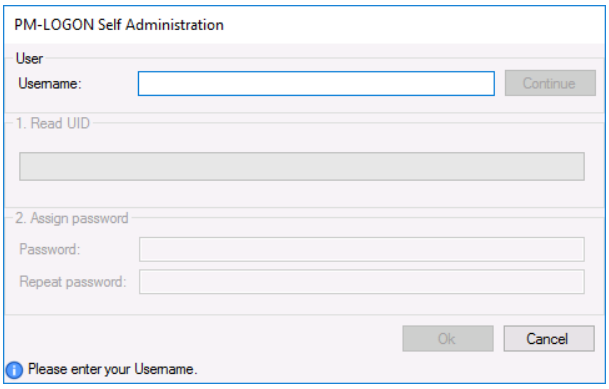
Multiple selections:

Some operations can be performed for multiple users at once. E.g. it is possible to unassign the unique id or the password in the user repository for multiple users in one step.



3.2.16 PM-LOGON Configurator self administration mode

By using the link “PM-LOGON Self Administration” the PM-LOGON Configurator is started in a dedicated mode. This is realized by starting the “PM-LOGON.Configurator.exe” with the command line switch /self.



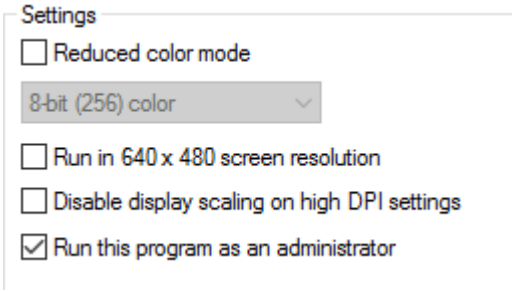
In order to use the self-administration mode the “PM-LOGON Configuration” has to be fully installed and configured (Logon Device, User Repository and User Packages).
As of PM-LOGON V2.0, a separate license is no longer required for the self-administration mode.
If no license for PM-LOGON Configurator has been installed (because only the self-administration mode is to be used, if applicable), PM-LOGON Configurator can be started in **configuration mode** via the command line parameter **"/config**".

In this mode, a user from the currently configured user repository can assign a RFID card that has not yet been used for another account, to its own login.
This also allows setting the current login password of the user account to match the one stored in the PM-LOGON user repository. This assignment is only possible if the password that is entered matches the current login password of the account.
If no action is performed within the dialog for 30 seconds, the application exits automatically without performing any changes.

The user name has to be entered without a domain prefix.

Please note that in the case when the local user management is used, the PM-LOGON Configurator has to be started with administrative rights. This can be done by right clicking the program and selecting “Run as administrator” from the context menu.

You can alternatively specify that the application shall always be started with administrative rights. For this purpose navigate to the installation folder (normally “C:\Program Files (x86)\Siemens\PM\PM-LOGON”) and edit the properties of the application:



If the self administration mode shall be started for a specific login (e.g. the user currently logged in) the name of the requested user can be appended to the command line switch /self (without domain prefix). In this case the user name in the dialog is already filled out and not editable.
Here is an example of the complete command line:

```
"C:\Program Files (x86)\Siemens\PM\PMLOGON\PM-LOGON.Configurator.exe" /self User1
```

Application example:

PM-LOGON Configuratoris started in self administration mode for the currently logged in user from a process screen in WinCC runtime. This can be done by e.g. a button that executes the following script in the OnClick event:

```
Sub OnClick(Byval Item)

   Dim currentUser

   currentUser = HMIRuntime.Tags.Item("@CurrentUser").Read(1)

   Dim objShell

   set objShell = CreateObject("shell.application")

   objShell.ShellExecute """C:\Program Files (x86)\Siemens\PM\PMLOGON\PM-
   LOGON.Configurator.exe""", "/self " + currentUser, "", "open", 1

   setobjShell = nothing

End Sub
```

Additional command line parameters for self-administration mode:

- **/changepassword**
  Using the "Change Password" mode, the user can change his Windows login password and store it in the PM-LOGON user repository at the same time.
  For this, the user must already be assigned a UID in order to be able to identify him uniquely.
  If the mode is to be started for a specific user, his user name can optionally be specified via the username parameter (without domain prefix).
  Here the user name can no longer be changed in the dialog.

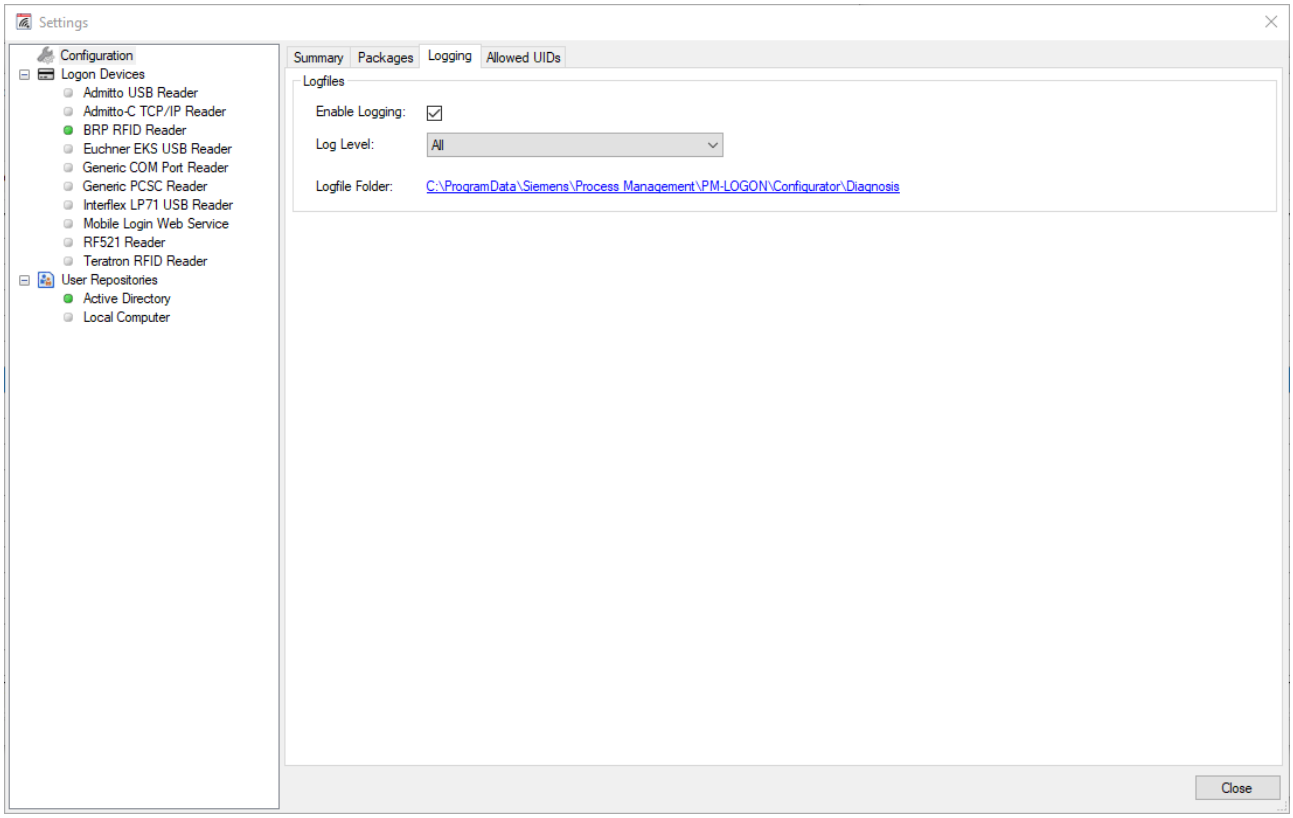
- **/changepin:**
  Via the "Change PIN" mode, the user can change his PIN stored in PM-LOGON.
  For this purpose, the user must already be assigned a UID in order to be able to identify him uniquely.
  If the mode is to be started for a specific user, his user name can optionally be specified via the username parameter (without domain prefix).
  Here the user name can no longer be changed in the dialog.

3.2.17 Diagnostics

Logging of trace information into log files for diagnostic purposes can be configured on the page “Logging” within the configuration section (“Enable Logging”).
The level of information written to the logs can be defined by selecting one of the options from the drop down list “Log Level”:

- All:
  All messages
- Error:
  Only errors
- Warning:
  Warnings and errors
- Information:
  Information messages, warnings and errors
- Verbose:
  Detail information, Information messages, warnings and errors

File logging should only be activated for diagnosing problems and should not be activated permanently. The size of the log files is limited to 10MB and the log files are automatically deleted after 7 days. The folder where the log files are stored can be opened by clicking the link to the right of the label “Logfile Folder”.



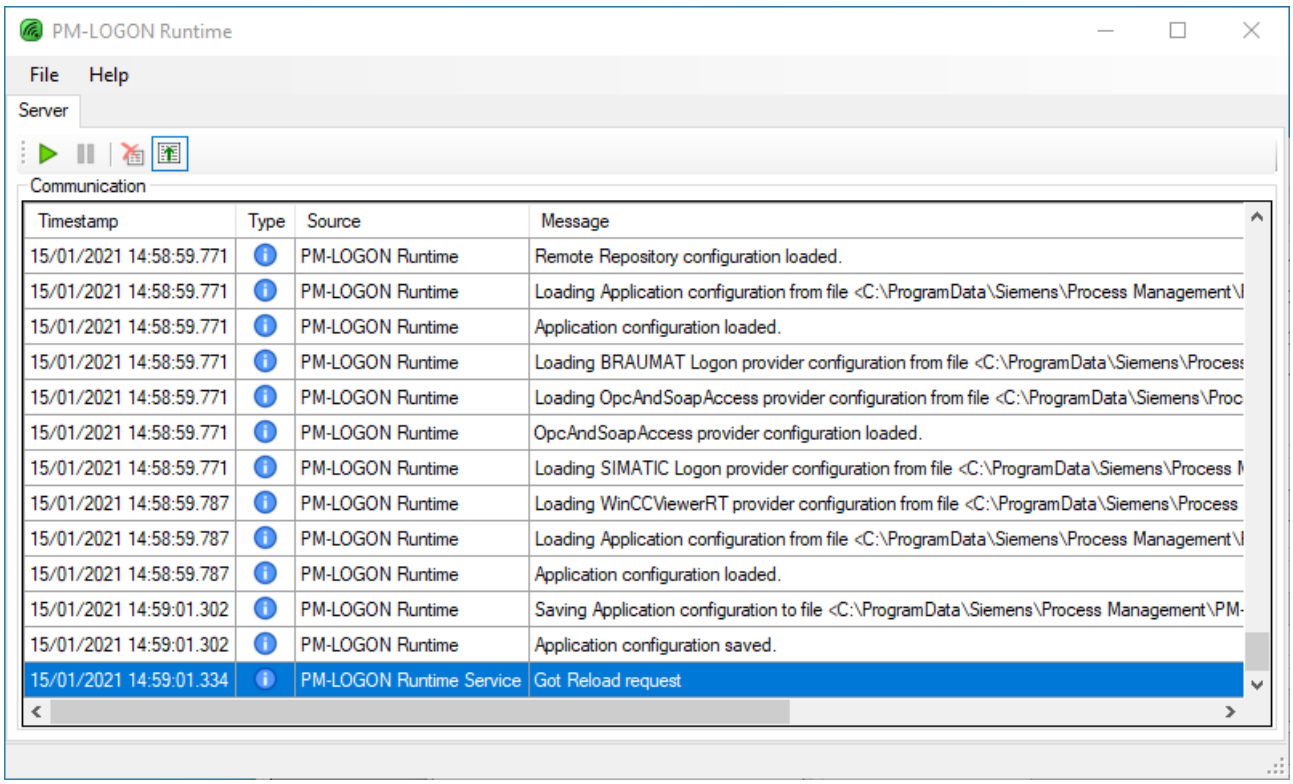
4 PM-LOGON Runtime

4.1 Introduction

PM-LOGON Runtime reads the RFID card entering the detection range of the reading device determines the associated user login by querying the associated user account from the configured user repository and finally performs the login operation with the stored credentials.

Additionally, the PM-LOGON Runtime provides a web service, which can be used as a “User Repository” (Remote PM-LOGON Runtime) for a remote PM-LOGON Runtime. This is required in the case when the PM-LOGON Runtime for Panels is used to relay the information sent from the comfort panels.

4.2 Application window

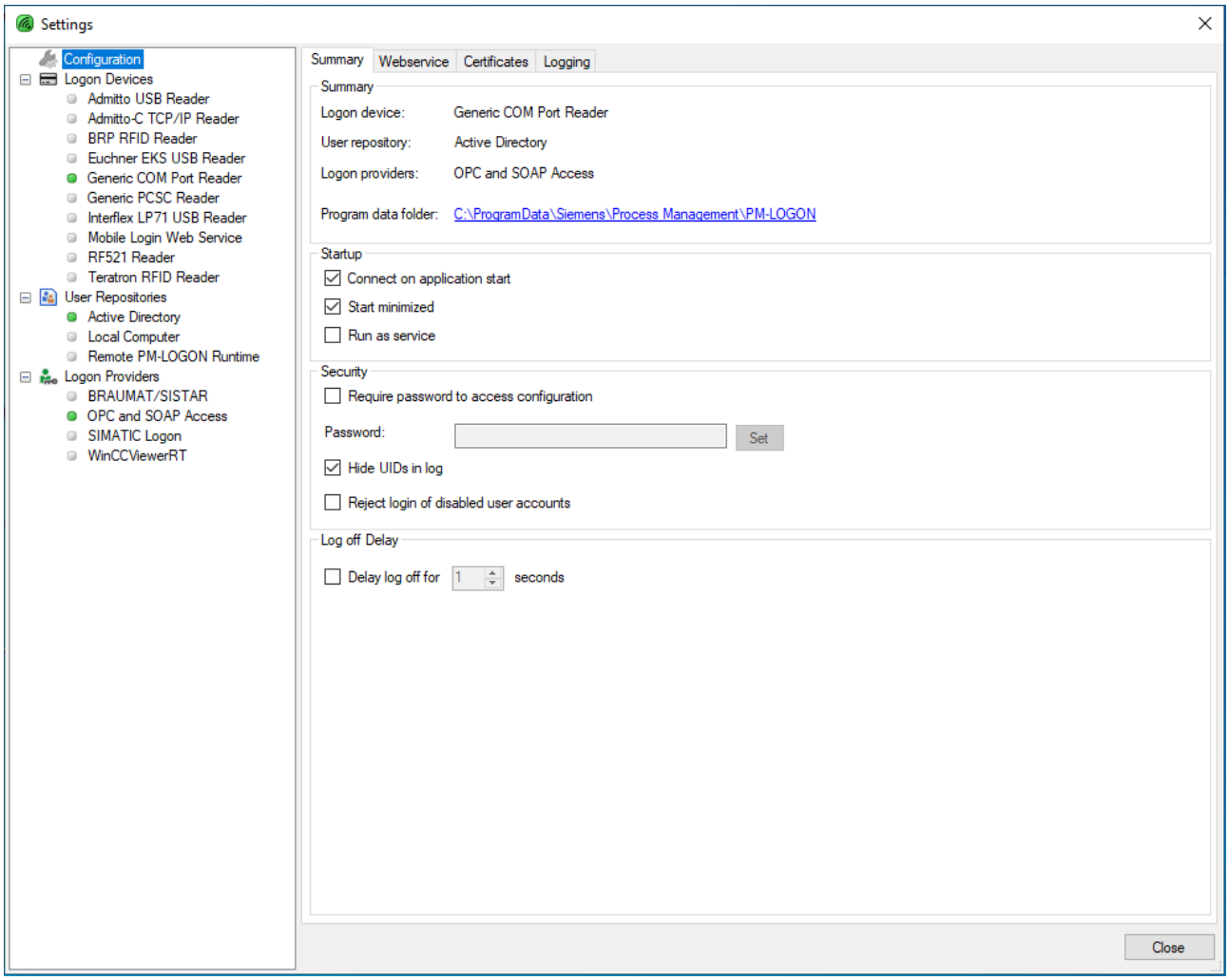


The main window displays information about current activities performed by the PM-LOGON Runtime. By using the buttons on the toolbar, the runtime can be activated (“Start”), deactivated (“Stop”) and the list of activities can be cleared (“Clear Log”).
The AutoScroll-function can be activated/deactivated via the "AutoScroll" button.

When starting the runtime for the first time, a warning message will be displayed that no default card reader has been configured yet. In this case open the configuration dialog to provide the settings for the operation of the PM-LOGON Runtime.

4.3 Configuration

Open the configuration of the PM-LOGON Runtime with the menu command File->Configuration. The configuration dialog of the PM-LOGON Runtime will be displayed.



The tree view on the left side allows you to navigate over the different configuration sections.

The element labeled “Configuration” opens the general configuration settings of PM-LOGON Runtime.

The section “Summary” in the tab “Summary” displays the logon device, the user repository and the logon provider that is currently being used by PM-LOGON Runtime.

The link allows you to navigate to the path in the file system where the configuration data is stored.

The section “Startup” defines if PM-LOGON Runtime shall automatically connect to the reading device, the user repository and the login provider upon application start (“Connect on application start”). The setting “Start minimized” defines if PM-LOGON Runtime is started minimized and displayed only on the system tray. The main window of PM-LOGON Runtime is restored by double clicking the tray icon.

The checkbox "Run as a service" can be used to specify whether you want to run PM-LOGON Runtime as an operating system service or interactively.

The configuration of PM-LOGON Runtime can be protected against unauthorized access. If the checkbox “Require password to access configuration” is activated, a password can be specified that is required to access the configuration. The password can be changed by using the button “Set”.

Since UIDs read from the RFID cards may be information that should be protected against unauthorized access the UIDs can be hidden from the diagnostic logs by activating the option “Hide UIDs in log”.

If the checkbox "Reject disabled users" is activated, PM-LOGON will reject the login for user accounts which are disabled in the user repository (e.g., Active Directory).

The "Delay log off for x seconds" setting in the "Log off Delay" section can be used to delay the logoff for up to 15 seconds after removing the card from the reader field. Prerequisite for this is that the option "Log off current user" has been selected as "Log off behavior" in the respective logon provider and the reader used signals the removal of the card from the field to PM-LOGON. If the card leaves the reader field and returns within the set time period, the logoff process is aborted and the previously logged in user remains logged in. If another card is brought into the field within the set period after leaving the reader field of a card, the log off process is also aborted and the user assigned to this card is logged in.

The “Webservice” tab allows the configuration of the PM-LOGON Runtime web service, which is especially required if the PM-LOGON Runtime for Panels is used to provide login information on panels.

The "Certificates" tab allows you to manage the security certificates which PM-LOGON uses for secure data exchange with OPC UA servers and other PM-LOGON Runtime instances.

Logging of trace information into log files for diagnostic purposes can be configured on the page “Logging” within the configuration section.

The element “Logon Devices” navigates to an overview of all currently supported login devices. Underneath this element the configuration sections for the individual login devices are located.

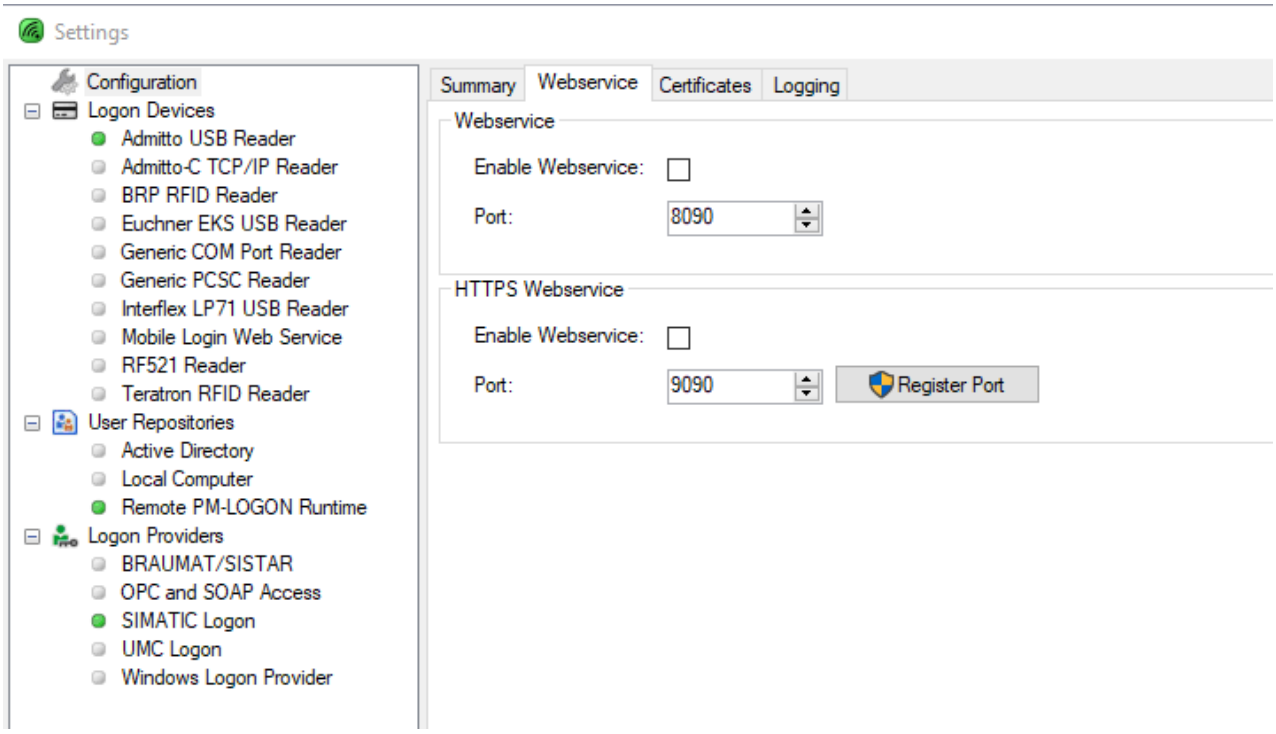
The element “User Repositories” navigates to the configuration section for the supported user management systems. Underneath this element the configuration sections for the individual user management repositories are located.

The "Logon Providers" element takes you to the overview of the supported logon services; below this are the configuration sections of the listed logon services.

PM-LOGON has a plug-in concept that allows the system to be expanded in order to support additional reading devices and user repositories.

4.3.1 Configuration of the PM-LOGON Runtime Web Service

The PM-LOGON Runtime Web Service is required if the respective PM-LOGON Runtime instance is operated together with other remote PM-LOGON Runtime or PM-LOGON Runtime for Panels instances.



PM-LOGON Runtime provides both a HTTP and a HTTPS web service.
PM-LOGON for Panels instances always use the HTTP web service, only HTTPS web service is allowed for connection between PM-LOGON runtime and server instances.

To establish an HTTPS connection, a port must be reserved to associate it with the PM-LOGON application certificate. The default port is already reserved by the installation of PM-LOGON Runtime, so that the port only needs to be reserved via the "Register Port" button when a change is made.

Activate the respective web service via the corresponding checkbox.

4.3.2 User specific configuration of the PM-LOGON Runtime

The configuration of the PM-LOGON Runtime is user independent by default and therefore valid for all users on the system. It is stored in the folder "%ProgramData%\Siemens\Process Management\PM-LOGON\Runtime".
By using a command line parameter on the "PM-LOGON.Runtime.exe" the configuration can also be stored user specific.
To store the configuration user specific call the PM-LOGON.Runtime.exe with the parameter „/userconf".
The configuration files of PM-LOGON Runtime will then be stored in the local user profile of the current Windows user.

4.3.3 Configuration of the SIMATIC RF1040R/RF1060R/RF1070R RFID card reader

See section 3.2.3.

4.3.4 Configuration of the Admitto USB reader

See section 3.2.4.

4.3.5 Configuration of the Admitto-C TCP/IP reader

See section 3.2.5.

4.3.6 Configuration of a generic COM port reader

See section 3.2.6.

4.3.7 Configuration of a generic PCSC card reader

See section 3.2.7.

4.3.8 Configuration of the Mobile Login Web Service

See section **Fehler! Verweisquelle konnte nicht gefunden werden.**.

4.3.9 Configuration of a RF521 RFID reader

See section 3.2.9.

4.3.10 Configuration of a Teratron RFID reader

See section 3.2.10.

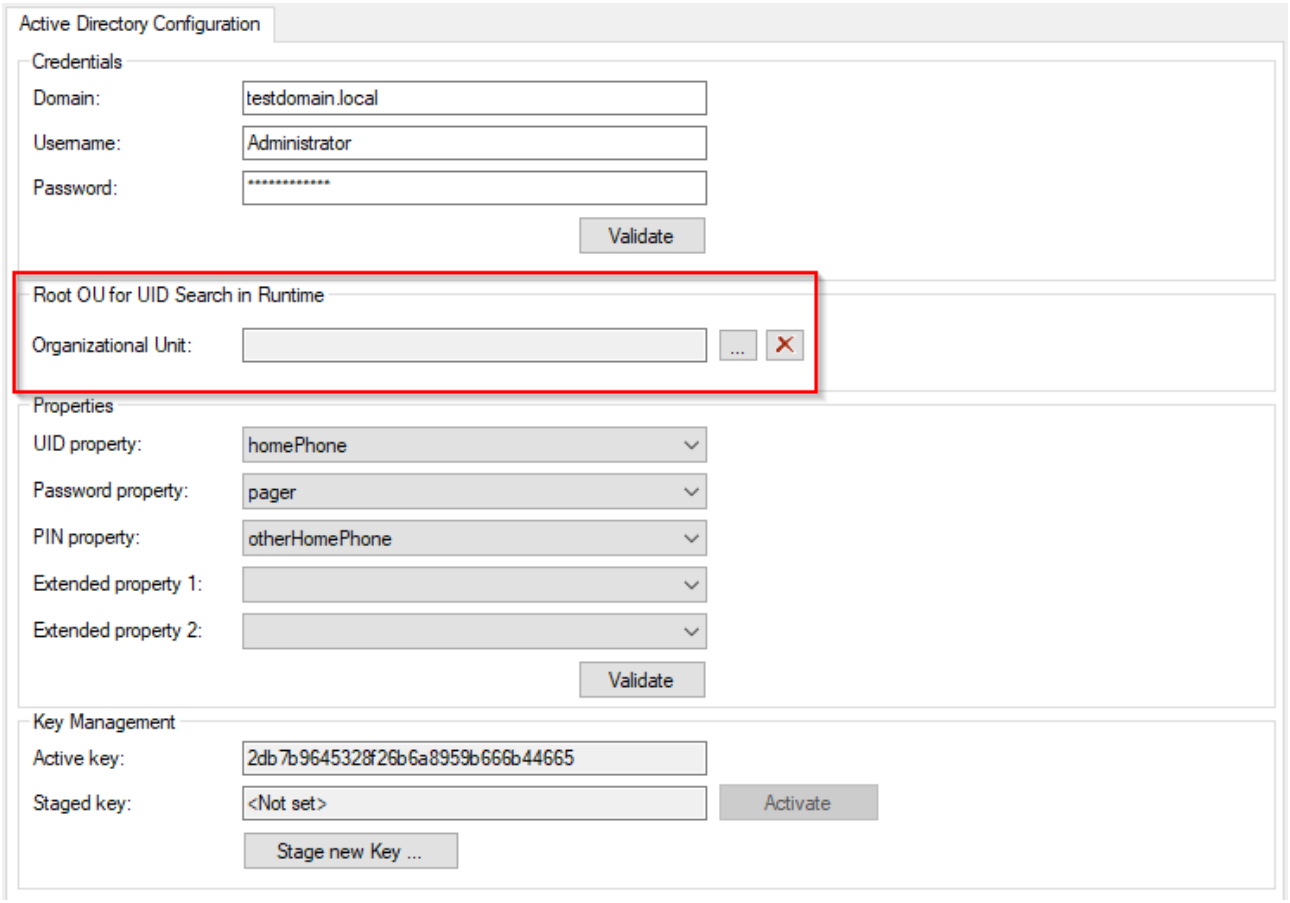
4.3.11 Configuration of an Euchner EKS USB Reader

See section 3.2.11.

4.3.12 Configuration of an Active Directory

See section 3.2.12.

Optimization of query performance in large Active Directory structures:
Large Active Directory structures with many users can lead to slower performance when determining the domain user assigned to a UID.
In order to optimize the query, the search within the Active Directory can be restricted to one Organizational Unit. The PM-LOGON Runtime then restricts the search for the user belonging to a UID to the specified Organizational Unit and the Organizational Units below it.
To do this, select the corresponding Organizational Unit in the "Root OU for UID Search in Runtime" section of the Active Directory Repository configuration.



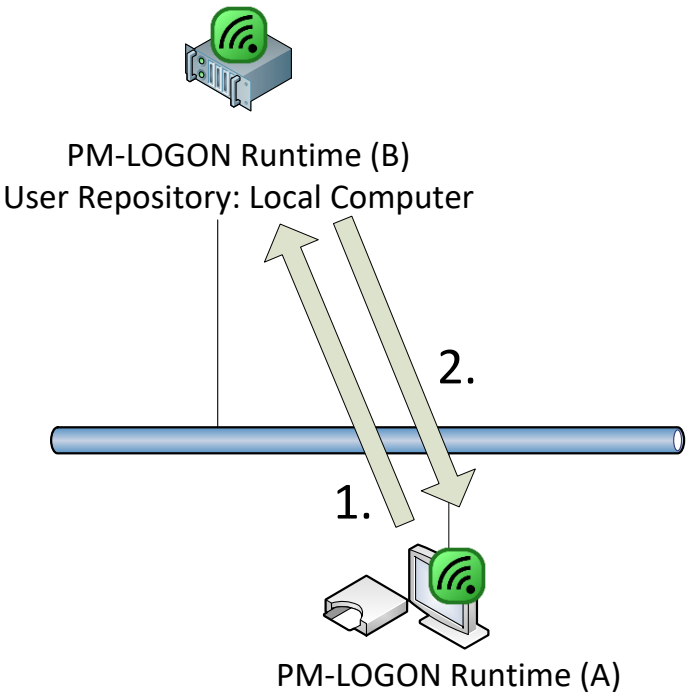
4.3.13 Configuration of the local user management

See section 3.2.13.

4.3.14 Configuration of a remote PM-LOGON runtime

If a local user management is used, access from a remote computer is not directly possible. In this case however, the user repository “Remote PM-LOGON Runtime” can be used.

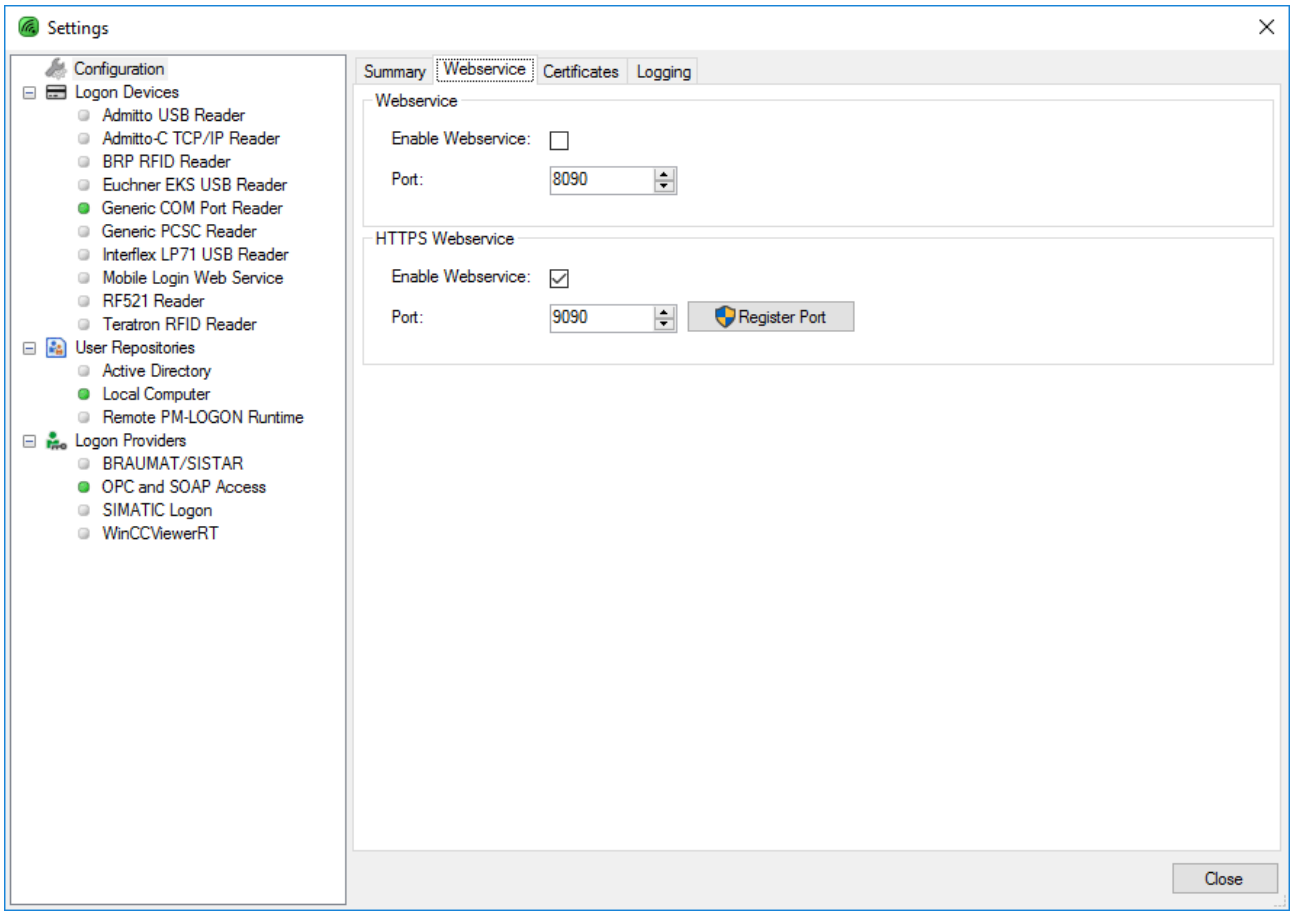
The working principle is as follows:



If a RFID card is detected at PM-LOGON Runtime (A) a remote PM-LOGON Runtime (B) is being queried by utilizing the integrated web service in order to retrieve the user information from the local user management. This information is then relayed back to the querying PM-LOGON Runtime (A) and is then used on this computer for the corresponding logon provider (e.g. SIMATIC Logon).The transfer of the password is done in an encrypted format.

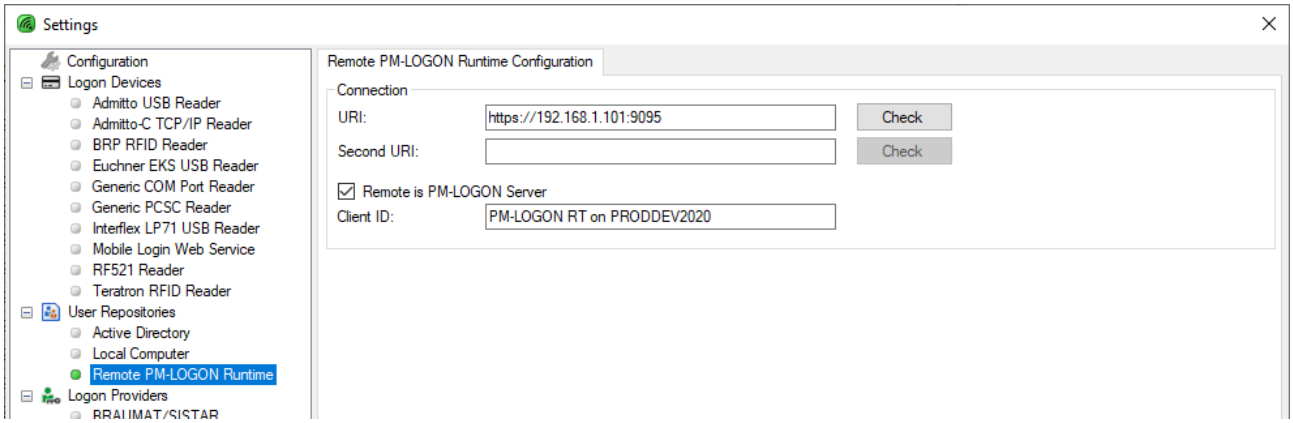
In the configuration of the “User Repository” to use at PM-LOGON Runtime (A) the web service that should be contacted has to be addressed by entering the URI of the service in the form “https://<IP/Name>:<Port>”. The default port number is 8090.

The HTTPS web service on PM-LOGON Runtime (B) must activated. As of PM-LOGON V2.0, the Remote Repository Plugin communicates exclusively with the HTTPS web service of the remote PM-LOGON Runtime. The HTTP web service is no longer supported for communication between two PM-LOGON Runtime instances.



The HTTPS connection is secured via security certificates. For this, the PM-LOGON Runtime (A) and (B) must exchange their security certificates.
For this, first make sure that the HTTPS web service of the PM-LOGON Runtime (B) is activated and the specified port has been registered.

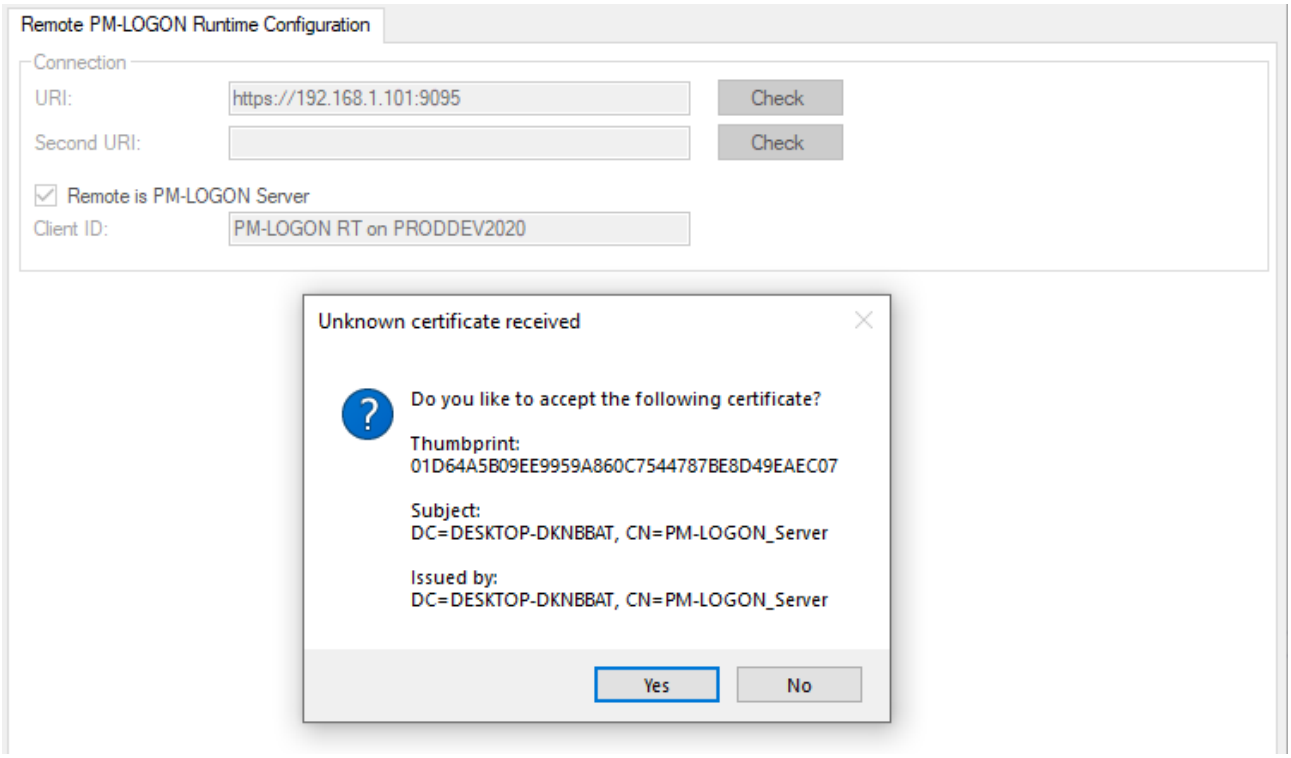
Then configure the URI of the HTTPS web service of Runtime (B) at PM-LOGON Runtime (A). Make sure that you have correctly specified the protocol https:// in the URI.



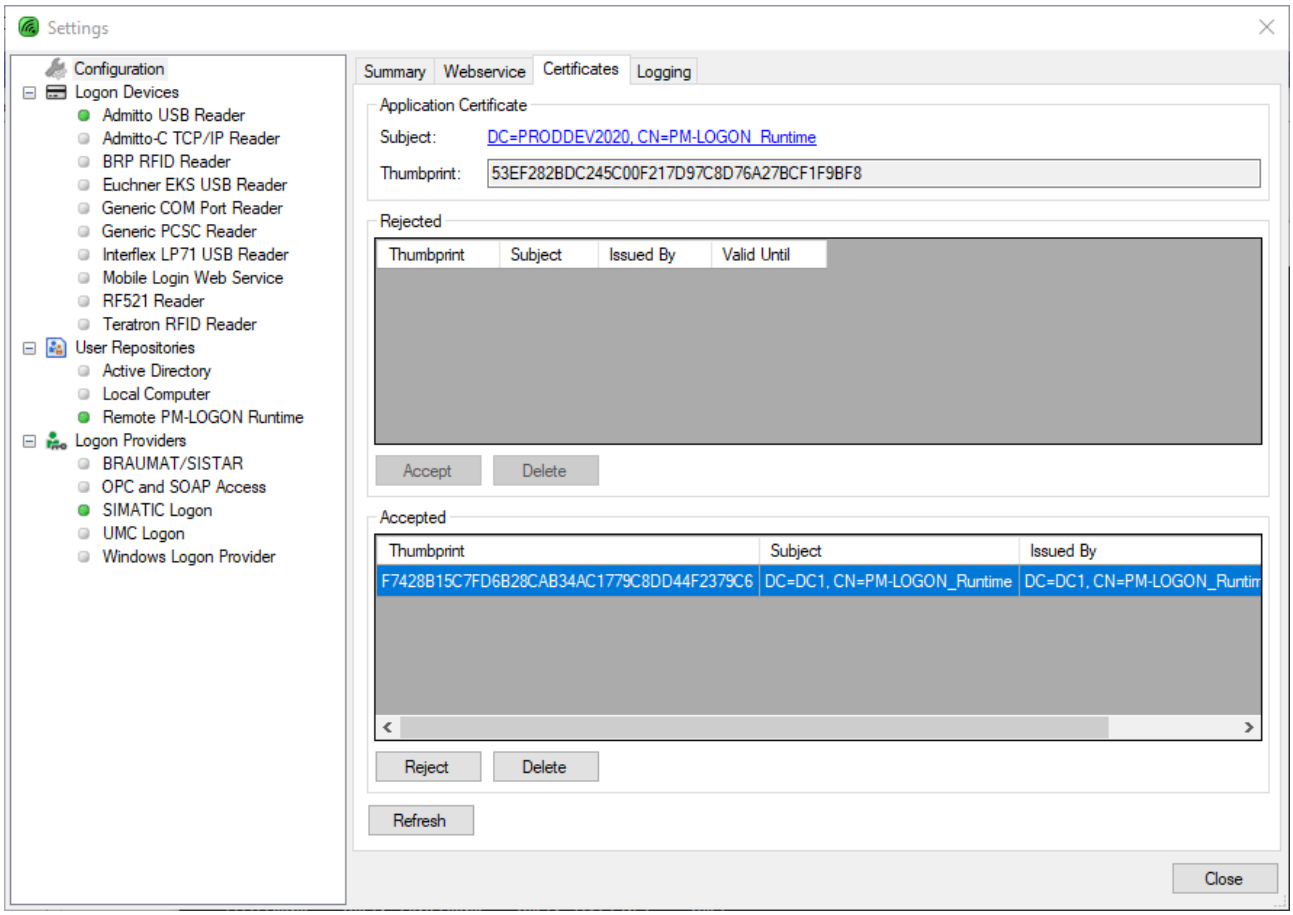
If the remote PM-LOGON runtime is a PM-LOGON server, you must check the "Remote is PM-LOGON Server" checkbox. Assign a unique name for the client.

Then, press the "Check" button.

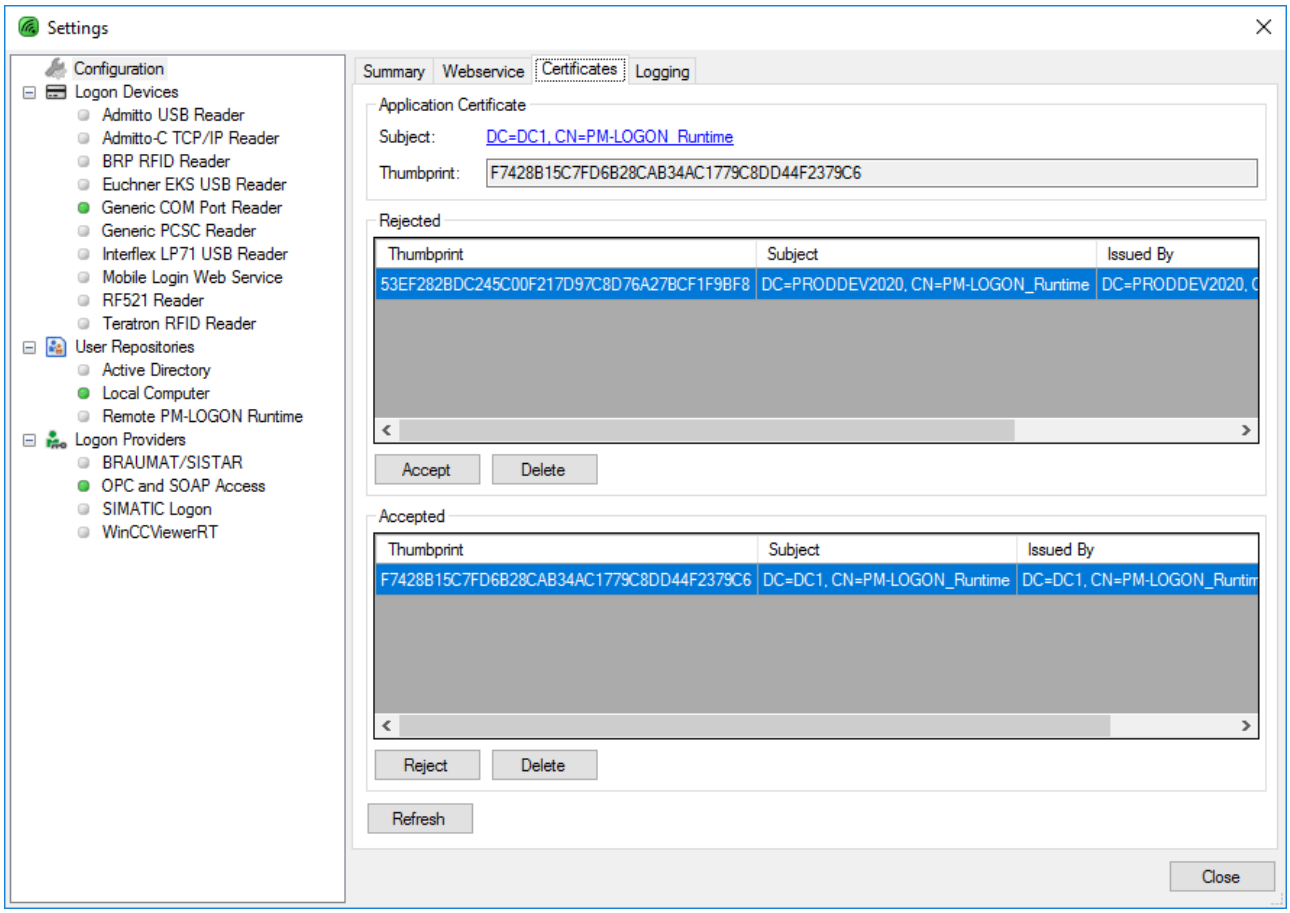
You will now be asked if you want to accept the security certificate of the web service of PM-LOGON Runtime (B).



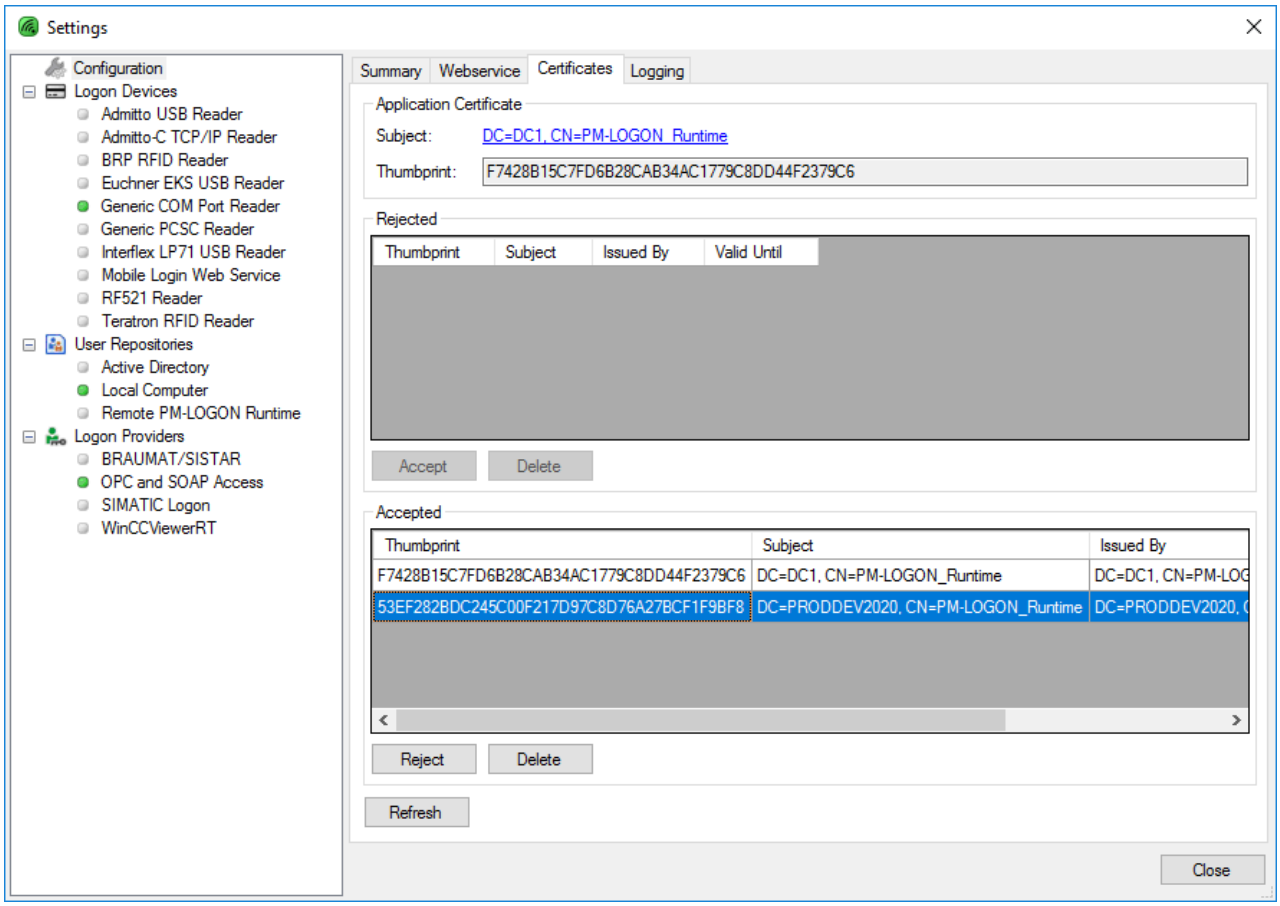
After you have checked the information and accepted the certificate, it will be displayed in the list of accepted certificates in the "Certificates" tab of PM-LOGON Runtime.



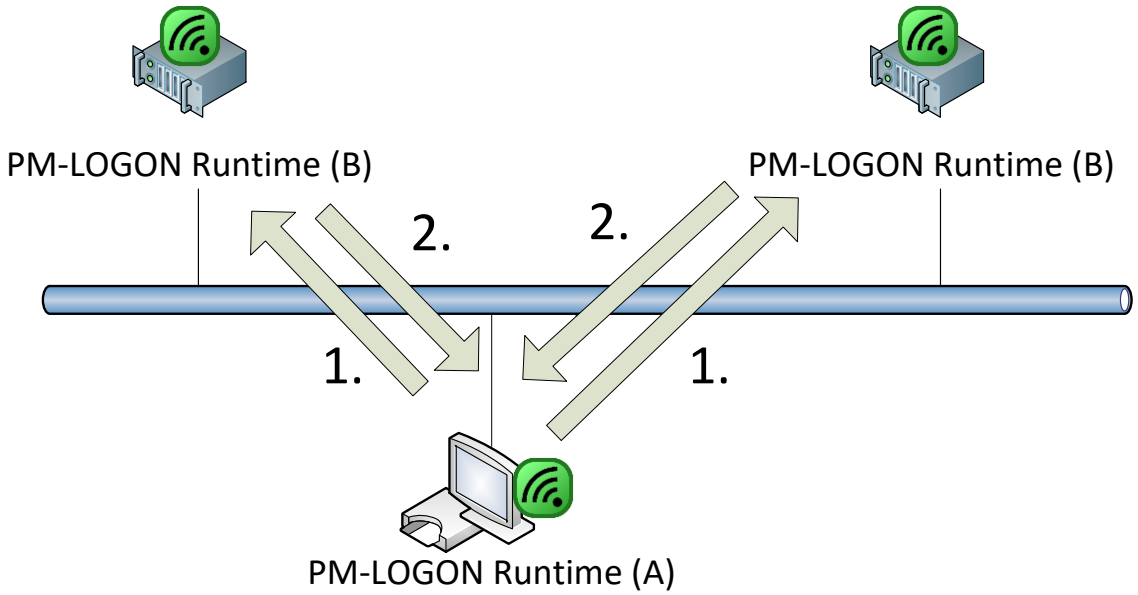
Now also make sure that the certificate of PM-LOGON Runtime (B) is accepted in the certificate management of PM-LOGON Runtime (A).



To do this, select the corresponding certificate in the "Rejected" list and press the "Accept" button. The certificate will be displayed in the "Accepted" list.



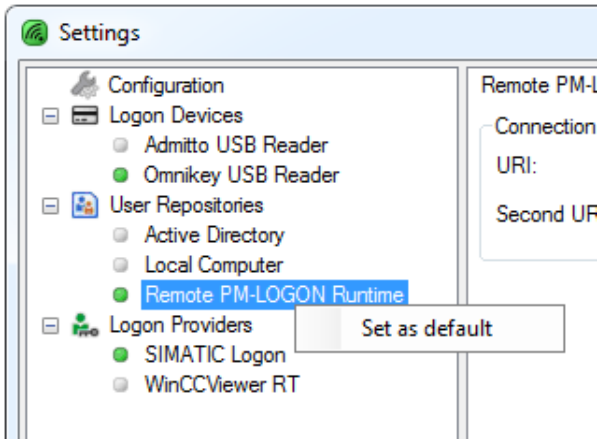
For redundant operation a second PM-LOGON Runtime (B) can be configured by entering a “Second URI” which will be simultaneously queried for logon credentials.



PM-LOGON Runtime (A) sends the request in parallel to both remote PM-LOGON Runtime (B) instances and uses the response that is coming back first. The second response is discarded.

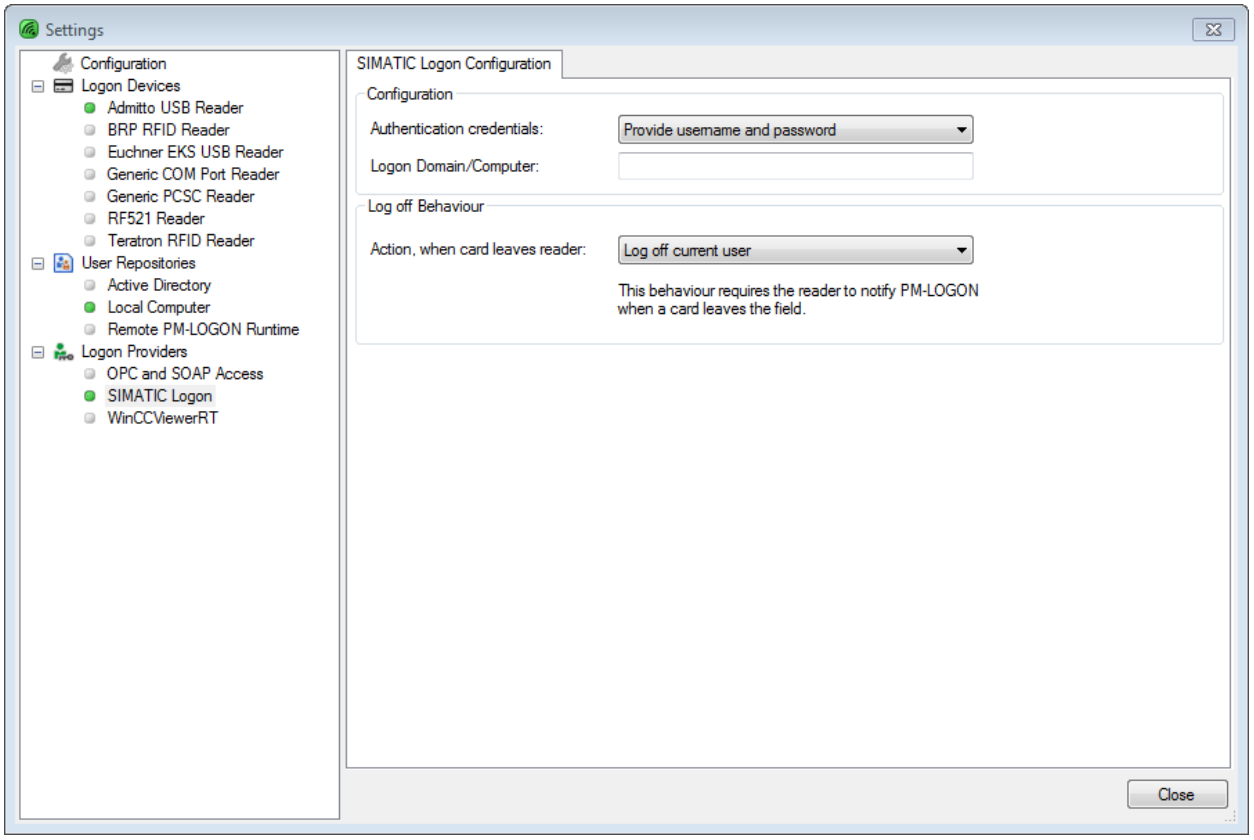
In this scenario if the local user management on both PM-LOGON Runtime (B) instances is used, those user repositories have to be kept in sync manually.

In order to utilize a remote PM-LOGON Runtime as the standard user repository it has to be activated with the “Set as default” command from the context menu.



4.3.15 Configuration of the SIMATIC Logon provider

The element “SIMATIC Logon” in the category “Logon Providers” is used to configure SIMATIC Logon as the service that performs the login operation.
This Plugin can only be used and configured when running PM-LOGON Runtime in Interactive Mode and not running as a service.



If a RFID card is detected, the login credentials (i.e. username and password) of the user that has been assigned to the detected card UID are queried from the configured “User Repository”. If the user has been registered with the appropriate password, the login information is handed over to SIMATIC Logon.

The way the login operation is to be executed can be specified by selecting one of the options under “Authentication credentials”:

- None
  The login dialog will be displayed.

- Provide username
  The login dialog will be displayed and the user name has been prefilled from the information associated with the detected RFID card. The user still has to enter the password.

- Provide username and password
  The login dialog is not displayed and a silent login is performed directly in SIMATIC Logon.

  Additionally in the field "Logon Domain/Computer" the computer name or the domain name must be entered that SIMATIC Logon is authenticating the user against. If the field is left empty, the local computer will be assumed.

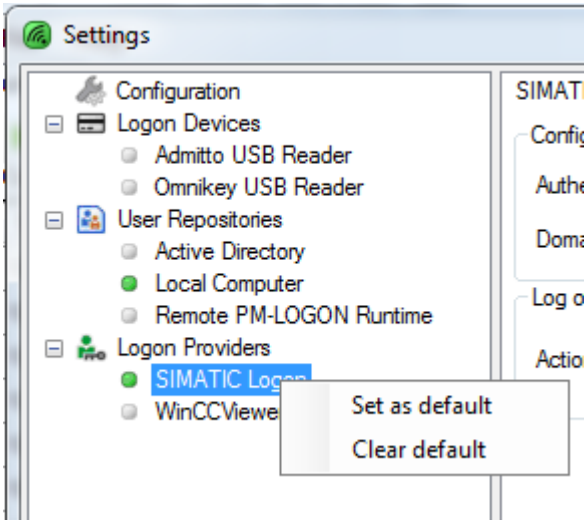
In the case that the RFID card leaves the reader an action can be defined how PM-LOGON should react in this case. The following alternatives are currently available:

- Do nothing
  A user that has been logged in remains logged in.

- Log off current user
  The current user is logged off.

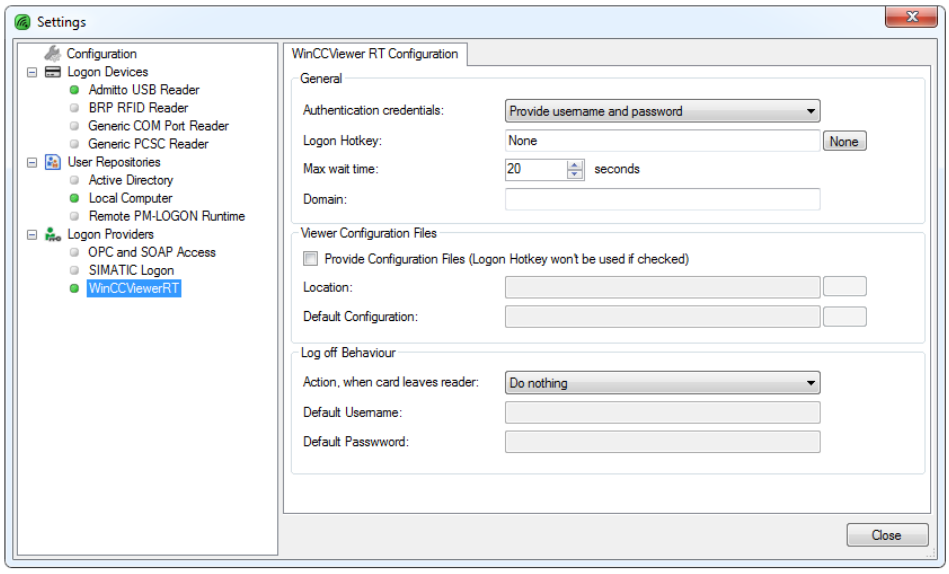
Please note that not all card reading devices provide a notification when a RFID card has left the reader detection range.

In order to use SIMATIC Logon as the logon provider service it has to be activated by selecting it as the standard “Logon Provider”. This is done by using the “Set as default” command from the context menu.


Settings
Configuration
Logon Devices
Admitto USB Reader
Omnikey USB Reader
User Repositories
Active Directory
Local Computer
Remote PM-LOGON Runtime
Logon Providers
SIMATIC Logon
WinCCViewe
Set as default
Clear default

4.3.16 Configuration of the WinCCViewerRT provider

If an automated login should be performed for the SIMATIC WinCC Web Navigator Client by using the “WinCCViewerRT.exe” application, the “Logon Provider” “WinCCViewerRT” needs to be selected in PM-LOGON Runtime.
This Plugin can only be used and configured when running PM-LOGON Runtime in Interactive Mode and not running as a service.



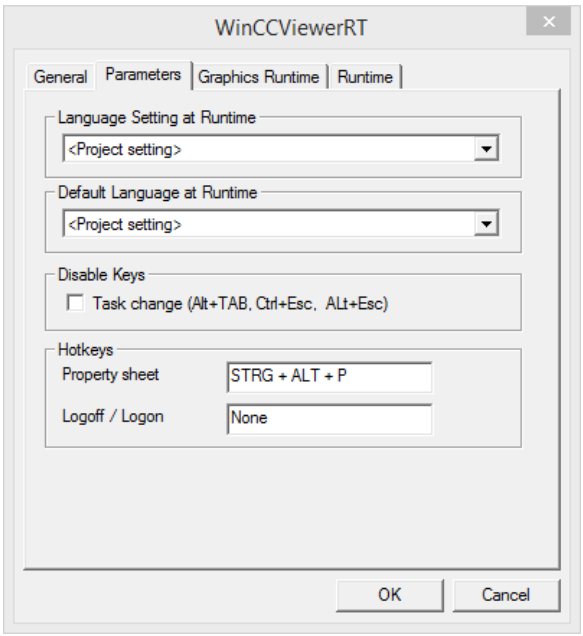
If a RFID card is detected, the login credentials (i.e. username and password) of the user that has been assigned to the detected card UID are queried from the configured “User Repository”. If the user has been registered with the appropriate password, the application “WinCCViewerRT.exe” is started.
After the application has started, the login dialog will be displayed. The further course of action depends on the setting that has been configured for the option “Authentication credentials”:

- None
  The login dialog is displayed. If a user has already been logged in, an implicit log off is performed. Username and password have to be entered manually

- Provide username
  The login dialog will be displayed and the user name has been prefilled from the information associated with the detected RFID card. The user still has to enter the password.

- Provide username and password
  The login dialog will be displayed and the user name has been prefilled from the information associated with the detected RFID card. The password will also automatically be filled in and the dialog will be closed as if the user would have entered the credentials manually and confirmed by clicking OK.

By defining a “Logon Hotkey” an eventually already running instance of “WinCCViewerRT.exe” can be instructed to show its login dialog. This hotkey must then match the hotkey that has been defined within the “WinCCViewerRT” configuration e.g.:



The hotkey is defined in the same way a hotkey can be defined in “WinCCViewerRT.exe”: Position the input focus in the hotkey field and press the key combination you want to use as the hotkey. If the hotkey definition is to be removed, you can use the button labeled “None” to the right of the field.

The setting “Max wait time” defines the maximum delay that PM-LOGON waits for the automated operation of “WinCCViewerRT.exe” to respond to commands. E.g. if this delay (defined in seconds) has been elapsed after the command to display the login dialog has been sent and no response was detected from the “WinCCViewerRT.exe”, the logon attempt is canceled and an error message is written to the diagnostics log.

If a remote SIMATIC Logon computer is used for the authentication of the WebNavigator users, the user name has to be prefixed with the corresponding domain e.g. “MyDomain\User”. The domain name to be used can be specified in PM-LOGON in the field labeled “Domain”; e.g. in the example above this would be “MyDomain”.

If users shall be using different configurations, the settings under “Viewer Configuration Files” can be used. In this case the option “Provide Configuration Files” needs to be activated and under “Location” a directory on the file system needs to be specified where configuration files for the WinCCViewerRT application are stored. At runtime the PM-LOGON Runtime searches in this directory for a file with the name “<username>.xml”. If such a file is present, it is handed over to “WinCCViewerRT.exe” upon start as a command line switch. If no personalized file is found, the optional configuration file specified under “Default Configuration” is used. If that file is also not found the “WinCCViewerRT.exe” is started without any command line switch.

Please note that when personalized configuration files are used, the usage of hotkeys for switching between different logins is not possible. The reason is that the configuration file is provided to “WinCCViewerRT.exe” only once upon startup on the command line.

WinCCViewerRT stores its standard configuration in the user specific file system folder. On a Windows 7 system e.g. under:

```
C:\Users\<Windows-user>\AppData\LocalLow\Siemens\SIMATIC.WinCC\WebNavigator\Client\WinCCViewerRT.xml
```

If this file is not present, the configuration dialog of “WinCCViewerRT.exe” is displayed upon startup and the settings made in the dialog are stored in a newly created file. If personalized configuration files are to be used, you can utilize this behavior by renaming an eventually existing “WinCCViewerRT.xml” and starting “WinCCViewerRT.exe”. As mentioned before the configuration dialog will be shown and the settings made will be saved in a newly created file. This new file can then be moved into the folder configured under “Location” and renamed to match the name of the user for which it should be used.

Personalized configuration files may also already hold login credentials. In this case no login dialog will be displayed upon startup of “WinCCViewerRT.exe”. If you want to make use of this functionality you should set the option under “Authentication credentials” to “None”, because otherwise PM-LOGON would wait for the login dialog to be displayed.

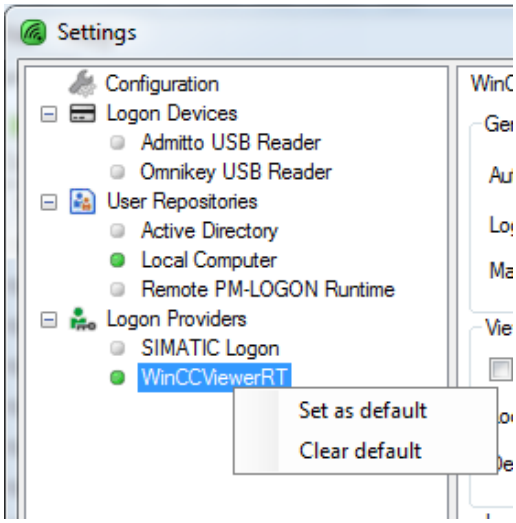
In the case that the RFID card leaves the reader an action can be defined how PM-LOGON should react in this case. The following alternatives are currently available:

- Do nothing
  A user that has been logged in remains logged in.

- Log on default user
  A default user will be logged in who’s login credentials needs to be supplied afterwards. If personalized configuration files are used, a configuration file that matches this user is being used. In this case no login information should be supplied in the default configuration file, since it is always expected for the default user that a login dialog is displayed.

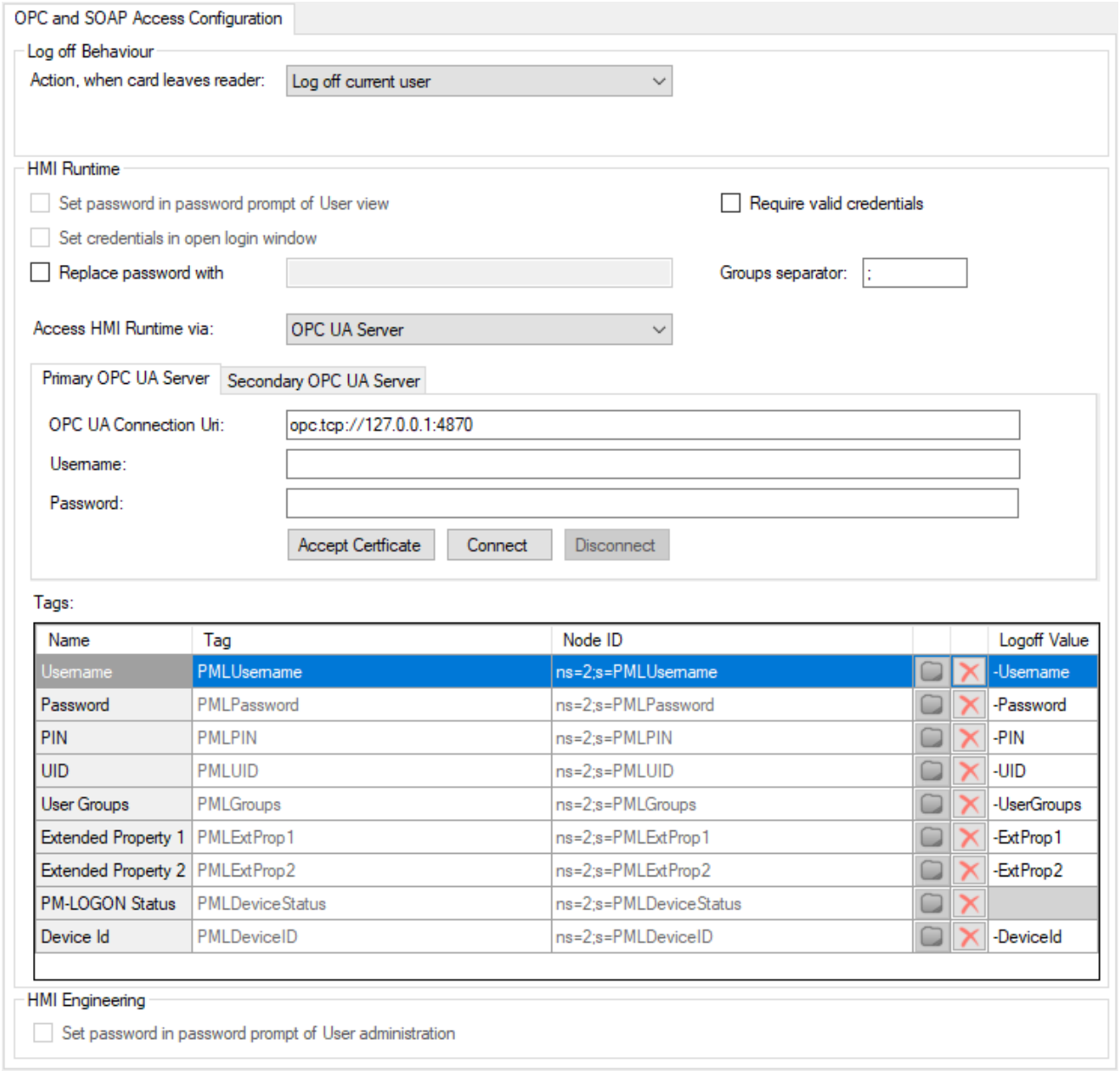
Please note that not all card reading devices provide a notification when a RFID card has left the reader detection range.

In order to use WinCCViewerRT as the logon provider service it has to be activated by selecting it as the standard “Logon Provider”. This is done by using the “Set as default” command from the context menu.



4.3.17 Configuration of the OPC and SOAP access provider

For the Runtime Advanced (PC) “OPC and SOAP access” can be used as the login provider.



For this configuration two tags of type string are required that will be used to hold the username and password for the user that is to be logged in. These tags need to be created upfront and can then be referenced from PM-LOGON Runtime (Tags **Username** and **Password**).

If a card is detected by the RFID reader the login credentials of the user are determined and transferred into the configured tags. A script within the HMI Runtime is triggered upon this tag change event and performs the login operation with the given username and password.

The **PIN** stored for the user can be transferred to the HMI via the PIN variable.

If a variable is attached to the **UID** property, the UID of the user token is transferred.

The user groups of which the user is a member can be transferred to the HMI via the variable **User Groups**.
Only user groups in which the user is a direct member are transferred. Memberships of groups in groups cannot be resolved.
The list of user groups is concatenated to a string with the separator defined in Groups Separator. It must therefore be ensured that the linked variable has a sufficient length.

The ID of the reader, that registered the UID, can be transferred by connecting the **Device Id** variable. If the reader is connected to the local PM-LOGON Runtime, the value "local" is written to the connected variable. If the local PM-LOGON Runtime is notified by PM-LOGON Server, the name of the corresponding reader is transmitted by PM-LOGON Server.

If attributes for the additional information **Extended Property 1** and **Extended Property 2** have been bound in the Active Directory Plugin, these can be written to two further string variables during logon, which are referenced via the fields "Write Extended Property 1 to Tag" and "Write Extended Property 2 to Tag".

The PM-LOGON Runtime can transmit status information to the HMI Runtime via the connection of a tag to the variable **PM-LOGON Status**.
Two status bits are transmitted cyclically every 30 seconds for this purpose:

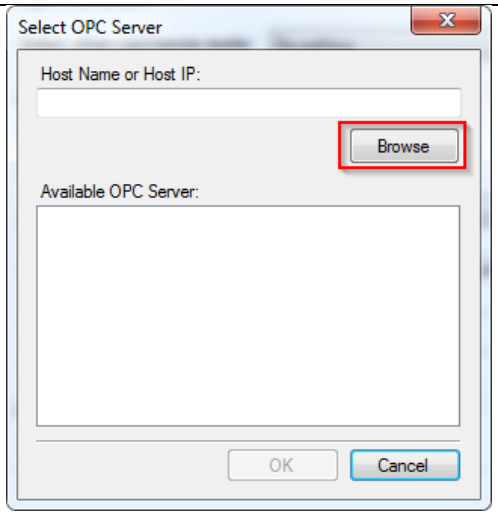
- Bit 0:
  While the PM-LOGON Runtime is running, this bit is written with the value 1 in the cycle of 30 seconds.
- Bit 1:
  If there is a connection between the reader and the PM-LOGON Runtime, this bit is written with the value 1 in the cycle of 30 seconds; if there is no connection, the bit is written with the value 0.
  If the status of the connection to the reader changes, the bit is updated accordingly after a maximum of 5 seconds.

If the **Require validated credentials** option has been activated, bit 3 of the status variable can be used to notify the HMI if the validation of the credentials has failed.
PM-LOGON Runtime then sets the value 1 to bit 3. The bit must be reset by the HMI after processing the value.

If you have selected the setting "Log off current user" as **Log off Behaviour**, you can use the "Logoff value" fields to define the values that PM-LOGON writes to the associated variables when the card leaves the field. If you do not specify a value, an empty string is written to the bound variable.

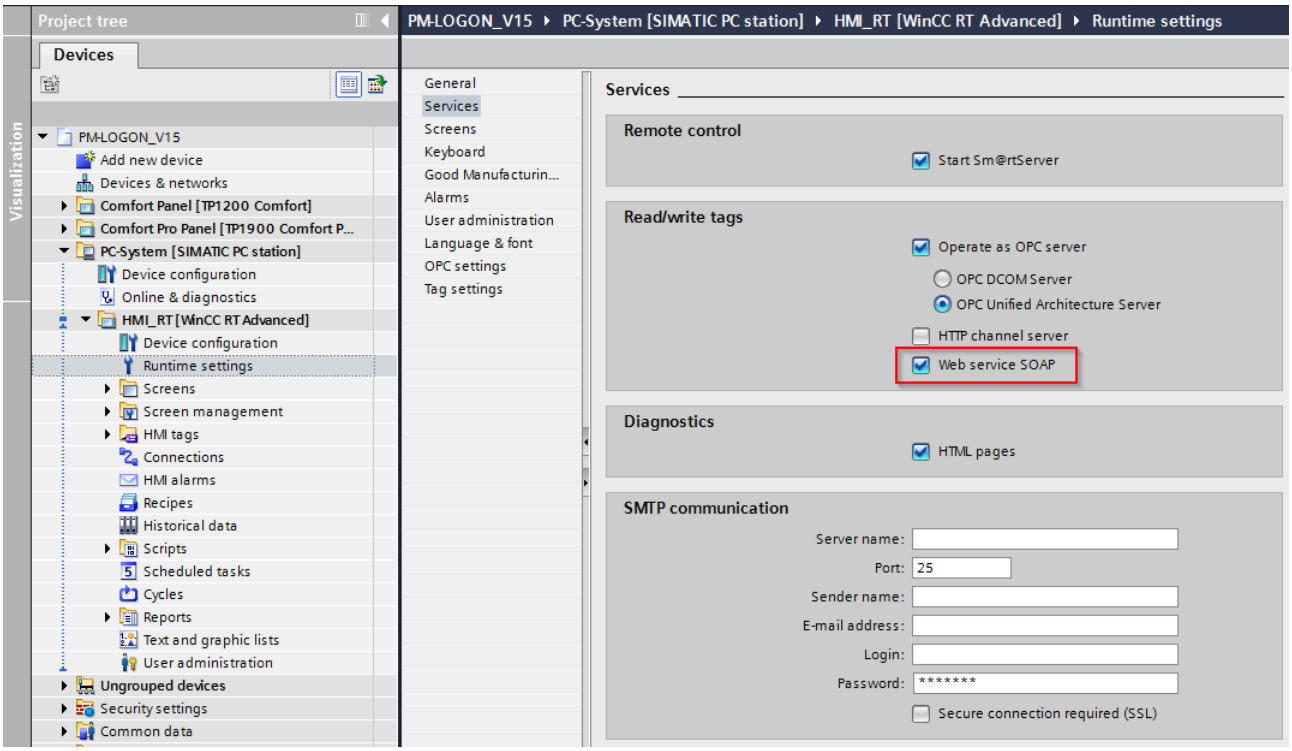
Log off behavior	Action, when card leaves reader	In the case that the RFID card leaves the reader an action can be defined how PM-LOGON should react in this case. The following alternatives are currently available: • Do nothing A currently logged in user remains logged in. • Log off current user A currently logged in user is logged off. For this purpose, a value of “-1” is written into the password tag.
HMI Runtime	Set credentials in open login window	For actions that require specific permissions the HMI Runtime displays a login dialog.

		If this option is activated and a card is brought into the detection range of the reader, the user name and password are entered by PM-LOGON and the dialog is automatically closed as if the OK button would have been clicked.
	Set password in password prompt of User view	This option is used by the PM-LOGON Basic Runtime when the user administration is done within the HMI Runtime.
	Require validated credentials	If this option is activated, PM-LOGON Runtime validates the credentials of the determined user before they are transferred to the target system. If the validation fails, the variables will not be written.
	Replace Password with	This option can be used to replace the password with a default value before writing to the bound variable.
	Groups separator	Defines the separator for the group list
	Access HMI Runtime via	This setting determines by which method the tags of the HMI Runtime should be written: • SOAP Webservice • OPC DA Server
	SOAP URI for Tag Access, SOAP Username und SOAP Password	This option is available when the SOAP access has been selected as the method to write the tags to the HMI Runtime. For this access method the URI defined here will be used. By default, the URI is: http://localhost/soap/RuntimeAccess Additionally, to enable writing tags to the HMI Runtime via SOAP access, a user that has the permissions to write tags via SOAP needs to be configured. These login credentials can be entered here. This user is configured in the “WinCC Internet Settings“ Control Panel Applet (described below). By default, the username and password “PM-LOGON” is used. For security reasons these default settings should by all means be changed.
	OPC Connection String	This option is available when "OPC DA Server" has been selected as the method to write the tags to the HMI Runtime. The connection string can be created by using the “Browse” button that opens up a dialog in which available OPC servers are listed for browsing.

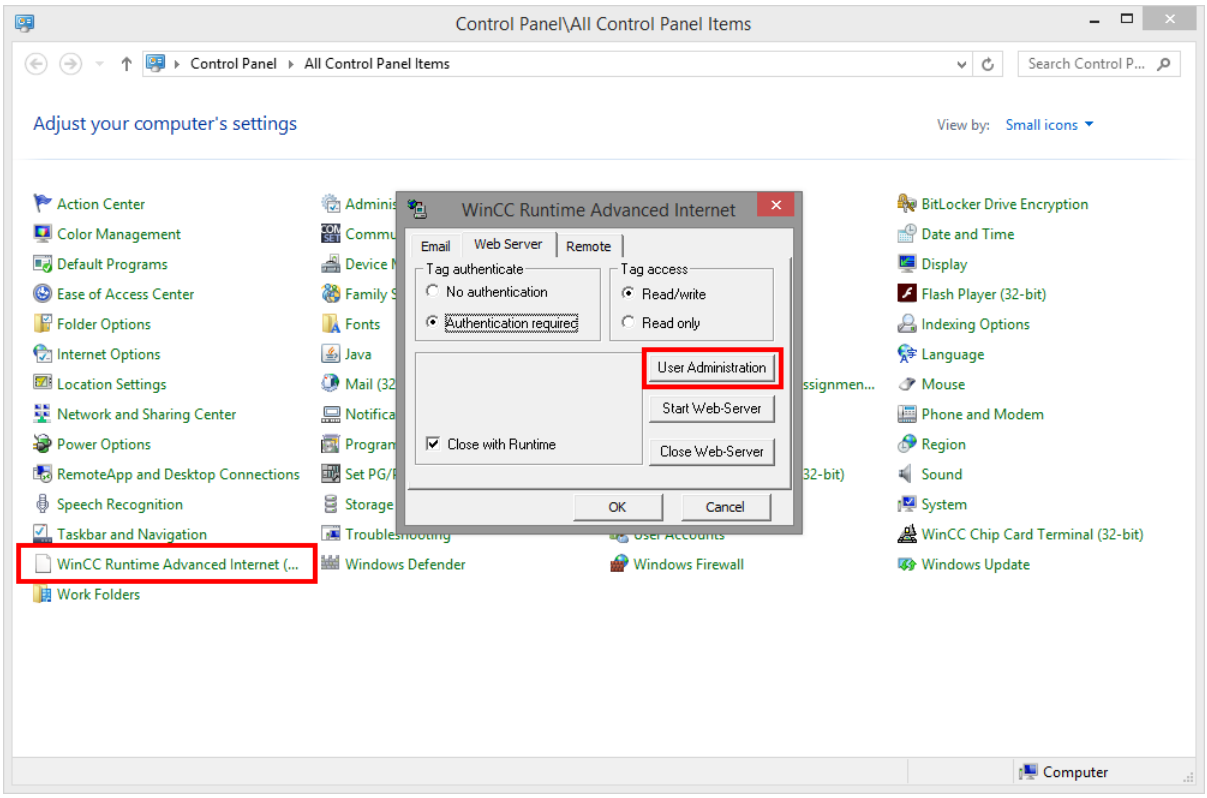
		
	Primary OPC UA Connection Uri	This option is available if "OPC UA Server" is selected as the method to write tags to the HMI Runtime. The default Uri of the OPC UA Server of WinCC Runtime Advanced is: "opc.tcp://127.0.0.1:4870" The detailed steps to configure the connection to the OPC UA Server are described in chapter 4.3.17.3.
	Secondary OPC UA Connection Uri	This option is available if "OPC UA Server" is selected as the method to write tags to the HMI Runtime. A second OPC UA server can be configured here. If the connection to the primary OPC UA Server cannot be established, the secondary OPC UA server will be targeted. The default Uri of the OPC UA Server of WinCC Runtime Advanced is: "opc.tcp://127.0.0.1:4870" The detailed steps to configure the connection to the OPC UA Server are described in chapter 4.3.17.3.
HMI Engineering	Set password in password prompt of User administration	This option is used by the PM-LOGON Basic Runtime if users are to be managed in the TIA Portal engineering.

4.3.17.1 SOAP access

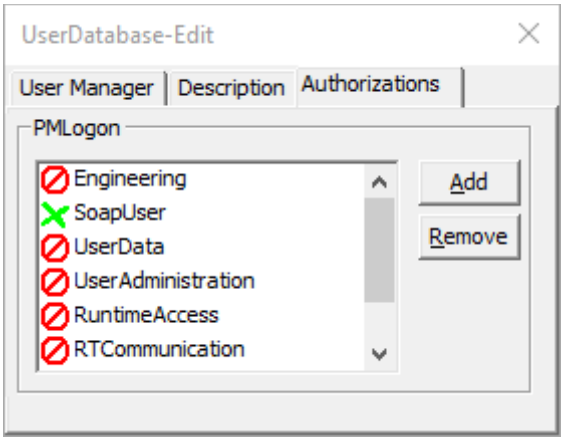
In order to set tag values in the runtime the SOAP-Service needs to be activated in the project settings.



Furthermore a user needs to be configured for the MiniWeb server. For WinCC V13 (or newer) Runtime Advanced this setting can be found in the configuration applet located in the control panel:

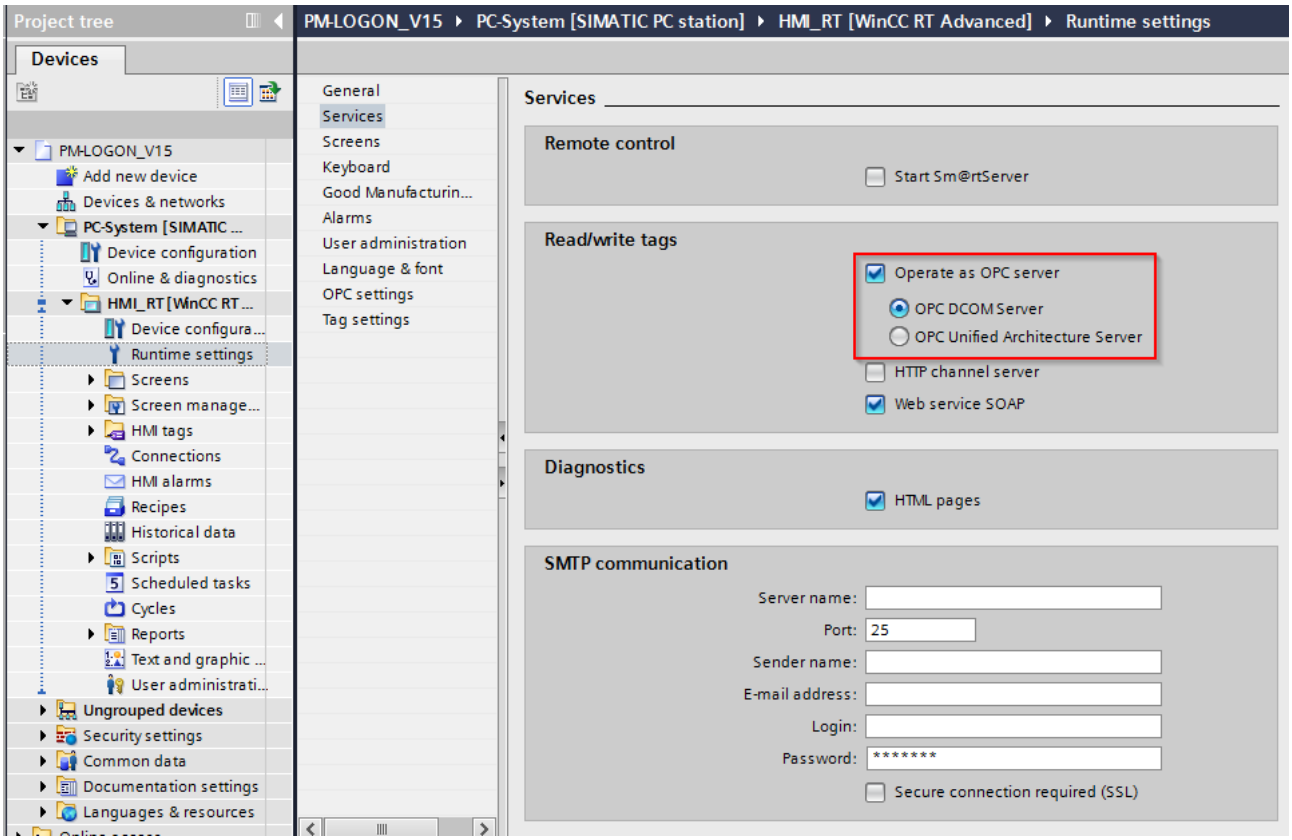


For this user to write tag values at runtime the permission “SoapUser” needs to be granted to the login.



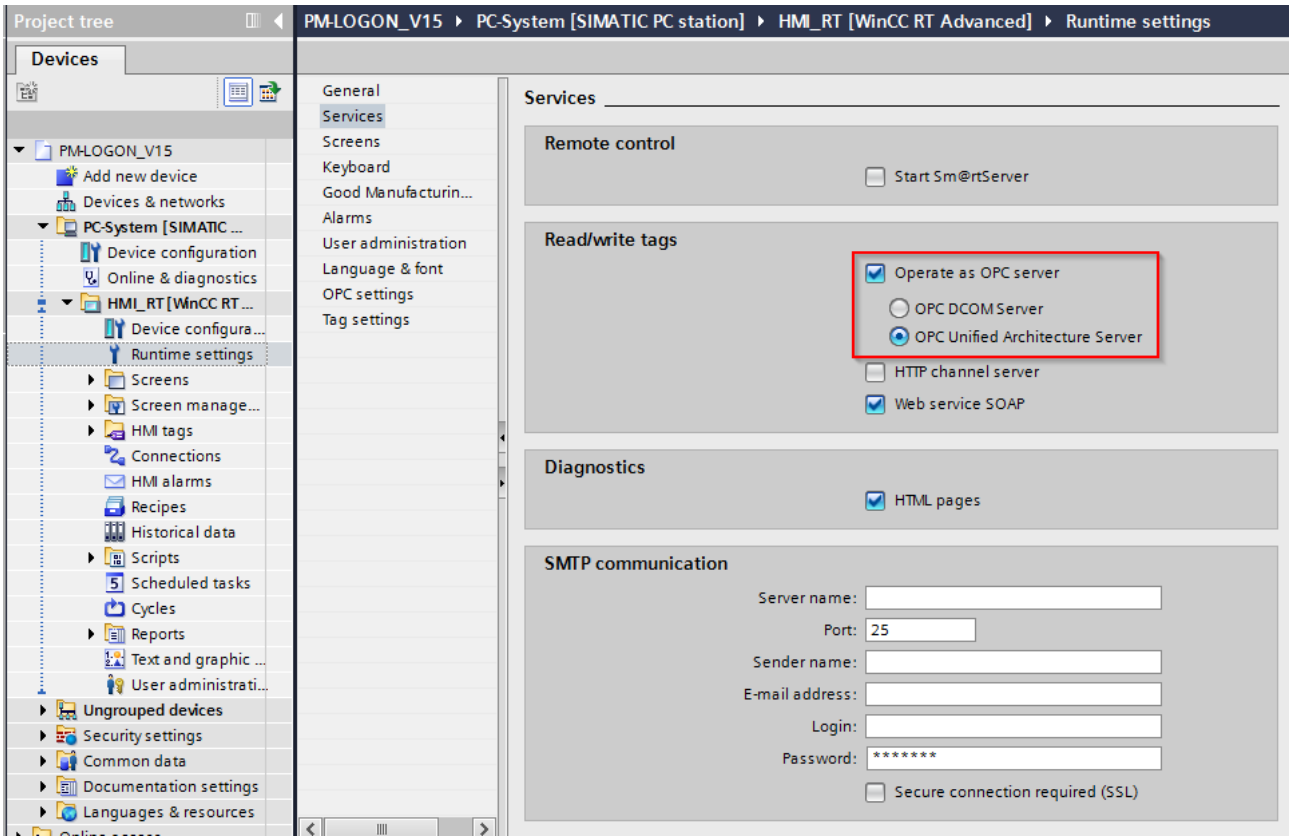
4.3.17.2 OPC DA access

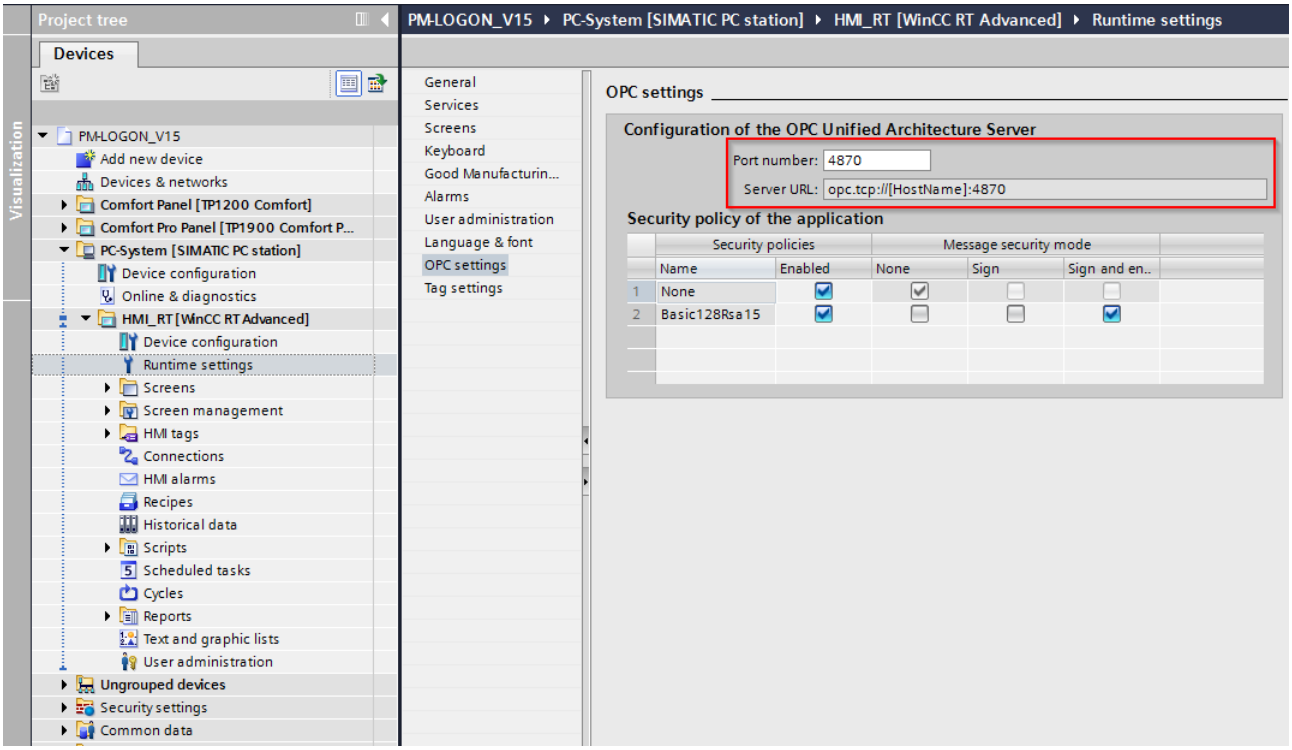
In order to write tag values to the runtime via the OPC service, the OPC-DCOM server needs to be activated in the project settings.



4.3.17.3 OPC UA Access

In order to write tag values to the runtime via the OPC service, at first the OPC-DCOM server needs to be activated in the project settings.





The Uri and port, The OPC UA Server of WinCC Runtime Advanced is listening is configured in the OPC settings of the TIA project.
After configuring the OPC UA Server of WinCC Runtime Advanced, you have to initiate the exchange of the Security certificates between OPC UA Server and PM-LOGON Runtime (OPC Client). Please follow these steps:

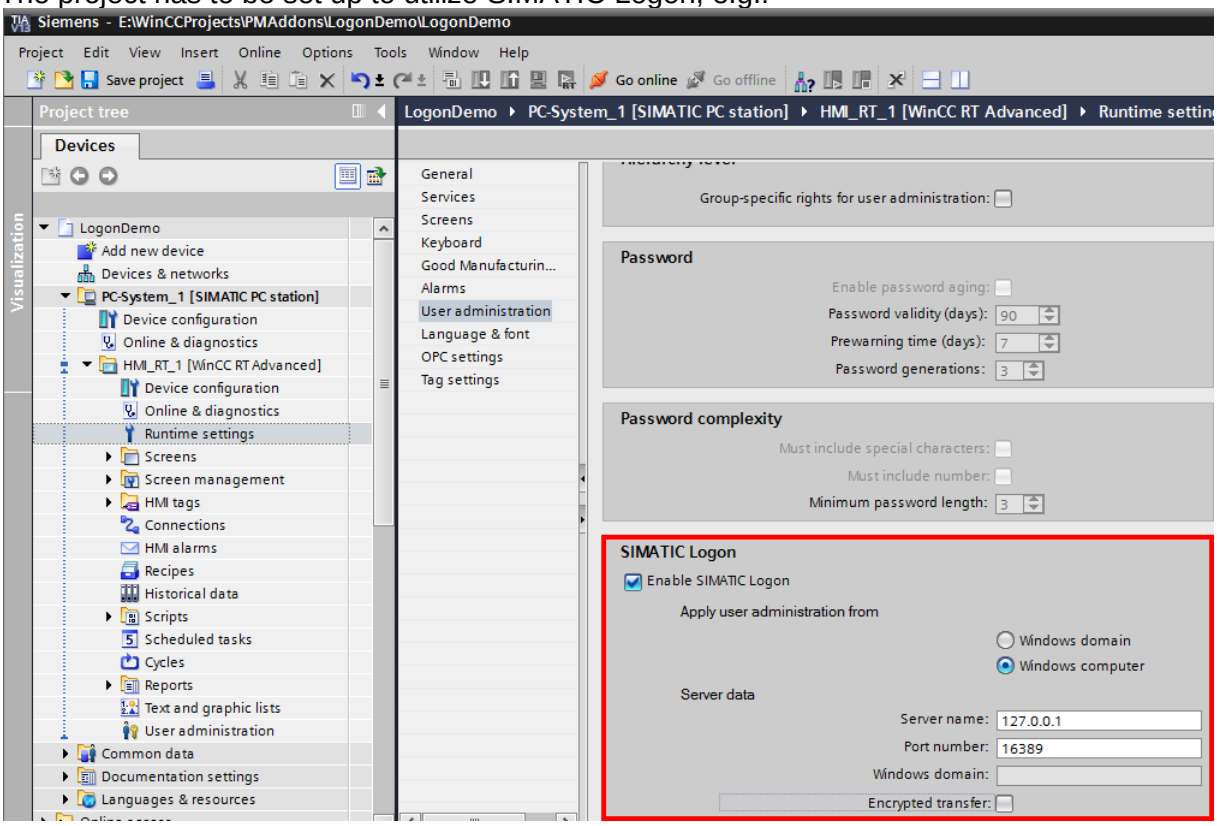
1. Start WinCC Runtime Advanced to get OPC UA Server running.
2. Open the configuration of PM-LOGON Runtime and select the section "OPC and SOAP Access".
3. As an interface to the HMI Runtime select "OPC UA Server". Make sure that the configured Uri is the same as configured in the OPC Settings of the TIA project.
4. Accept the Security Certificate of the OPC UA Server by clicking the button "Accept Certificate". The certificate will be stored in the directory "C:\ProgramData\Siemens\Process Management\PM-LOGON\Runtime\OPCUA\ Certificates" by PM-LOGON.
5. Thereafter click the button "Connect" to establish a connection to the OPC UA Server. This first attempt to connect will fail. The PM-LOGON Runtime has transmitted its own security certificate to the OPC UA Server. The OPC UA Server rejected the connection attempt because it does not trust the certificate yet.
6. To make the OPC UA Server trust the certificate of PM-LOGON Runtime, go to the directory "C:\ProgramData\Siemens\CoRtHmiRTm\MiniWeb1x.x.x\SystemRoot\SSL\rejected".Then move the rejected certificate of PM-LOGON Runtime to the directory "C:\ProgramData\Siemens\CoRtHmiRTm\MiniWeb1x.x.x\SystemRoot\SSL\certs".
7. If you then try to connect to the OPC UA Server again, the connection should be established successfully.
8. After connecting to the OPC UA Server, you can now assign the target variables of WinCC Runtime Advanced via the tag selection dialog.

The accepted or rejected certificates from communication partners can be managed via the section “Certificates” in the configuration of PM-LOGON Runtime.

Important notice:
After the upgrade from PM-LOGON V1.x to V2.x the security certificates of OPC UA Server and PM-LOGON Runtime must be updated or exchanged again, if necessary.

4.3.17.4 TIA project configuration

The project has to be set up to utilize SIMATIC Logon, e.g.:



Additionally two tags of type “WString” have to be created. These tags will be used by PM-LOGON Runtime to write the username and password, e.g.:

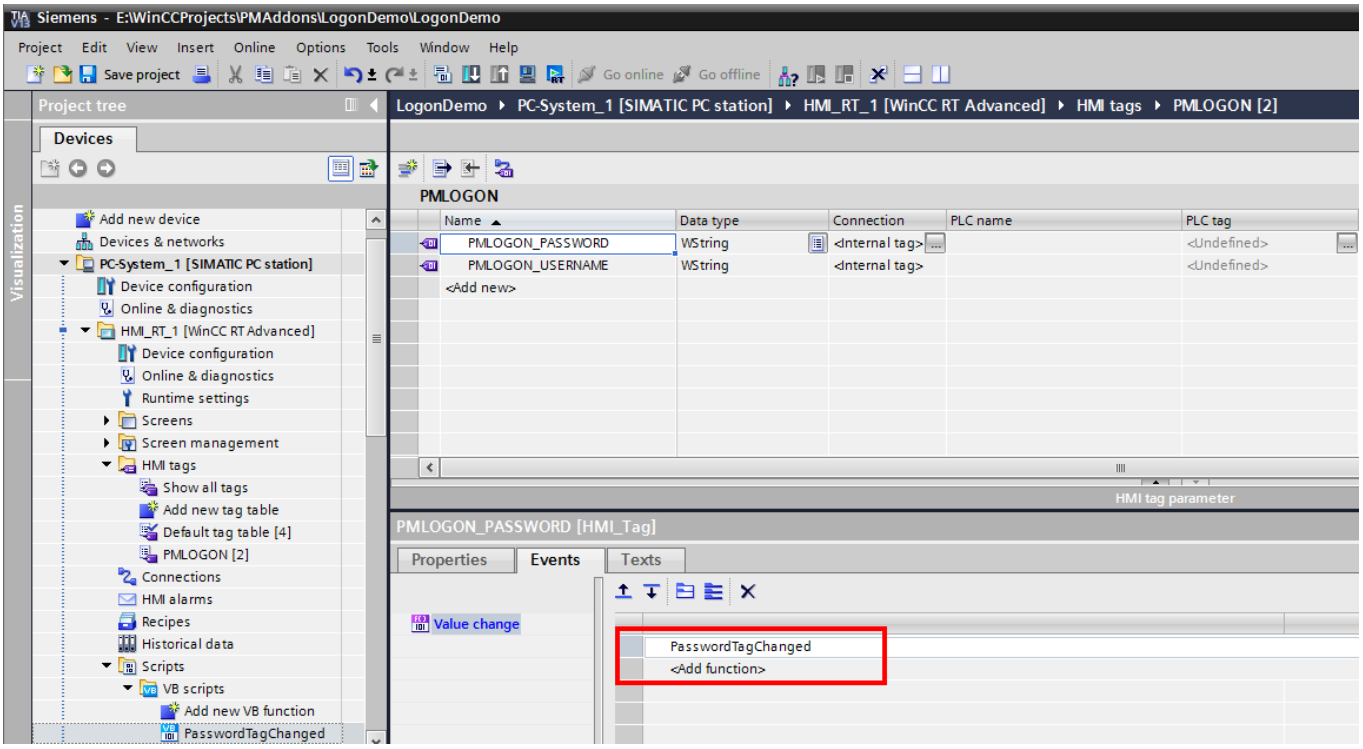
- PMLOGON_USERNAME
- PMLOGON_PASSWORD

Please make sure that the tags have been created with a sufficient initial length setting, e.g. at least 20 characters.

In order to perform the login operation a script is needed that is executed upon tag change:

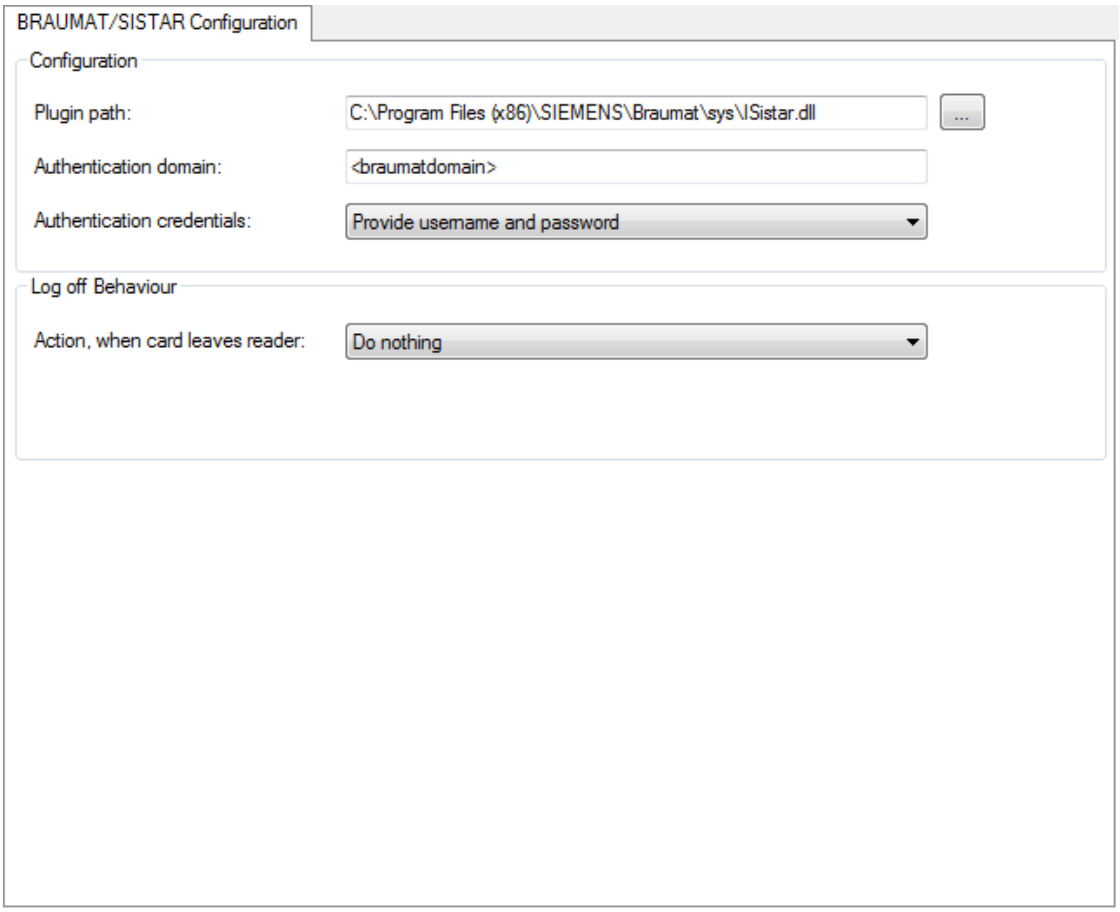
```
Sub PasswordTagChanged()
      If SmartTags("PMLOGON_PASSWORD") = "-1" Then
            Logoff
            SmartTags("PMLOGON_PASSWORD") = ""
      ElseIf SmartTags("PMLOGON_PASSWORD") = "" Then
            Logoff
      Else
            Dim usernameTag
            usernameTag = SmartTags("PMLOGON_USERNAME")
            Dim passwordTag
            passwordTag = SmartTags("PMLOGON_PASSWORD")
            Logon passwordTag, usernameTag
            SmartTags("PMLOGON_PASSWORD") = passwordTag
      End If
End Sub
```

This script must be executed upon tag change of the password tag (in this example “PMLOGON_PASSWORD”). "-1" is the default value that is written to the bound variable when PM-LOGON is logging off a user. If you have specified a different value in the PM-LOGON configuration, adjust this value.



4.3.18 Configuration of the BRAUMAT/SISTAR Provider

Via the plugin "BRAUMAT/SISTAR Provider" the login to a BRAUMAT/SISTAR system via PM-LOGON can be configured.



Plugin path:
The path to the BRAUMAT/SISTAR plugin for PM-LOGON must be specified here.

Authentication domain:
The domain, against which the user authenticates.

Authentication credentials:

- None:
  There is no logon to BRAUMAT/SISTAR.

- Provide username and password:
  When logging on, the user name and password are transferred to BRAUMAT/SISTAR.

- Provide username and empty password:
  The user name and an empty string for the password are transferred during logon.

- Provide empty username and empty password:
  When logging in, both an empty string as user name and an empty string for the password are passed.

Action when card leaves reader:

- Do nothing:
  There is no logout at BRAUMAT/SISTAR.

- Provide last logged on username:
  When logging out, the user name of the user last logged in via PM-LOGON is transferred.

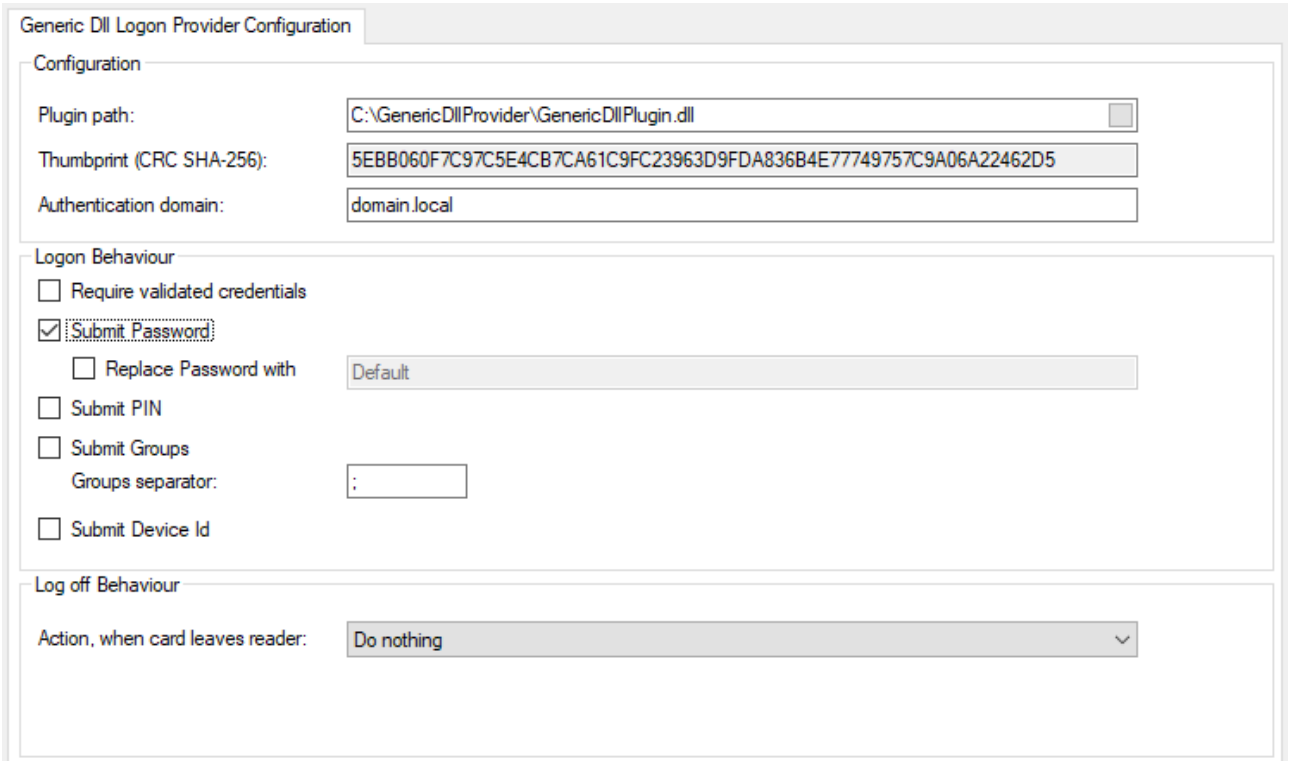
- Provide empty username:
  When logging out, an empty string is passed as the user name.

Not all readers support the signaling that the RFID card has been removed.

Activate the BRAUMAT/SISTAR Logon Provider by selecting "Enable Provider" in the context menu. You can activate multiple logon providers, e.g. to log a user on to SIMATIC Logon and simultaneously write variables via OPC or SOAP.

4.3.19 Configuration of the Generic Dll Logon Provider

Text



The Generic Dll Logon Provider can be used to connect a third-party system to PM-LOGON Runtime.
As an interface to the target system, the third-party system must provide a DLL that implements the following interface methods:

- BOOL WINAPI GenericLogonProvider_LogonW
  (const wchar_t* pszUser, const wchar_t* pszPassword)
- BOOL WINAPI GenericLogonProvider_LogonExW
  (const wchar_t* pszUser, const wchar_t* pszPassword,

const wchar_t* pszPin, const wchar_t* pszUserGroups,
const wchar_t* pszDeviceID)

- BOOL WINAPI GenericLogonProvider_LogoffW(const wchar_t* pszUser)

The path to this DLL is stored in the configuration of the Generic Logon Provider Plugin of PM-LOGON Runtime

If the Generic Dll Logon provider is activated in the PM-LOGON Runtime configuration, the DLL is loaded at runtime and the interface methods are called on the following events:

- The reader signals to PM-LOGON Runtime that a transponder has been detected.
- If an assigned user can be determined for the transponder in the Active Directory, PM-LOGON Runtime calls the *GenericLogonProvider_LogonW()* or the *GenericLogonProvider_LogonExW()* method of the interface DLL, depending on the configuration..

  The configuration of the Generic Dll Logon provider can be used to set which data is passed in addition to the user name when calling the method:
  - Submit password:
    The password is passed to the dll. Via “Replace Password with” a replacement value can be defined which is passed instead of the password.
  - Submit PIN:
    If a PIN has been stored for the user in the user repository, this is passed to the target system.
  - Submit Groups:
    Only user groups in which the user is a direct member are transferred.
    Memberships of groups in groups cannot be resolved.
    The list of user groups is concatenated to a string with the separator defined in Groups Separator.
    It must therefore be ensured that the linked variable has a sufficient length.
  - Submit Device Id:
    The name of the reader that recognized the UID is transmitted. If it is the locally connected reader, "local" is transmitted for this. If the local PM-LOGON Runtime is notified by PM-LOGON Server, the name of the corresponding reader is transmitted by PM-LOGON Server.

  If only the passing of username and password is configured in the plugin, the *GenericLogonProvider_LogonW()* method is called.
  If additionally the passing of PIN, user groups or DeviceID was configured, the method *GenericLogonProvider_LogonExW()* is called instead.
  For parameters which are not used, an empty string is passed by PM-LOGON Runtime.

- The reader signals PM-LOGON Runtime that the transponder has left the reader field:
  The *GenericLogonProvider_LogoffW()* method is called. The configuration of the Generic Logon Provider can be used to set which data is passed when calling the method:
  - Username of the last logged in user:
    The username of the last user logged in by PM-LOGON is passed for pszUser.
  - Empty username:
    An empty string is passed for the username.

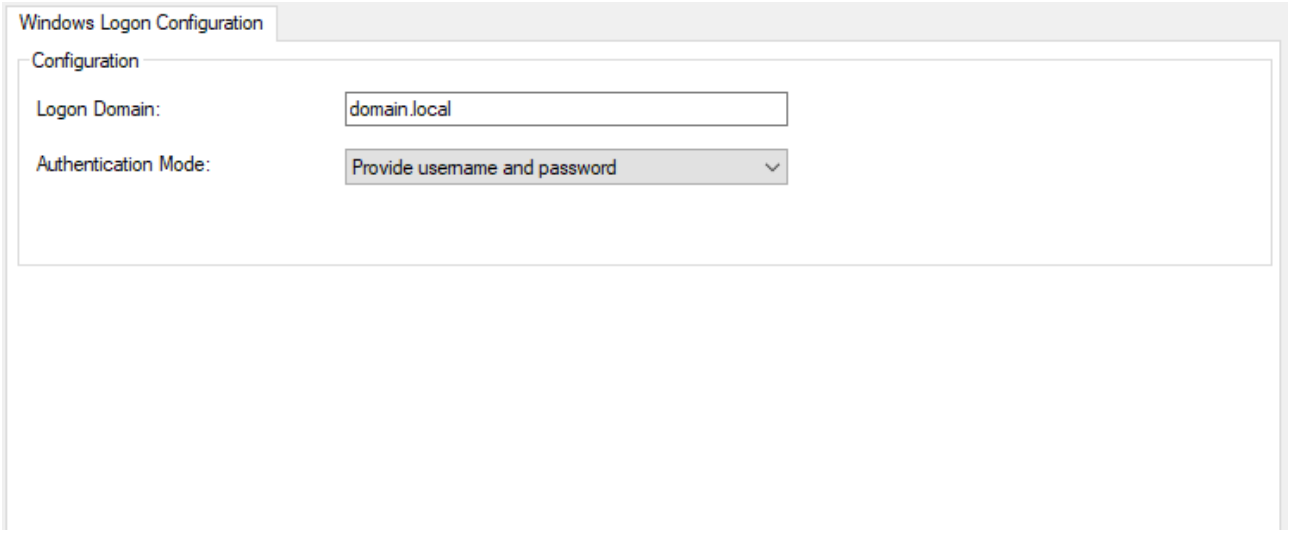
Authentication of the user against Active Directory must be performed by the third-party system itself.

To secure the communication with the DLL, the thumbprint of the plugin dll is registered in the configuration of the local PM-LOGON Runtime.
At runtime PM-LOGON Runtime can then verify the DLL via the registered thumbprint.

If you need further information about the connection of a third party system via this Logon Provider, please contact the WinCC Competence Center Mannheim (mailto:winccaddon.automation@siemens.com).

4.3.20 Configuration of the Windows Logon Provider

Via the plugin "Windows Logon Provider" the login to Windows via PM-LOGON can be configured.
To use and configure this plugin, PM-LOGON Runtime must be run in Service Mode.



Logon domain:
You can enter the domain, to which the user should be logged in. If this field is empty, the local computer name will be used.

Authentication Mode:
Here, you must select which Logon Mode should be used.

- Provide username and password:
  The user will be logged in with the stored credentials.

- Logon with password:
  The username will be preset, the user must enter its password in order to login.
- Logon with PIN:
  The user is prompted to enter his PIN. If the PIN entered matches the PIN stored in the user repository, the user is logged in with the stored credentials.
  If no PIN has been stored for the user, the "Logon with password" mode is automatically applied.

Activate the Windows Logon Provider by selecting "Enable Provider" in the context menu. You can activate multiple logon providers, e.g. to log a user on to SIMATIC Logon and simultaneously write variables via OPC or SOAP.

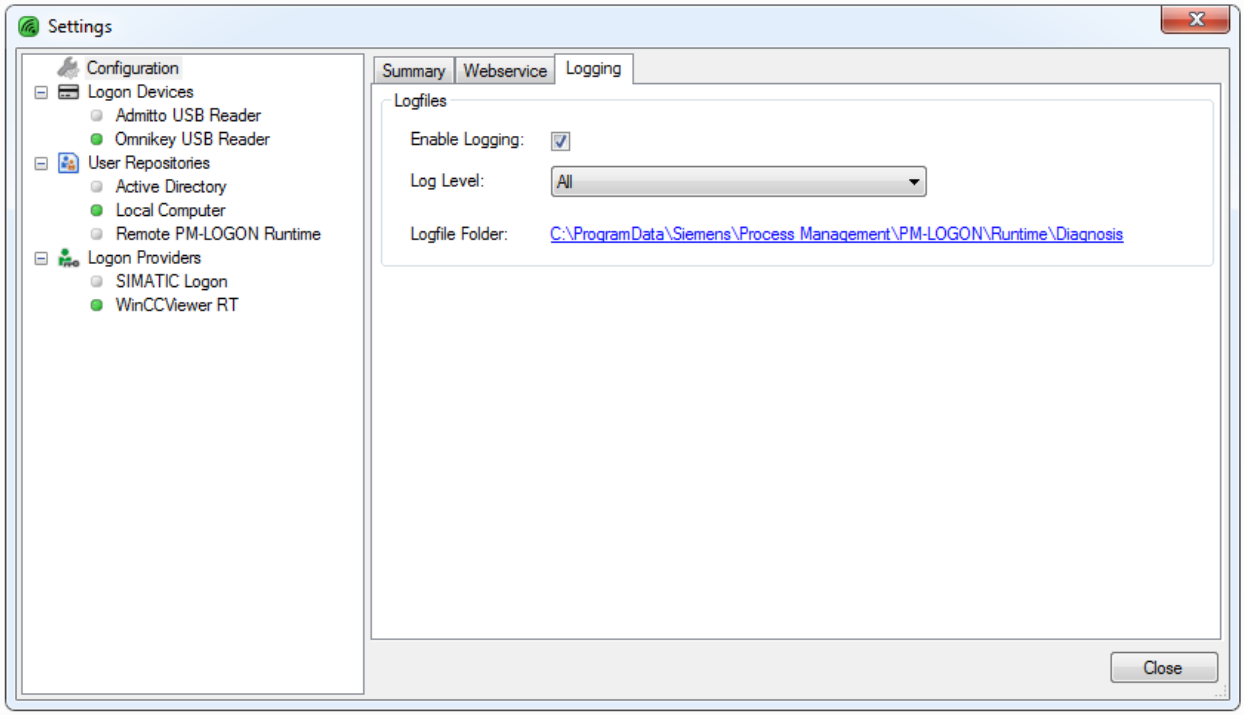
The PM-LOGON tile in the lock screen will only be shown, if the Windows Logon Provider is activated.

4.4 Diagnostics

Logging of trace information into log files for diagnostic purposes can be configured on the page “Logging” within the configuration section (“Enable Logging”).
The level of information written to the logs can be defined by selecting one of the options from the drop-down list “Log Level”:

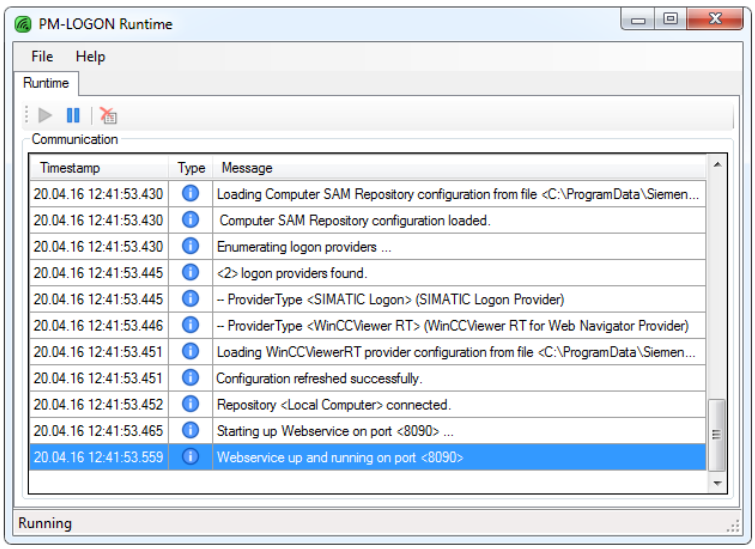
- All:
  All messages
- Error:
  Only errors
- Warning:
  Warnings and errors
- Information:
  Information messages, warnings and errors
- Verbose:
  Detail information, Information messages, warnings and errors

File logging should only be activated for diagnosing problems and should not be activated permanently. The size of the log files is limited to 10MB and the log files are automatically deleted after 7 days. The folder where the log files are stored can be opened by clicking the link to the right of the label “Logfile Folder”.



4.5 Operation

The setup routine creates an entry in the start menu and the PM-LOGON Runtime is configured to automatically start upon system restart after the user login of the operating system.



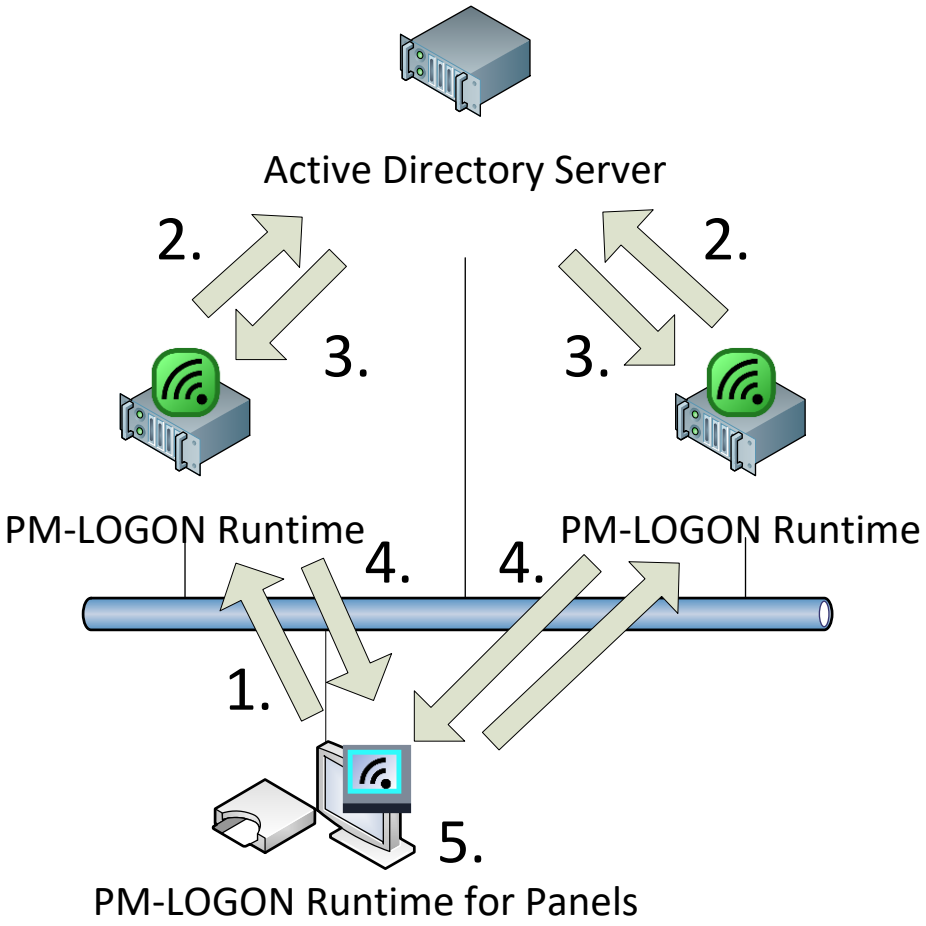
The PM-LOGON Runtime is activated if the “Play” button has been pressed. After activation the connections to the reading device, the user repository and the login provider are established. If a RFID card is detected by the reader, the login information associated with the UID of the card is determined from the user repository and handed over to the login provider (e.g. SIMATIC Logon).

5 PM-LOGON Runtime for Panels

5.1 Introduction

For the execution on Comfort Panels the “PM-LOGON Runtime for Panels” is required.

While the PM-LOGON Runtime is determining the login credentials of the user that has been assigned to a card sensed by the reading device directly from e.g. the active directory, this process is performed indirectly by the PM-LOGON Runtime for Panels:



The login credentials are queried from one or two remote PM-LOGON Runtime instances (1), that are relaying the query to an active directory (2). The response delivered from the active directory server (3) is then relayed back to the PM-LOGON Runtime for Panels (4). The username and password that have been received on the panel are written into tags on the Panel Runtime (5). Within the panel runtime a script is executed that performs the login operation by utilizing the system function “Logon”.

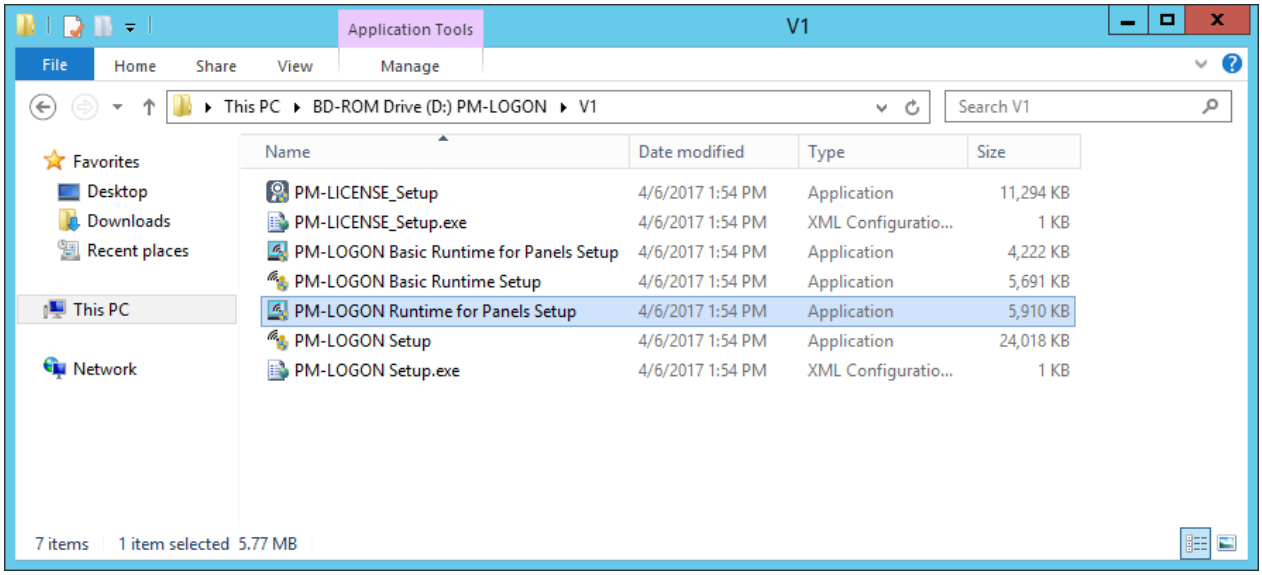
5.2 Installation on a Comfort Panel

The following prerequisites are required:

- Panel:
  - SIMATIC TP Comfort Panel with x86 processor architecture(starting from 7”); KP400 Comfort and KTP400 Comfort are not supported!
  - SIMATIC TP Comfort Pro Panel with x86 processor architecture
- A supported card reader:

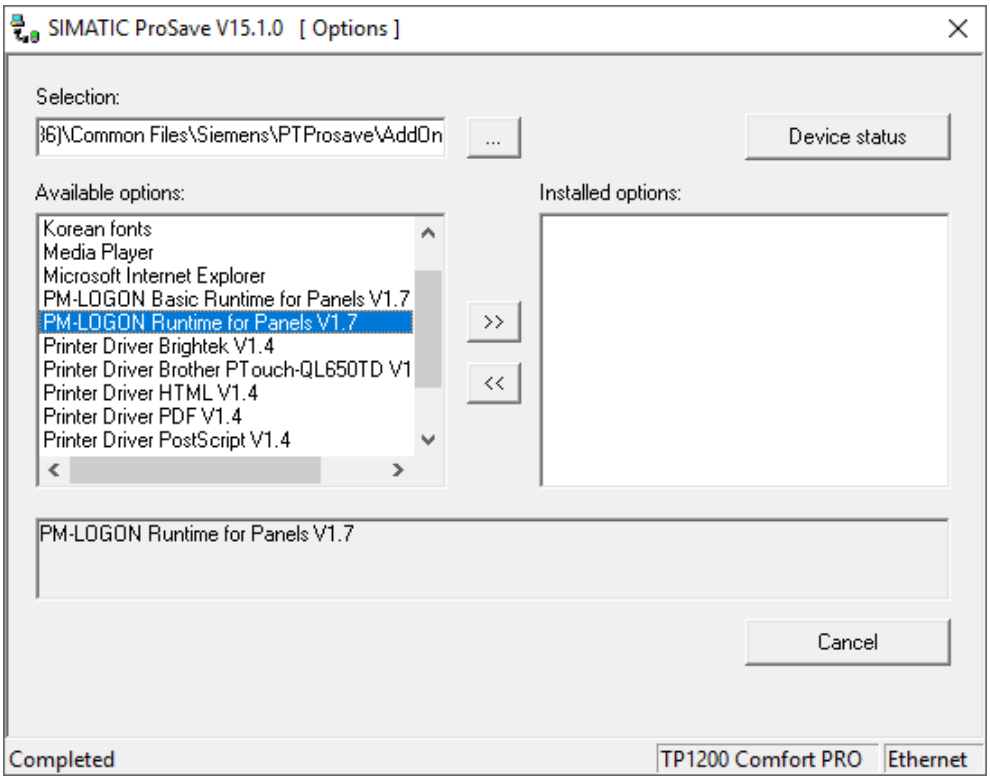
  - SIMATIC RF1040R/RF1060R/1070R or
  - Admitto USB card reader operating in the mode “active send”
- A free USB port on the panel
- Engineering PC with TIA Portal V13 or V14
- At least one PC with PM-LOGON Runtime on the same network
- Optional: A USB keyboard and mouse connected to the panel is recommended during configuration

The installation is done by “SIMATIC ProSave”. In order to add this option to ProSave, the “PM-LOGON Runtime for Panels Setup.exe” needs to be installed on the engineering PC.



The setup installs the option “PM-LOGON Runtime for Panels V1.x”into “SIMATIC ProSave”, which is part of the TIA engineering system. If “SIMATIC ProSave” cannot be found on the target system the setup will be cancelled.

After successful installation “SIMATIC ProSave” can be started and the option “PM-LOGON Runtime for Panels” can be transferred to the panel.



After the transfer has completed successfully the panel will be restarted.

“PM-LOGON Runtime for Panels” is automatically executed upon each restart of the panel so no further activities are required. If the application has been shut down, it can be manually restarted by using the link from the start menu “PM-LOGON”➔“PM-LOGON Runtime For Panels”.

The transfer via “SIMATIC ProSave” does also install the required device drivers for the SIMATIC RF1040R/RF1060R/RF1070R and the Admitto USB readers which are ready for operation after the panel has been restarted.

The simultaneous installation of “PM-LOGON Runtime for Panels” and “PM-LOGON Basic Runtime for Panels” on the same device is not supported.

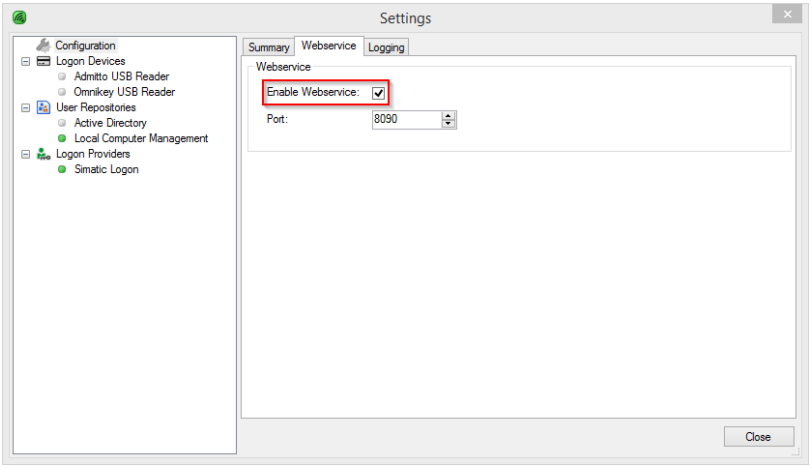
If an older version of “PM-LOGON Runtime for Panels” that has not been installed via ProSave has been manually installed on the device, this old version needs to be removed completely before the new version is installed. This can e.g. be done by loading the firmware image again onto the device (e.g. also from ProSave). Please perform a backup of the device before that in order to prevent data loss.

5.3 Configuration

For the operation the “PM-LOGON Runtime for Panels” as well as the access to the “PM-LOGON Runtime” and the HMI project needs to be configured.

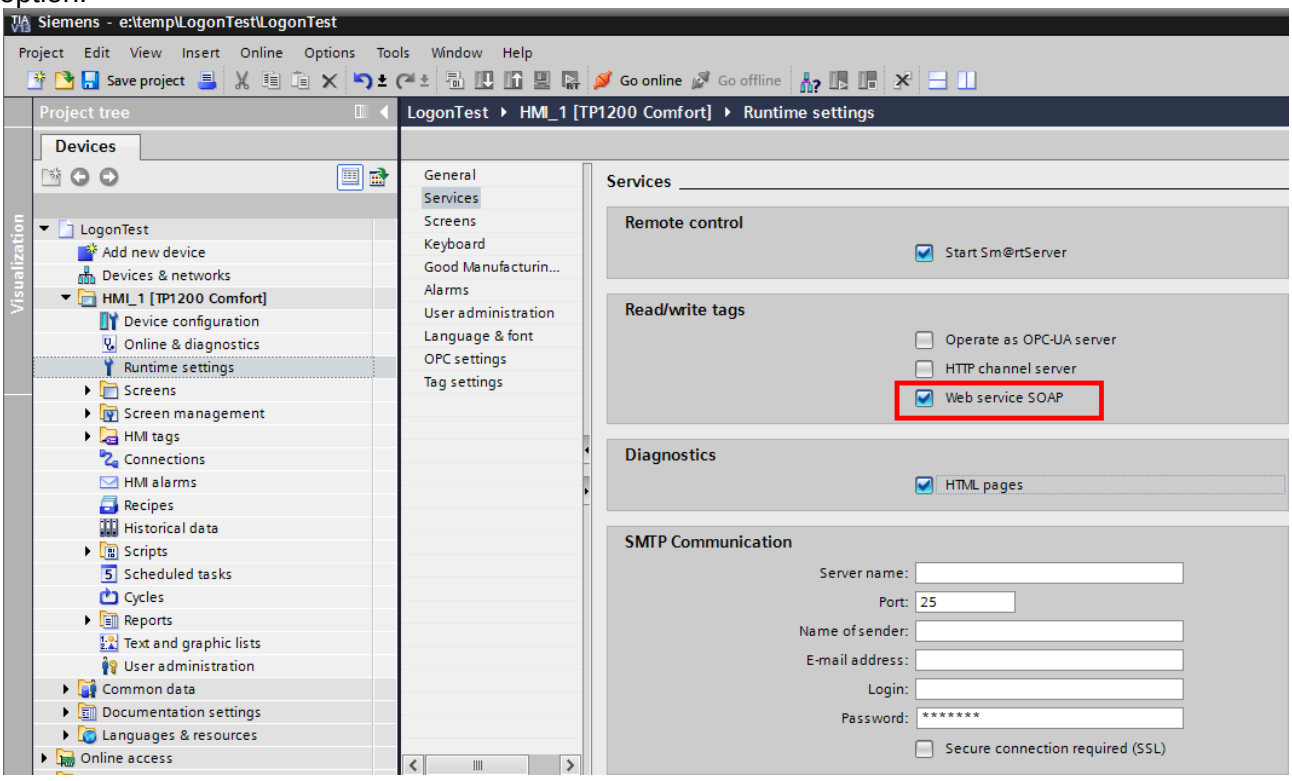
5.3.1 PM-LOGON Runtime

PM-LOGON Runtime for Panels gets the credentials to perform a login operation from a PC on the network where PM-LOGON Runtime is executed. On the PM-LOGON Runtime the functionality to provide information to remote PM-LOGON Runtime for Panels instances via the integrated web service needs to be enabled:

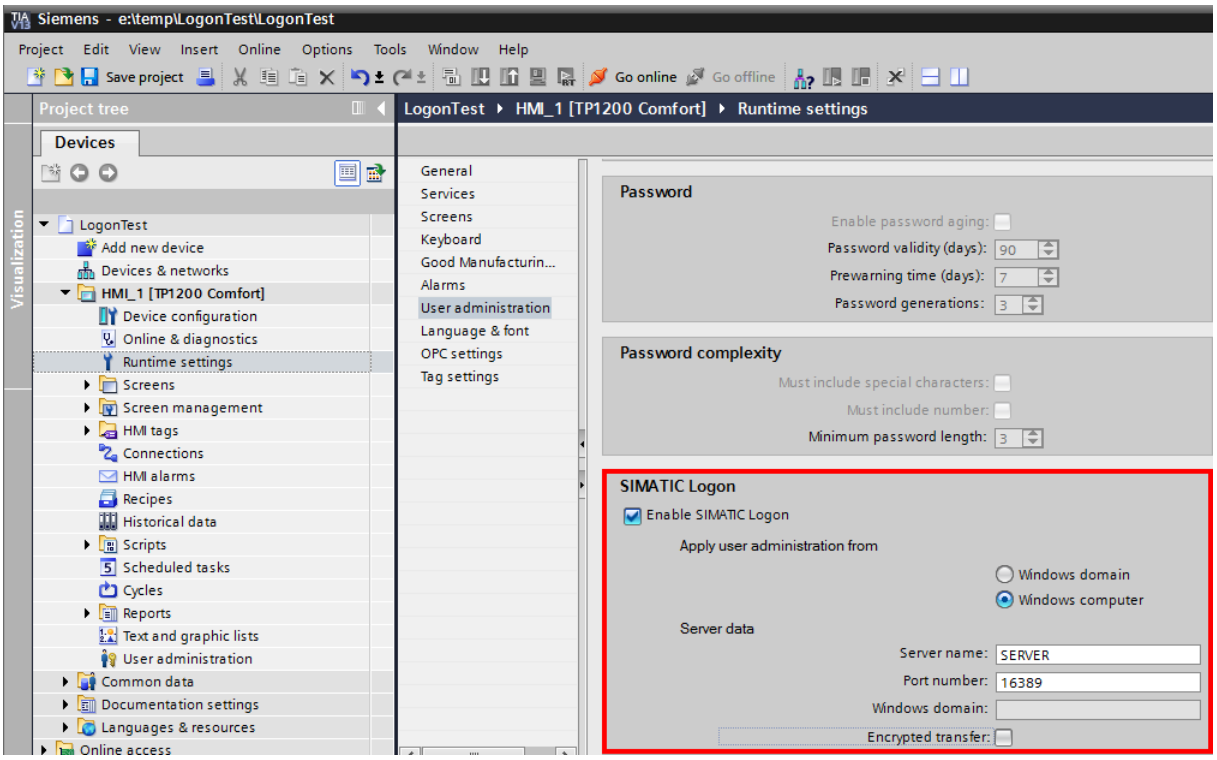


5.3.2 TIA portal project

The project must be configured to enable the writing of tags to the runtime via the SOAP service. This can be done in the services settings for the runtime by activating the “Web-Service SOAP” option:



The project also needs to be configured to utilize SIMATIC Logon for user authentication e.g.:



Furthermore two string tags have to be created where PM-LOGON Runtime for Panels is writing the login credentials to, e.g.:

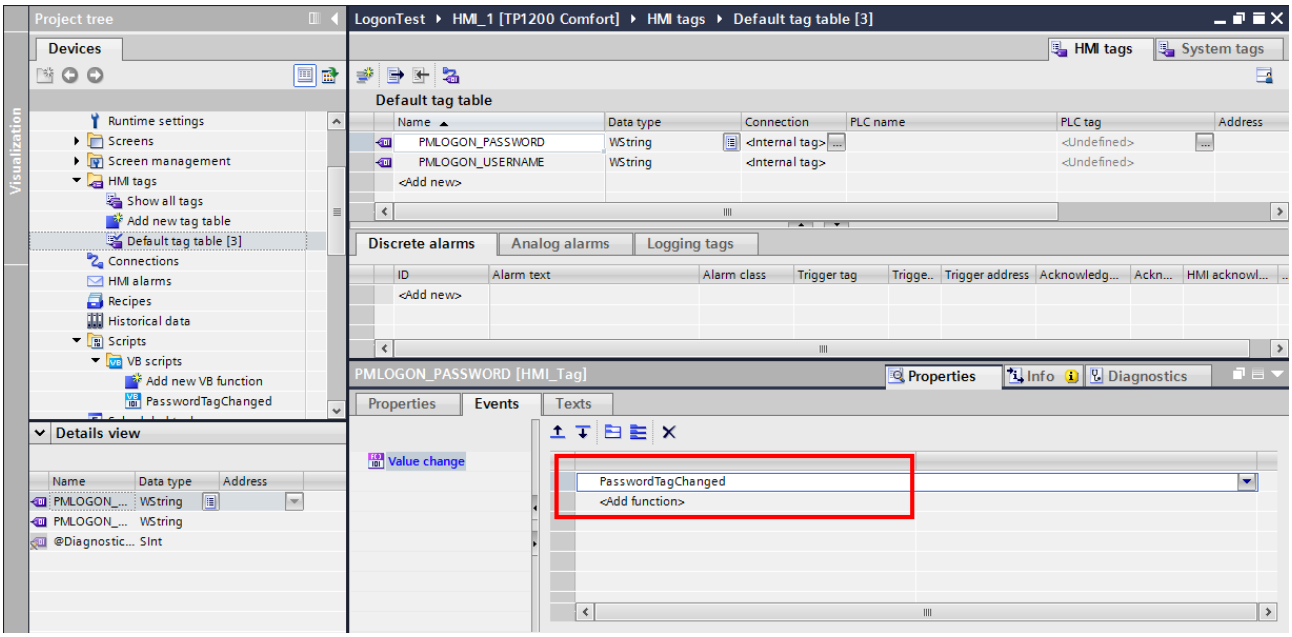
- PMLOGON_USERNAME
- PMLOGON_PASSWORD

Please make sure that the tags have been created with a sufficient initial length setting, e.g. at least 20 characters.

In order to perform the login operation a script is needed that is executed upon tag change:

```
Sub PasswordTagChanged()
	If SmartTags("PMLOGON_PASSWORD") = "-1" Then
		Logoff
		SmartTags("PMLOGON_PASSWORD") = ""
	ElseIf SmartTags("PMLOGON_PASSWORD") = "" Then
		Logoff
	Else
		Dim usernameTag
		usernameTag = SmartTags("PMLOGON_USERNAME")
		Dim passwordTag
		passwordTag = SmartTags("PMLOGON_PASSWORD")
		Logon passwordTag, usernameTag
		SmartTags("PMLOGON_PASSWORD") = passwordTag
	End If
End Sub
```

This script must be executed upon tag change of the password tag (in this example “PMLOGON_PASSWORD”).

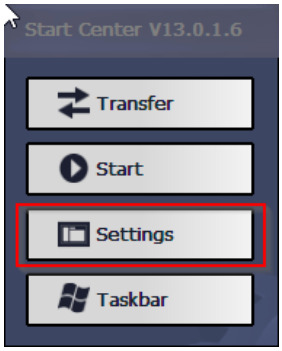


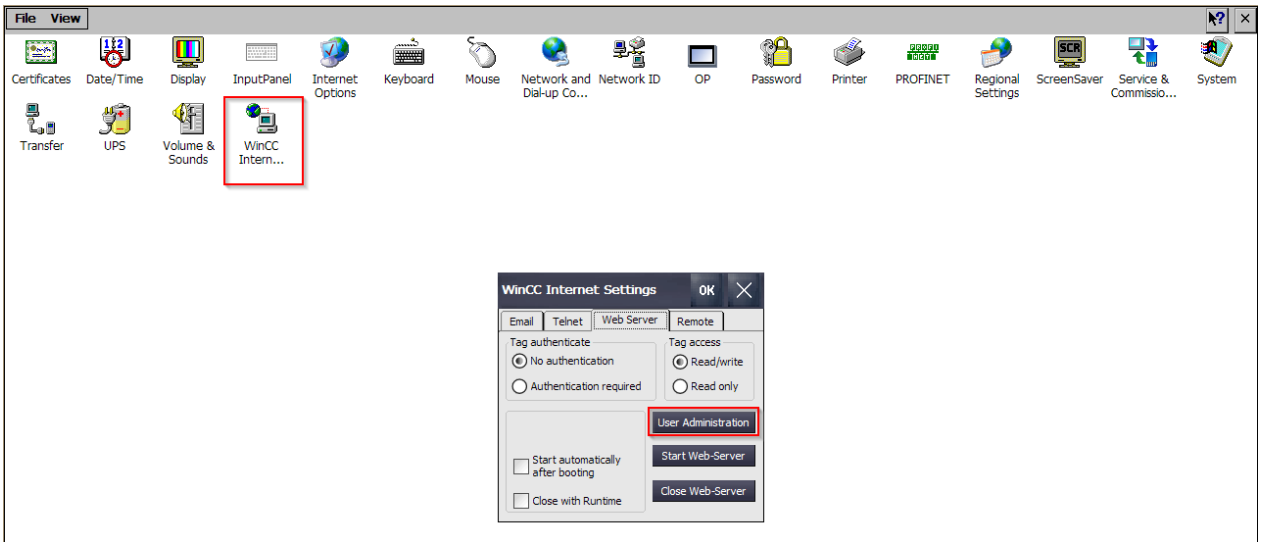
*

5.3.3 MiniWeb

Furthermore a user needs to be configured for the MiniWeb server.

On the Comfort Panel these settings are located under Settings in the Start Center:

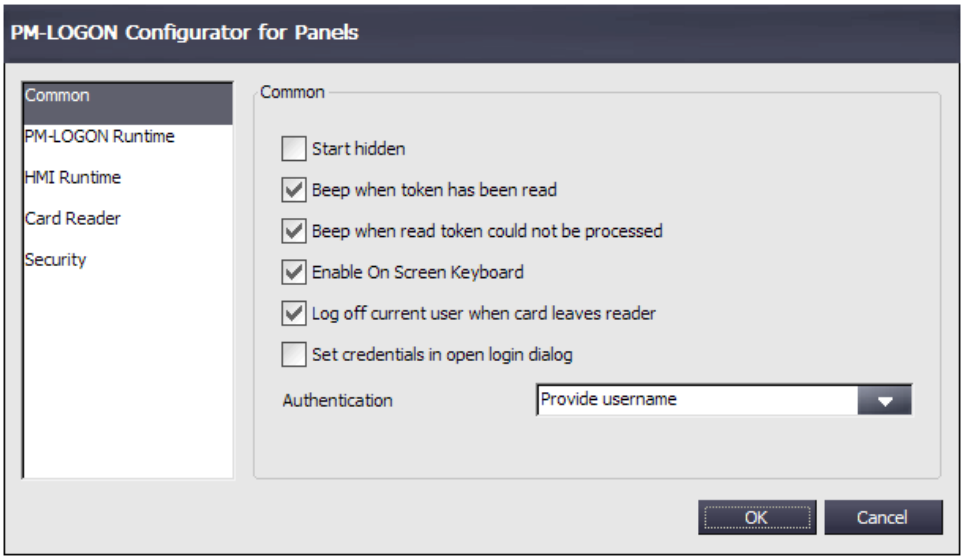


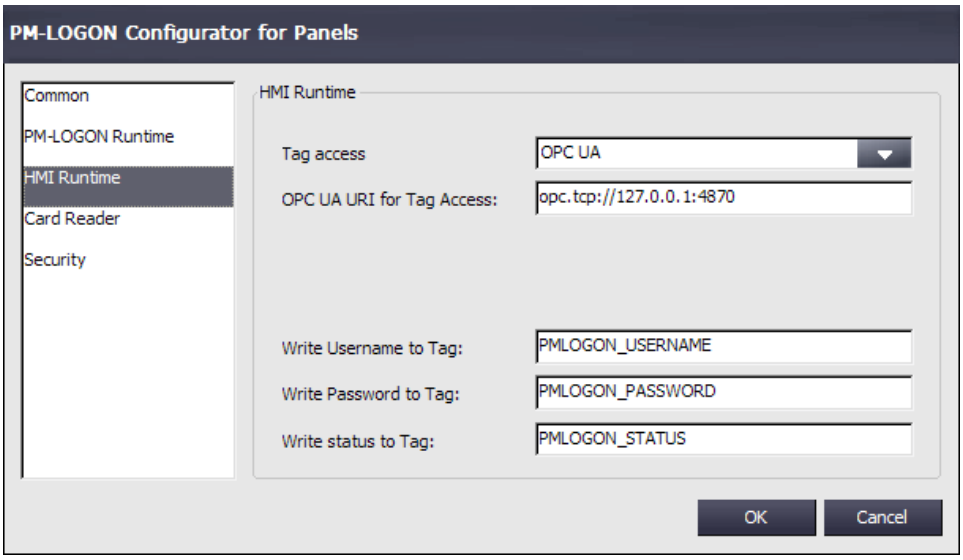


For this user to write tag values at runtime the permission “SoapUser” needs to be granted to this login.

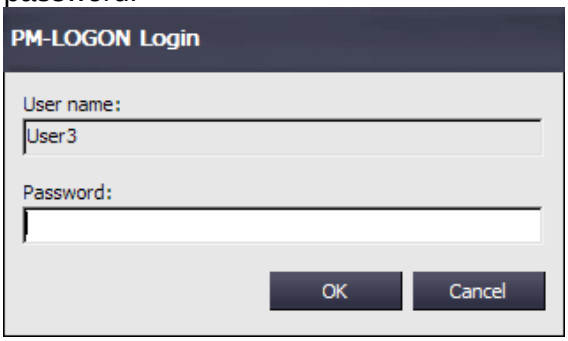
5.3.4 PM-LOGON Configurator for Panels

The configuration application of “PM-LOGON Runtime for Panels” can be accessed via the start menu link “PM-LOGON“ ➔“PM-LOGON Configurator for Panels”:





Section	Setting	Description
Common	Start hidden	If this option has been activated the PM-LOGON Runtime for Panels is started hidden and is only visible on the system tray; the main window can be opened by double clicking the symbol on the tray. 
	Beep when token has been read	An information sound will be played when a RFID card has been recognized by PM-LOGON Runtime for Panels.
	Beep when read token could not be processed	An error sound will be played if the card detected by the reader could not successfully be processed. The processing may fail e.g. for the following reasons: • No remote PM-LOGON Runtime could be contacted. • No login credentials have been configured for the RFID card presented to the reader. • The login credentials could not be transferred to the HMI runtime. The exact reason why the login has failed can be narrowed down by looking into the diagnostic log.
	Enable On Screen Keyboard	If a login dialog is displayed by the PM-LOGON Runtime, this setting determines if the on screen keyboard should be displayed to enter the password. This setting is only relevant if the “Authentication credentials” have been configured as “Provide username”.
	Log off current user, when card leaves reader	If this option has been activated a currently logged in user is logged off when the previously detected card is removed from the card reader. For this purpose a value of “-1” is written into the password tag.

		Please note that not all card reading devices provide a notification when a RFID card has left the reader detection range.
	Set credentials in open login dialog	If this option has been activated the login credentials associated with the presented RFID card are written into an eventually currently open login dialog displayed by the HMI Runtime. The login dialog is always displayed by the HMI Runtime when an action is to be executed that requires specific permissions that are not granted to an eventually currently logged in user. “PM-LOGON Runtime” enters the user name and the password into this dialog automatically and closes the dialog with OK.
	Authentication credentials	This setting defines how the login information is being used to perform a login: • Provide username The login dialog will be displayed and the username is pre filled with the username associated with the RFID card detected by the reader. The user has to manually enter the password.  • Provide username and password The login dialog will not be displayed and the username and password associated with the RFID card detected by the reader is automatically handed over to the runtime to perform the login.
PM-LOGON Runtime	Uri / Second Uri	AT least one PM-LOGON Runtime has to be entered that will be queried for login credentials when a RFID card has been detected. If two addresses have been entered both PM-LOGON Runtime instances will be queried simultaneously. However only one response is needed for operation, the second response will be discarded. Entering two addresses provides a redundancy mechanism if one PM-LOGON Runtime cannot be reached on the network. The address is entered in the following format: http://<COMPUTER>:<PORT> COMPUTER:

		IP or hostname of the PC, where PM-LOGON Runtime is executed. PORT: Port number in the PM-LOGON Runtime that is used for the web service. The default setting is 8090. The port number can be changed within the PM-LOGON Runtime. Please note that the access is performed by using the HTTP protocol. If a proxy server is being used on the system, it might be necessary to bypass the proxy. The login information is always transferred in a encrypted format.
HMI Runtime	SOAP URI for Tag Access	Username and password are written to tags of the PM-LOGON Runtime for Panels. To enable this access the SOAP access has to be enabled for the panel runtime. SOAP is based on HTTP and communication with the runtime is established by using a URI. For the panel runtime, this URI currently defaults to the following format: http://127.0.0.1/soap/RuntimeAccess
	SOAP Username / Password	For security reason accessing the SOAP service for the reading and writing of tags requires authentication credentials. The login information of the user that has been configured in 5.3.3needs to be entered here. The password is stored in the configuration in encrypted format.
	OPC UA Connection Uri	Wurde OPC UA zum Schreiben der Variablen ausgewählt, so ist hier die Uri zum OPC UA Server anzugeben. Die Einrichtung einer OPC UA-Verbindung ist im Kapitel 4.3.17.3 beschrieben.
	Write Username / Password to Tag	If a PM-LOGON Runtime has been successfully queried for login credentials that are associated to the detected RFID card the username and password will be written into tags by using the SOAP web service of the panel runtime. The password that is used to perform the login operation needs to be written to the tag in clear text i.e. not encrypted. Therefore for security reasons this tag should not be displayed anywhere in the HMI of the panel.
	Write status to Tag	If a variable is bound here, "PM-LOGON Runtime for Panels" cyclically transmits status information regarding the PM-LOGON Runtime and the connection status of the reader every 5 seconds. For this purpose, 2 status bits are written: • Bit 0: While the PM-LOGON Runtime is running, this bit is written cyclically with the value 1.. • Bit 1: If the connection between the reader and the PM-LOGON Runtime is established, this bit is written cyclically with the value 1; if there is no connection to the reader, the bit is written with the value 0.

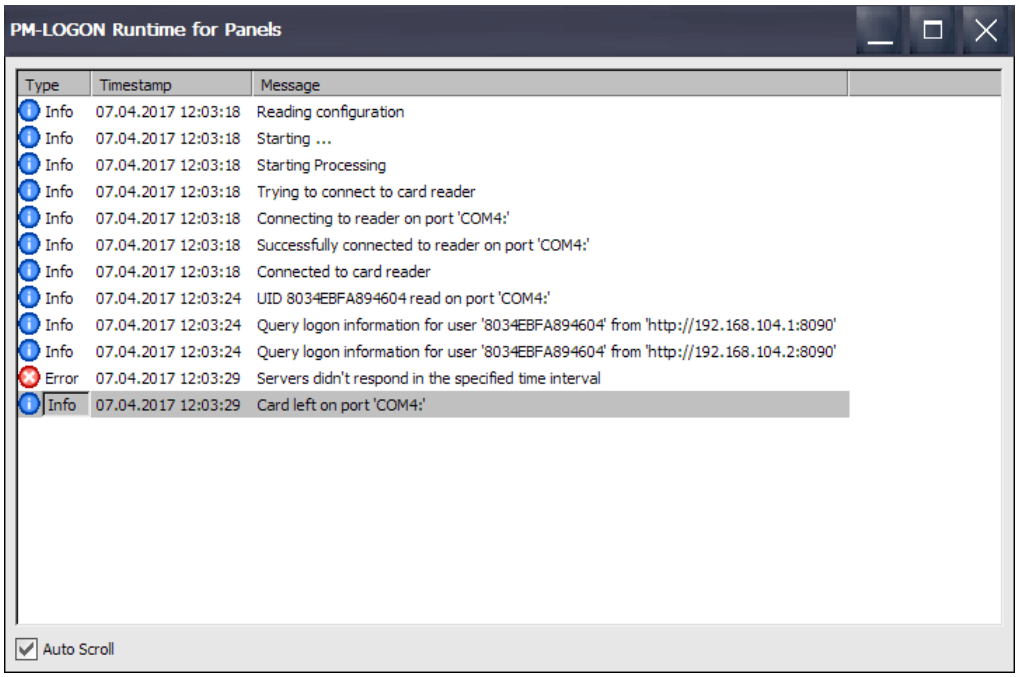
Card Reader	Reader Type	Selection of the card reading device. The following card readers are supported: • SIMATIC RF1040R/RF1060R/RF1070R • Admitto USB reader
	Serial Port	If “Admitto USB reader” has been selected as the card reader a serial port needs to be specified. By default this port is set to “COM4:”. Please note that for the addressing of a serial port a colon (:) at the end is required, e.g. “COM4:”
	Reverse UID	If different readers are used it may be required to reverse the byte order of the UID read from the device.
	Use AutoRead Mode	Only for RF1040R/RF1060R/RF1070R: If the option “Use AutoRead Mode” is activated the reader doesn’t read the card UID but automatically reads a configured memory block depending on the card type. For this it is necessary that the reader is prepared with an “AutoRead” configuration.
Security	Require password to access configuration	The configuration of the “PM-LOGON Configurator for Panels” can be protected against unauthorized access by specifying a password. If this option is activated and a password has been entered, this password will be required the next time “PM-LOGON Configurator for Panels” is started. The password can be changed by clicking the button “Set”.
	Hide UIDs in log	Since UIDs read from RFID cards might represent sensitive information, the UIDs can be hidden from the diagnostic log output.

Changes made to the configuration are saved when the OK button is clicked and the confirmation dialog that is displayed has been confirmed. Changed configuration settings only become active after the runtime has been restarted.

5.4 Diagnostics

The main window of PM-LOGON Runtime for Panels is shown only if the application has not been started in hidden mode (“Start hidden” in the configurator is deactivated) or if the window has been brought into the foreground by double clicking its tray icon:

The window displays a list with diagnostic entries that are sorted by timestamp in ascending order (new entries are always added to the end of the list). The list contains a maximum of 1000 entries.



If the system does not react as expected the log can be checked to narrow down the cause of the problem. In the above example e.g. both configured remote servers cannot be reached.

The diagnostic entries are not persistently stored.

New entries are added to the end to the list. If the option “Auto Scroll” is activated, the view will always be scrolled to the end of the list and the most recent entry will be selected. If another entry is selected manually by clicking on it, the “Auto Scroll” will be deactivated. The deactivated “Auto Scroll” prevents the list entries from moving in order to determine the cause of the problem at hand.

By using the minimize button the main window will be hidden, leaving the application actively running in the background. By double clicking the tray icon the main window can be brought back into view.

6 Changing the login password from a WinCC screen

6.1 Introduction

The password of a user login stored in PM-LOGON and also in the window user management can be changed from within a WinCC screen. In order to do this a screen needs to be created with the required internal tags. Additionally a VB script will be needed that utilizes a so called COM-Object("PMLogon.RuntimeCOMAccess") that has been installed together with the setup routine of PM-LOGON, which offers the required functionality to change the password in parallel in both locations.
In order to enable the COM-object to access the PM-LOGON Runtime the runtime has to be started and the web service has to be enabled (Configuration->Webservice, see. chapter. 4.3)

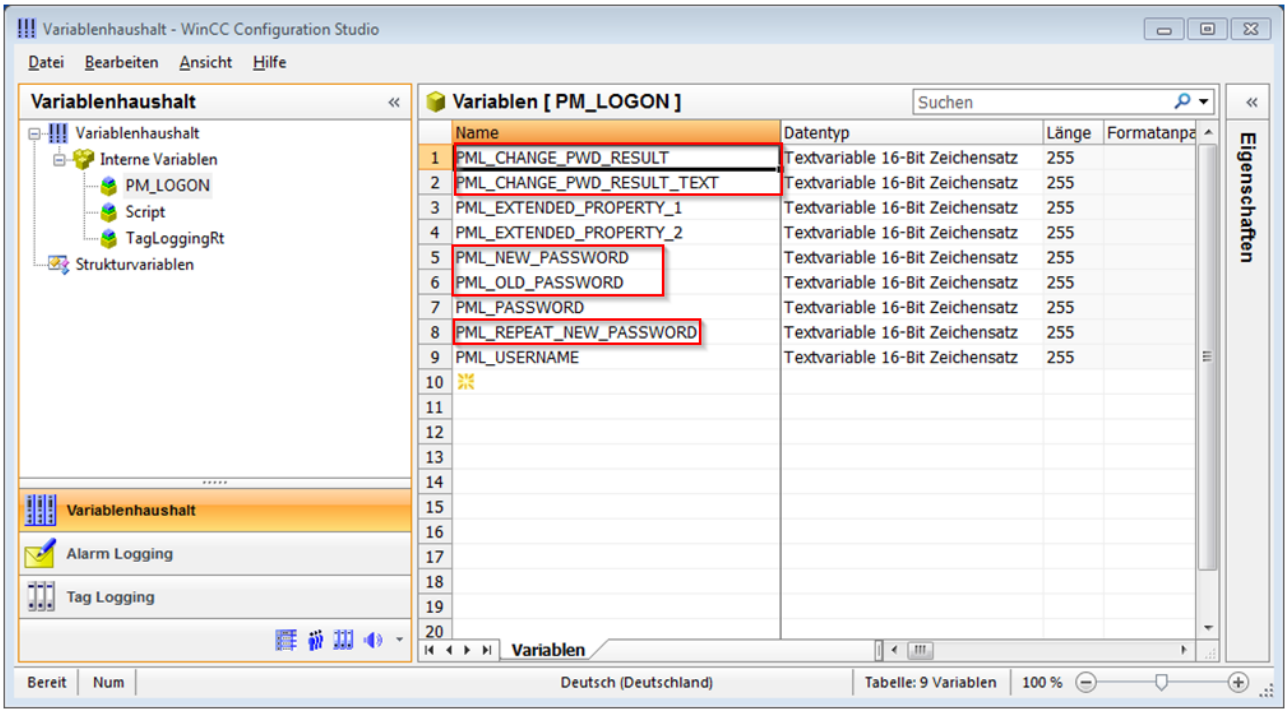
Note:
If the user repository “Local Computer” is used, the PM-LOGON Runtime has to be executed under a Windows account with administrative privileges. In this case it is preferable to automate the startup of the PM-LOGON Runtime by using the Windows scheduled task feature as opposed to

the default autostart mechanism. The reason for this is that with the scheduled tasks feature the account that is to be used for the application to start can be explicitly specified.

6.2 Creating the WinCC screen

The “ChangePassword()” method that performs the actual password changing action requires the following three parameters:
The currently logged in user, the old password and the new password.

First all required tags need to be created.
The following internal tags are needed:



For the execution of the “ChangePassword” method the following tags are relevant:

- The system tag “@CurrentUserName” provides the currently logged in user.
- “PML_OLD_PASSWORD” is used to stored the old password.
- The tag “PML_NEW_PASSWORD” is used to hold the new password.

Additionally:

- “PML_REPEAT_NEW_PASSWORD” is used in the script to provide a location to store the repeated new password in order to make sure that the repeated new password matches
- “PML_CHANGE_PWD_RESULT” is used to hold the result of the ChangePassword operation.

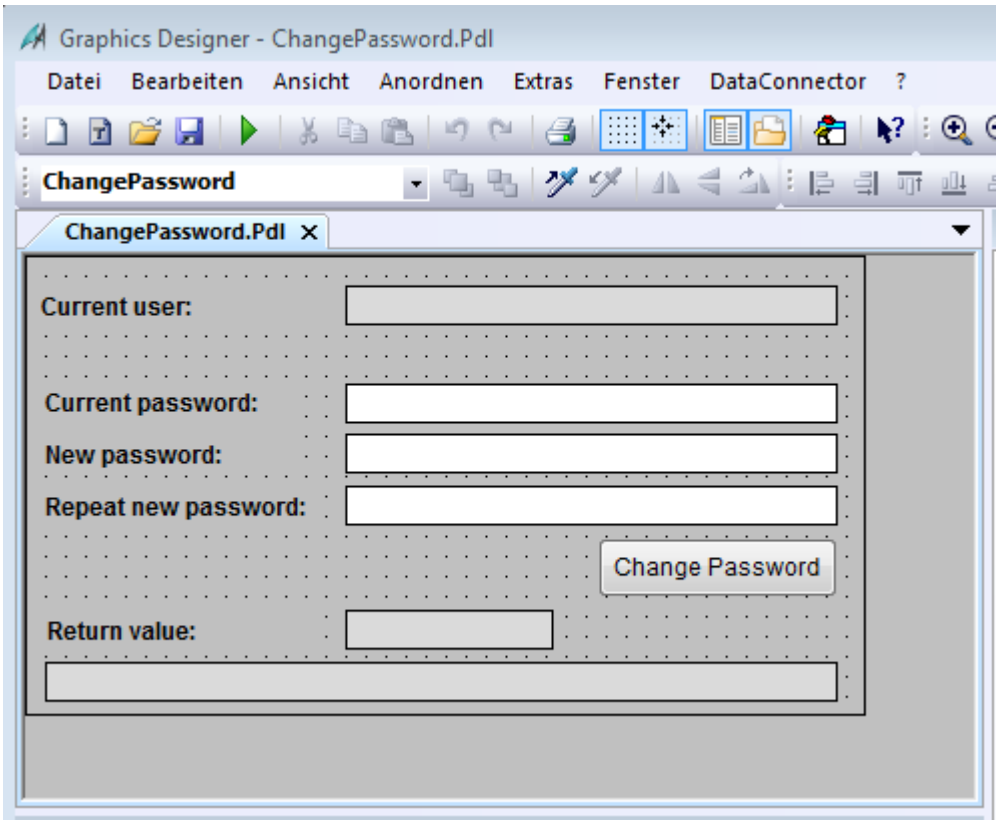
  The method provides the following return codes:
  0: The password has been successfully changed
  -1: The user name provided was not found
  -2: The old password provided does not match the current login password
  -3: Password violates the complexity policy, is too short, or similar
  -4: Connection to PM-LOGON Runtime Webservice could not be established

-5: The current password could not be decrypted
-6: The user has no UID assigned
-99: Unknown error

The corresponding error messages can be assigned within the script based on the return value of the function.
Detailed error messages will also be displayed in the diagnostic output of the PM-LOGON Runtime.

- Optional “errorcode”, which can be used to indicate success or failure of the operation with a different color on the HMI screen.

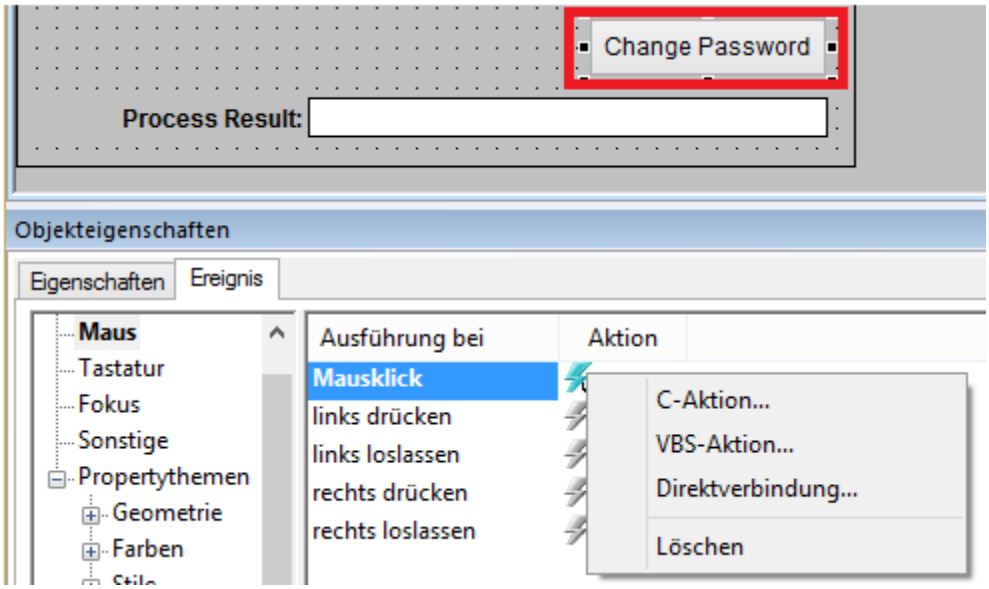
The HMI screen could be built as shown in this example:



The IO-fields have to be connected to the corresponding WinCC tags previously created. Finally two VB scripts need to be added.

6.3 VB Scripts

In order to access the COM-interface a script needs to be created.

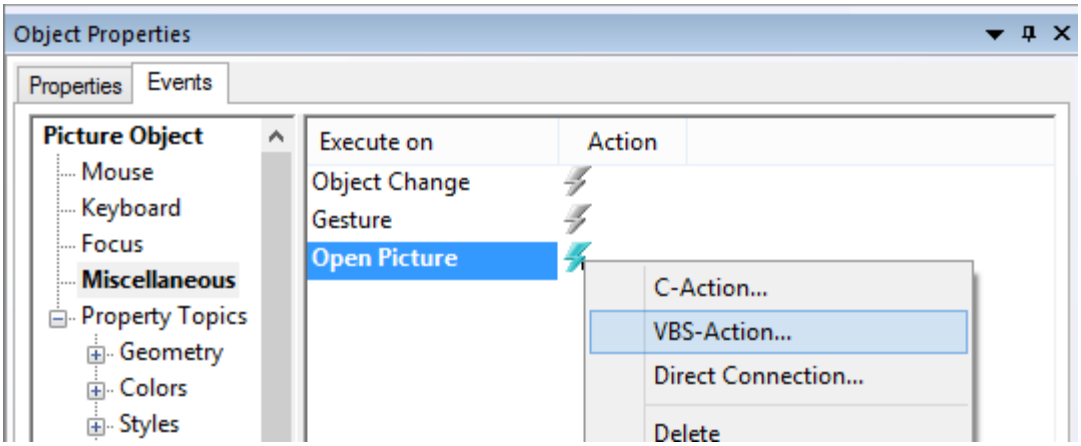


For this purpose you can create a button that executes the following script in the OnClick Event:

```
Sub OnClick(ByVal Item)

  Dim result
  Dim logonRuntime
  Dim changePwdResult

HmiRuntime.SmartTags("PML_CHANGE_PWD_RESULT_TEXT") = ""
HmiRuntime.SmartTags("PML_CHANGE_PWD_RESULT") = ""

'Create COM interface PMLogon.RuntimeCOMAccess
  Set logonRuntime = CreateObject("PMLogon.RuntimeCOMAccess")

'Initialize COM interface with URI the PM-LOGON Runtime Webservice
logonRuntime.Init("http://localhost:8090")

'Get current user's username
  Dim currentUserName
currentUserName = HmiRuntime.SmartTags("@CurrentUser")

  'Check, if current username contains the domain prefix and cut it off
  Dim userNameSplits :userNameSplits = Split(currentUserName,"/")

  If UBound(userNameSplits) > 0 Then
      currentUserName = userNameSplits(1)
  End If

'Check old and new passwords
  Dim oldpw :oldpw = HmiRuntime.SmartTags("PML_OLD_PASSWORD")
  Dim newpw :newpw = HmiRuntime.SmartTags("PML_NEW_PASSWORD")
  Dim repeatpw :repeatpw = HmiRuntime.SmartTags("PML_REPEAT_NEW_PASSWORD")

  If newpw<>repeatpw Then
HmiRuntime.SmartTags("PML_CHANGE_PWD_RESULT_TEXT") = "New passwords do not
                                                     match."

HmiRuntime.SmartTags("PML_CHANGE_PWD_RESULT") = -1
    Exit Sub
```

```
  End If

'Call ChangePassword function of PM-LOGON COM interface
result = logonRuntime.ChangePassword (currentUserName, oldpw, newpw)

  If result = 0 Then
HmiRuntime.SmartTags("PML_CHANGE_PWD_RESULT_TEXT") = "Password updated
                                                      successfully."
  Else
HmiRuntime.SmartTags("PML_CHANGE_PWD_RESULT_TEXT") = "Error - Password
                                                     could not be updated."
  End If

HmiRuntime.SmartTags("PML_CHANGE_PWD_RESULT") = result

Set logonRuntime = Nothing

End Sub
```

Additionally a small script is required that resets the result value in the OnOpen event of the screen:




```
Sub OnOpen()

  Dim changePwdResult
  Set changePwdResult = HMIRuntime.Tags("PML_CHANGE_PWD_RESULT")
  changePwdResult.Write" "

End Sub
```

6.4 Further methods PM-LOGON Runtime COM Interface

The PM-LOGON Runtime COM interface provides the following additional methods:

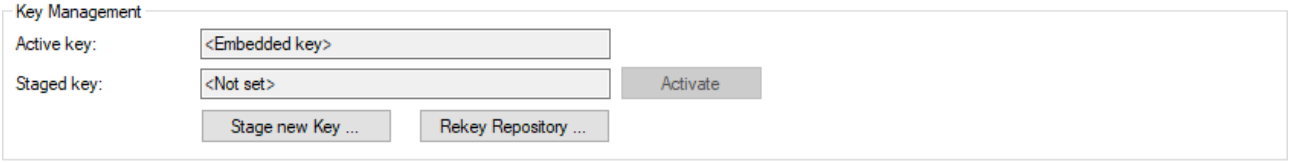
- **AssignPassword**(string username, string password):
  If only the user's current password is to be stored in PM-LOGON's user repository without changing it in Windows (since this may have already been done previously via operating system mechanisms), the method AssignPassword can be called.
  The method AssignPassword() must be supplied the user name and the current login password of the user. The supplied password is validated against the user repository before being assigned. If the supplied password does not match the login password, the password will not be applied.

These methods can only be used via the HTTPS web service of the PM-LOGON Runtime.

7 Key Management

7.1 Introduction

PM-LOGON uses a predefined key (<Embedded key>) to encrypt UID and password in the respective user repository. This key can be replaced by a user-defined key as of V1.8. The keys are managed via the configuration interface of the user repository in the section "Key Management".



The configured keys of the repository are displayed here.
The "Active key" is the key currently used by the PM-LOGON Configurator to encrypt UID and password of a PM-LOGON user. "<Embedded key>" refers to the predefined key that is embedded in PM-LOGON.
"Staged key" refers to the key that has been prepared for future use.
A user-defined key is valid only for the particular user repository (Local Computer/Active Directory) for which it was created.
User-defined keys can only be used if all PM-LOGON Configurator and all PM-LOGON Runtime instances have been upgraded to V1.8 or higher.

The creation of a user-defined key is described using the "Active Directory" repository as an example but can be done in the same way for the "Local Computer" repository.

Procedure:

1. First, a user-defined key is generated via PM-LOGON Configurator and stored on a license dongle.
2. The license dongle is then used to distribute the user-defined key to all PM-LOGON Runtime instances.
   Before the next steps it must be ensured that all PM-LOGON Runtime instances have received the new key, otherwise no user can be logged in.
3. After all PM-LOGON Runtime instances have received the user-defined key, the rekeying of the user credentials in the user repository is performed via the PM-LOGON Configurator. During this process, the UID and password of all PM-LOGON users are encrypted with the user-defined key.
   If you have not yet created any PM-LOGON users in your repository or this is a new installation, no rekeying is required and you can proceed directly with the activation of the key.
4. After the rekeying process, the user-defined key must be activated for PM-LOGON to use the user-defined key to encrypt the UID and password.
   From this point on PM-LOGON Configurator will only use the new key.

7.2 Staging a user-defined key

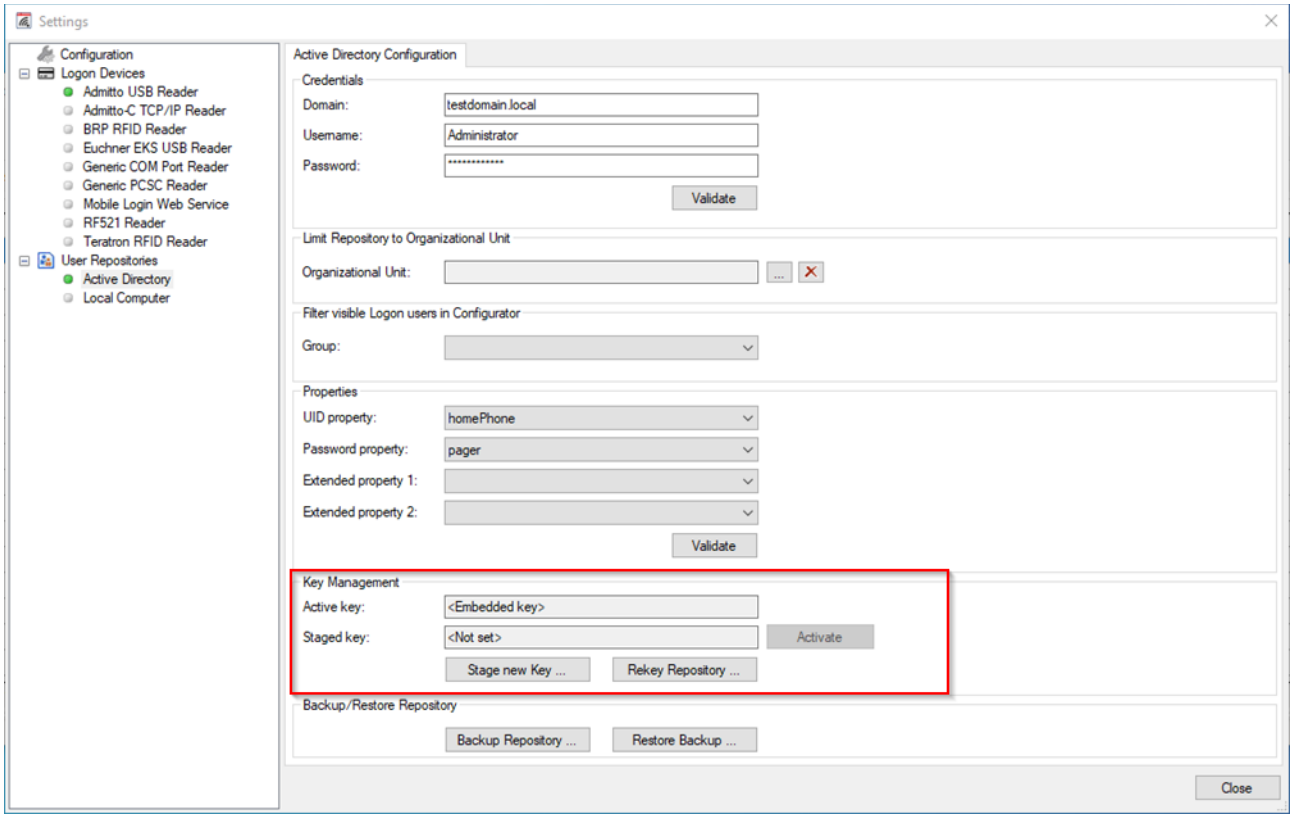
A user-defined key can be created in the PM-LOGON Configurator via the configuration interface of the user repository (Local Computer/Active Directory) in the section "Key Management".
For this, a special key dongle is required, which is included in all deliveries of PM-LOGON base packages from V1.8.

If you are using an older version of PM-LOGON prior to version 1.8 and want to update to version 2.0, please contact the WinCC Competence Center Mannheim (mailto:winccaddon.automation@siemens.com) to obtain such a key dongle.

The first step is the so called "Staging". During "Staging", a new key is prepared for use in the PM-LOGON Configurator/Runtime.

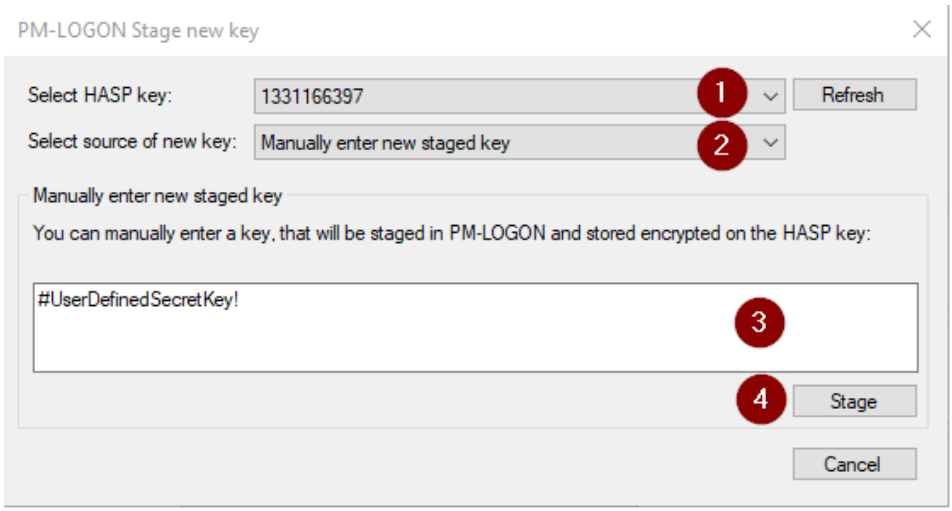
To create the user-defined key, the key dongle must be connected to the computer running the PM-LOGON Configurator instance.

Open the configuration interface of your user repository via the menu "File->Configuration" in PM-LOGON Configurator.



Press the "Stage new Key ..." button to open the staging dialog:

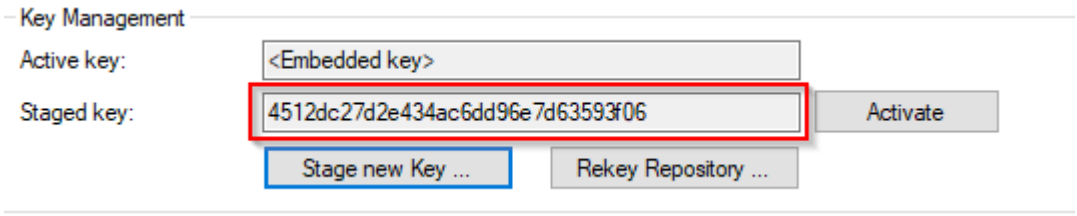
If the key dongle is connected correctly, the ID of the dongle (HASP key) is displayed in the selection list (1).
Select the entry "Manually enter new staged key" in the selection list (2).
Enter your user-defined key in the input field (3) and press the "Stage" button (4) to accept the key as the "Staged key".



The user-defined key is now stored in encrypted form on the key dongle and transferred to the configuration of the user repository as "Staged key".

If another key has already been stored on the key dongle, it will be overwritten by the new key. The previous key is moved to the list of previous keys. The last 10 keys are stored in this list. The list can be viewed via the entry "Previous key on HASP key".
You can also use a previous key as a "Staged key" via this function.

In the display field for the “Staged key” in the section “Key Management” of the user repository, the hash code of the key is now displayed to make it easier to identify.



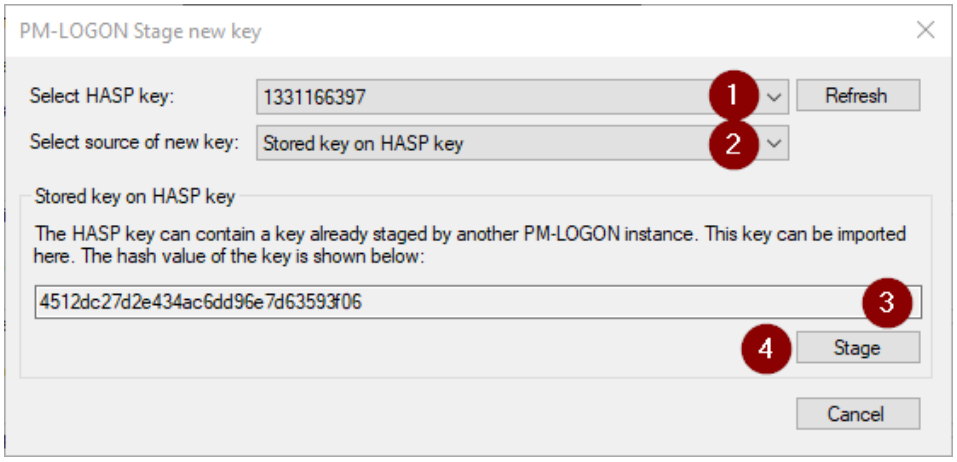
After the new user-defined key has been created, it must first be distributed to all PM-LOGON Runtime instances and, if existent, to all further PM-LOGON Configurator instances, before it can be activated.

7.3 Distributing the user-defined key

After creation, the user-defined key must be distributed to all PM-LOGON Runtime instances and, if existent, to all further PM-LOGON Configurator instances, before it can be activated.
PM-LOGON Runtime for Panel instances are excluded from this, they do not need a user-defined key.
For the transfer of the user-defined key, the key dongle on which the user-defined key has been stored, must be connected to the computer on which the PM-LOGON Configurator/Runtime instance is operated.

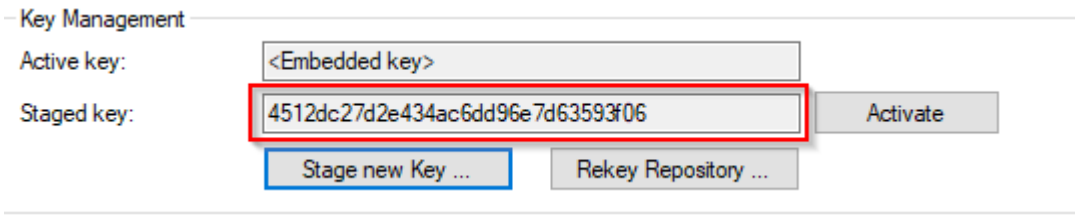
Then, open the configuration interface of the respective user repository via the menu "File->Configuration" in PM-LOGON Configurator.

If the key dongle is connected correctly, the ID of the dongle (HASP key) is displayed in the selection list (1).
Select the entry "Stored key on HASP key" in the selection list (2) "Stored key on HASP key":
The user-defined key is now displayed in the display field (3).



Press the "Stage" button (4) to accept the key as a "Staged key".

In the display field for the “Staged key” in the section “Key Management” of the user repository, the hash code of the key is now displayed to make it easier to identify.



From this point on, PM-LOGON Runtime will use both keys to find the user assigned to the UID in the user repository. This way it is ensured that a user can be logged in, even after rekeying the user repository.

Proceed in this way for all further PM-LOGON Runtime and PM-LOGON Configurator instances.

7.4 Rekeying the user repository

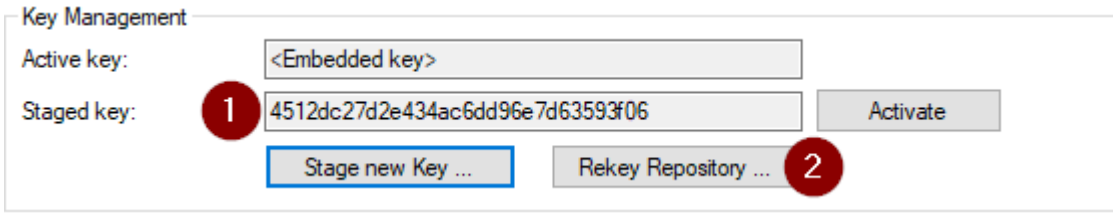
If the user repository already contains PM-LOGON users, you must perform the rekeying process. During this process, the credentials stored for each PM-LOGON user are decrypted using the previous key and then re-encrypted using the new key.

Before the next steps it must be ensured that all PM-LOGON runtime instances have been upgraded to PM-LOGON V2.0 or higher and have received and staged the new key, otherwise no user logon can take place.

For the rekeying process, the key dongle must be connected to the computer running the PM-LOGON Configurator instance.

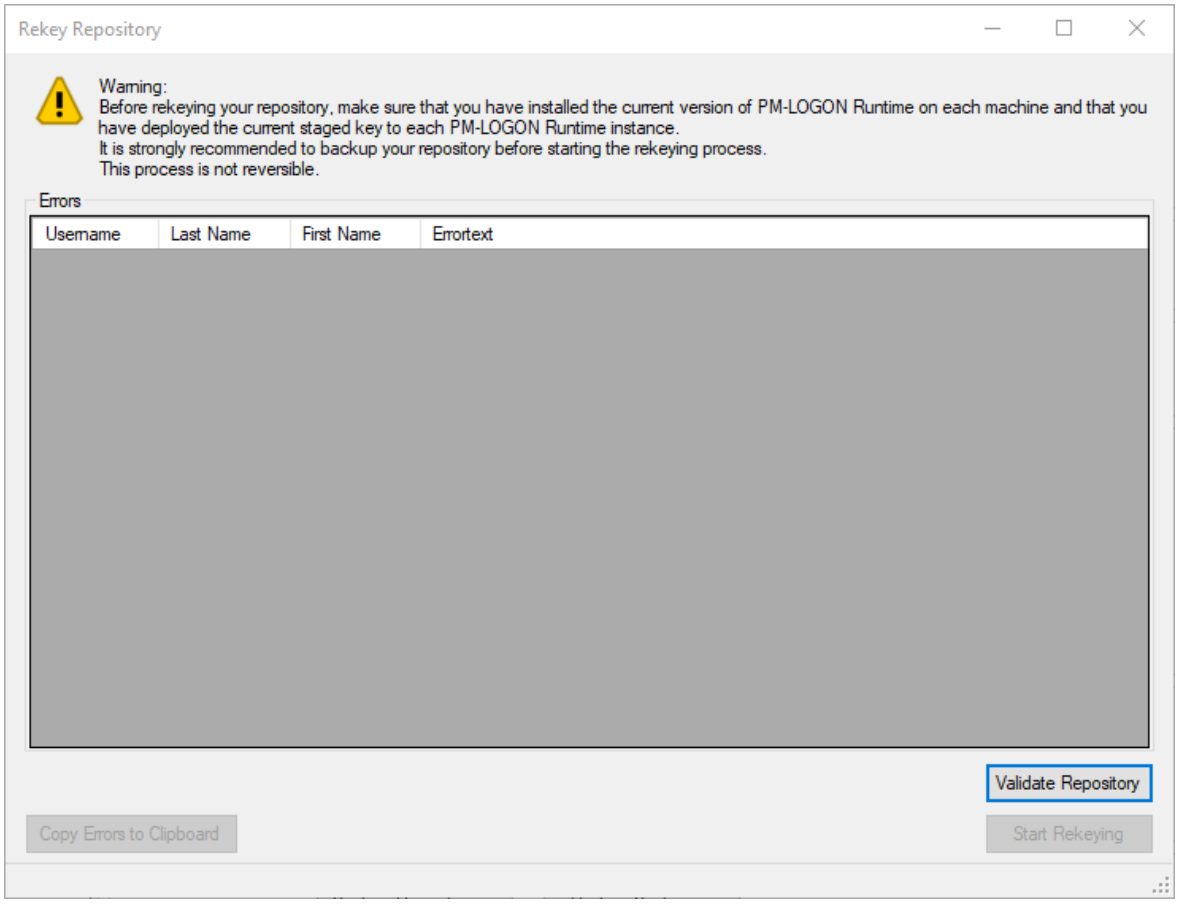
It is strongly recommended to backup the user repository before rekeying as described in chapter 8.1.

Open the configuration interface of the respective user repository via the menu "File->Configuration" in the PM-LOGON Configurator.

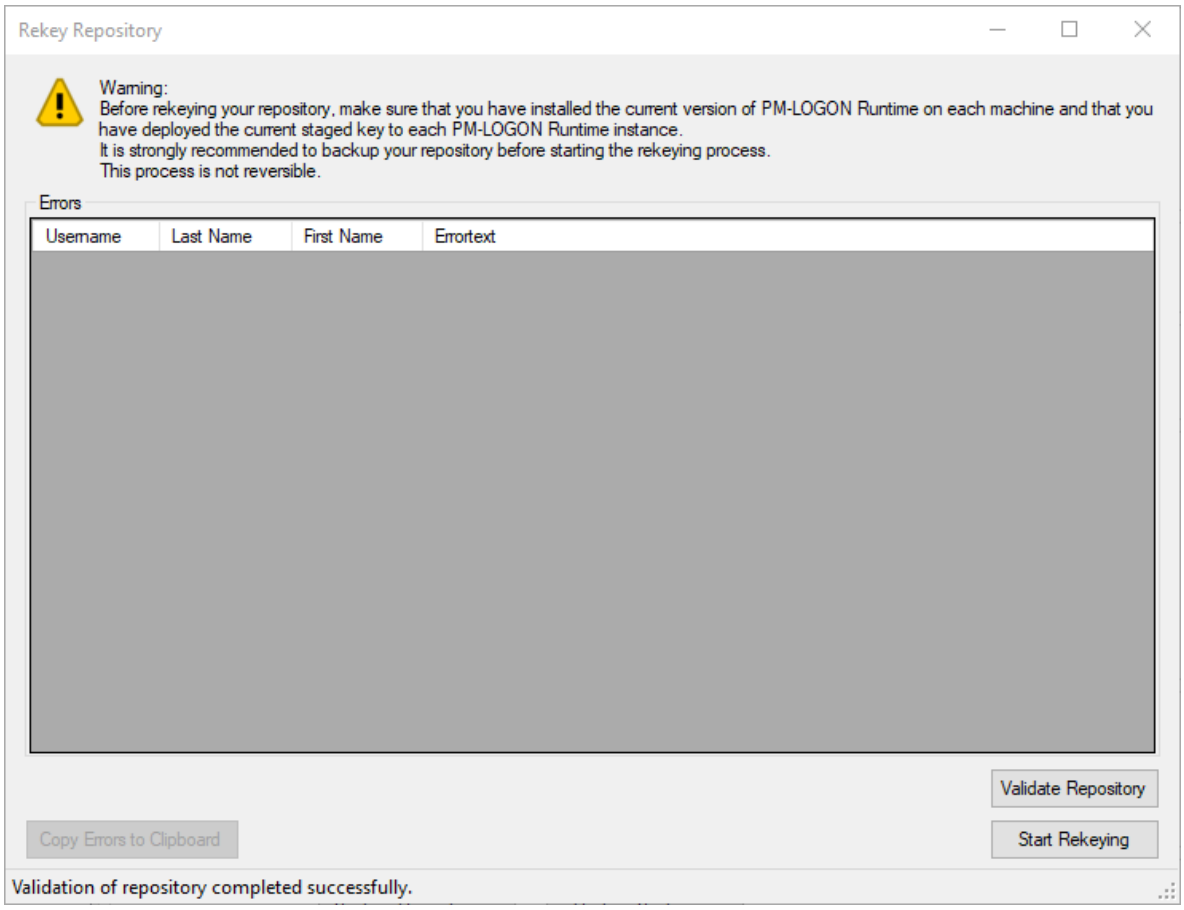


Make sure that the display field for the "Staged key" (1) shows the hash code of the key you created earlier.

Now press the "Rekey Repository …" button (2) to open the rekeying dialog.

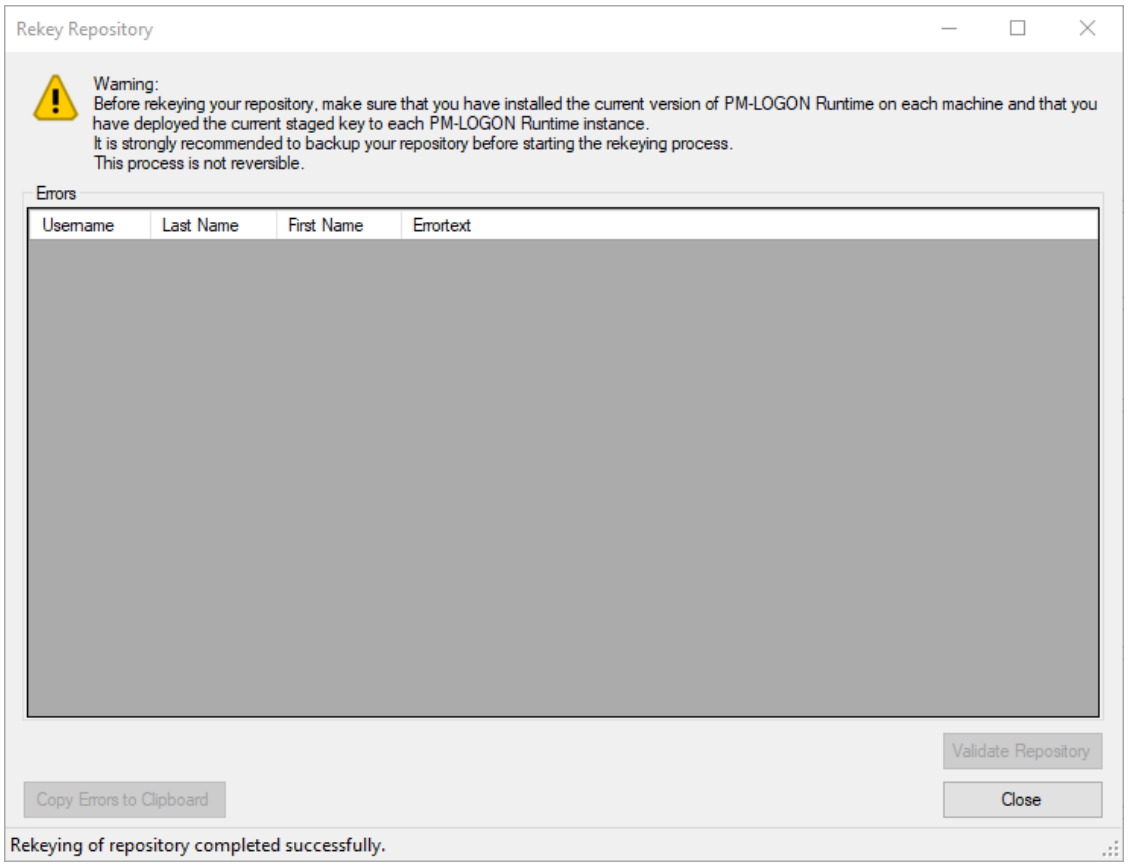


First, validate the user repository by clicking the "Validate Repository" button.
The validation of the repository ensures that the credentials of the PM-LOGON users can be decrypted with the current key ("Active key").
If errors occur during the validation of the repository, they are displayed in the section "Errors". It is recommended to fix any errors that may have occurred before the actual rekeying.
The list of errors can be copied to the clipboard using the "Copy Errors to Clipboard" button, in order to be able to store them in a text file, for example.



After successful validation, you can start the actual rekeying process.
To do this, press the "Start Rekeying" button.

The rekeying process is now executed. Wait until it has finished.
If errors occur during the rekeying process, they are listed in the section "Errors". In this case, correct the errors and run the rekeying process again.



Now close the rekeying dialog with the "Close" button.

If rekeying was successful, the "Staged key" will be activated automatically.
The rekeying process is now finished, PM-LOGON Configurator uses the new key for decryption and encryption.

If you run further PM-LOGON Configurator instances, you must activate the "Staged key" there manually (see chapter 7.5).

PM-LOGON Runtime will continue to use both keys even after rekeying. We therefore recommend activating the key in all PM-LOGON Runtime instances as soon as possible after rekeying the user repository, so that PM-LOGON Runtime does not use the old key anymore.

7.5 Activating the user-defined key

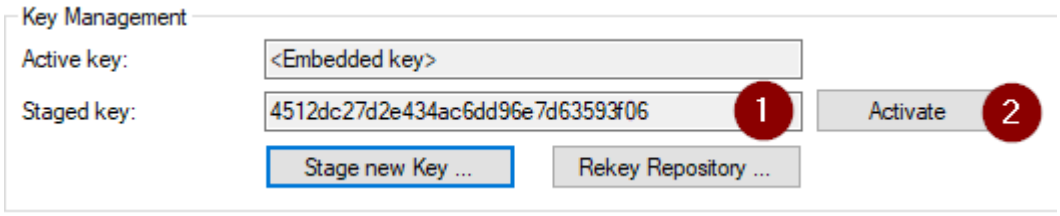
The "Staged key" must be activated manually in the following cases:

- If this is a new installation or if no PM-LOGON users are stored in the user repository yet, the "Staged key" can be activated directly without performing the rekeying process first.
- If several PM-LOGON Configurator instances are operated, the "Staged key" must be activated manually in all other instances after rekeying by one of the instances, so that they also use the new key afterwards.

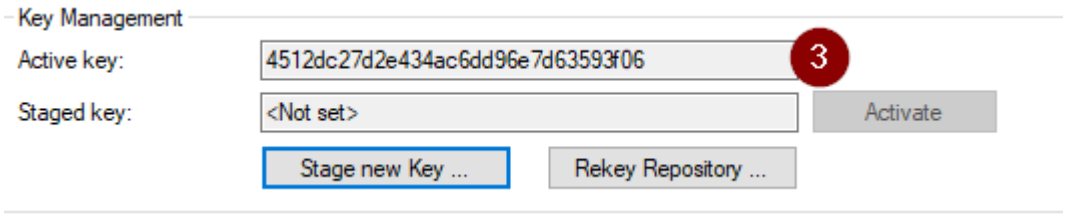
Open the configuration interface of the respective user repository via the menu "File->Configuration" in PM-LOGON Configurator or PM LOGON Runtime.

Make sure that the display field "Staged key" (1) shows the hash code of the key you have created before.

Now press the "Activate" button (2) to activate the "Staged key".



The hash code of the "Staged key" is displayed in the display field for the “Active key” (3) after activation.



8 Backup/Restore of a user repository

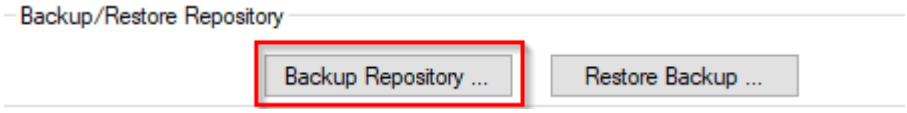
8.1 Create a backup of the user repository

You can create a backup of the user repository in the section "Backup/Restore Repository" of the user repository configuration interface.
The credentials stored for a user are encrypted and exported to an xml file.
This file can be used to restore the state of the user repository at the time the backup was created.

It is strongly recommended to create a backup of the user repository before rekeying.

Open the configuration interface of the respective user repository via the menu "File->Configuration" in the PM-LOGON Configurator.

Press the "Backup Repository" button in the section "Backup/Restore Repository".



In the next step, select a file name and a location to save the backup.

8.2 Restore a backup of the user repository

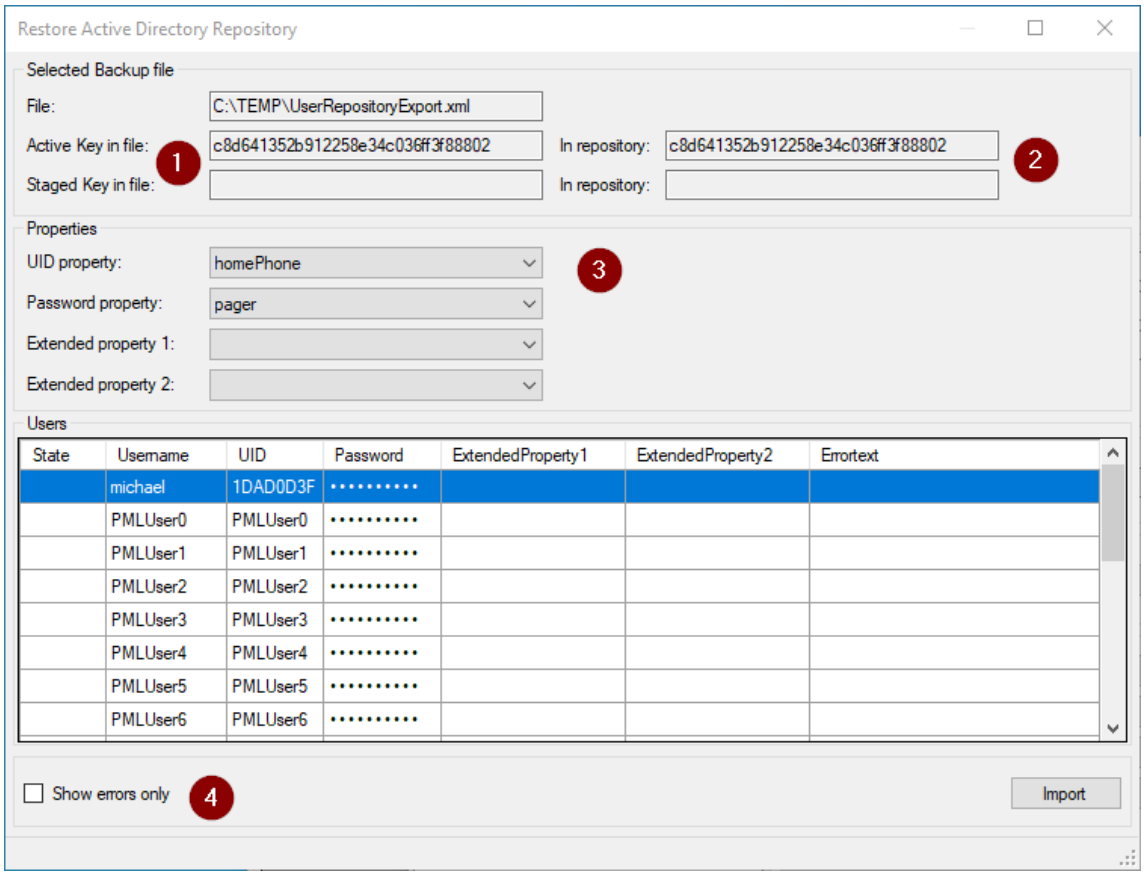
For the rekeying process, the key dongle must be connected to the computer on which the PM-LOGON Configurator instance is operated.

Via the configuration interface of the user repository you can restore a backup of the user repository in the section "Backup/Restore Repository".

Open the configuration interface of the respective user repository via the menu "File->Configuration" in the PM-LOGON Configurator.

Press the "Restore Repository" button in the "Backup/Restore Repository" section.

In the following file dialog, select the backup file you want to restore and open it.



The following dialog shows the keys that are currently assigned in the repository (2), as well as the keys from the backup file that were assigned at the time of the backup (1).

For the Active Directory repository, the user attributes to which the data should be restored can be selected in the Properties section. The attributes selected when opening the backup correspond to the configured attributes of the user repository at the time of the backup.

If the current "Active key" in the user repository is different from the "Active key" of the backup, PM-LOGON will try to decrypt the data using the list of predecessor keys on the key dongle and re-encrypt it using the current "Active key".
No changes are made to the current "Staged key" of the user repository by restoring the backup.

Make sure that no errors are displayed in the list of users. You can filter faulted records using the "Show Errors Only" checkbox.

Press the "Import" button to import the users.

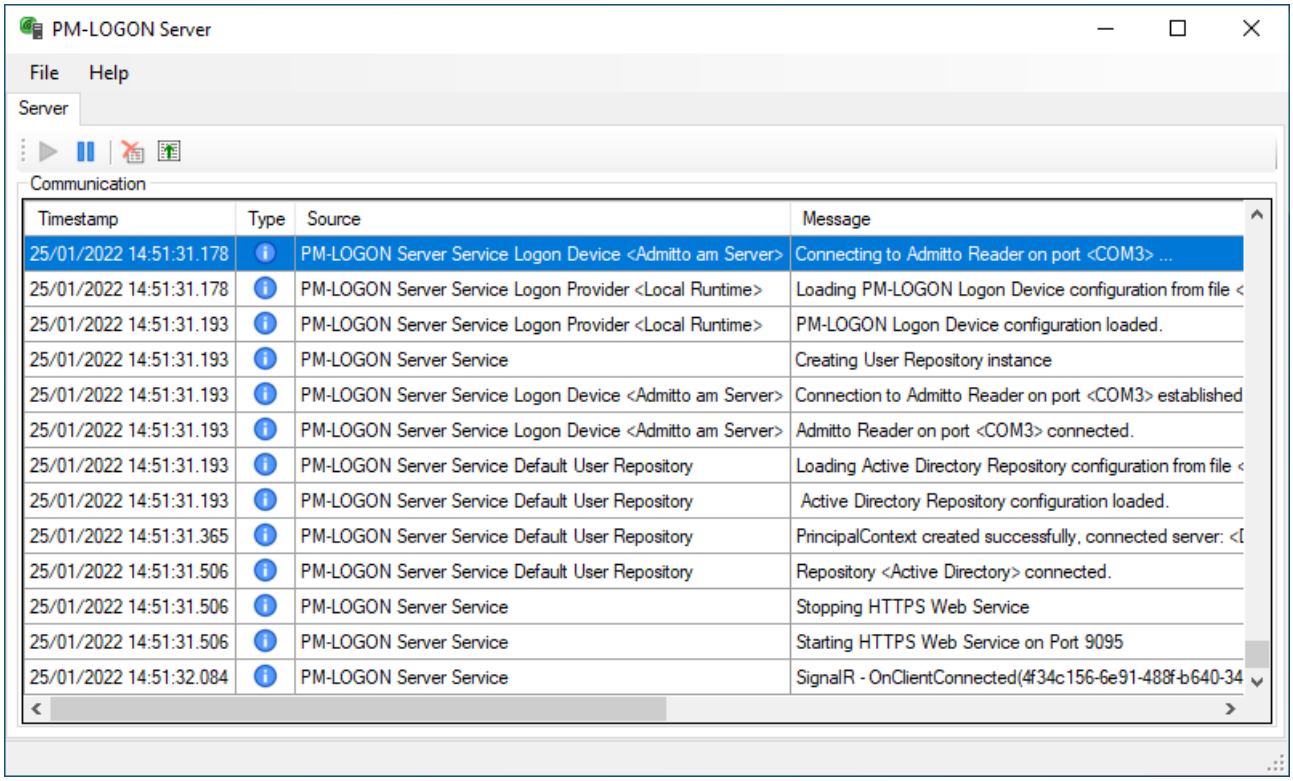
9 PM-LOGON Server

9.1 Introduction

PM-LOGON Server is a stand-alone application and basically has the same functionality as PM-LOGON Runtime. Unlike PM-LOGON Runtime, PM-LOGON Server can connect multiple Logon Devices. A logon to a device can be forwarded to multiple target systems, but unlike PM-LOGON Runtime, multiple target systems of the same type (e.g. OPC UA Server) can be addressed. Readers and target systems can be connected via so-called logon mappings, e.g. the logon to a reader can be passed on to several target systems as well as the logon to different readers can be passed on to the same target system.
Furthermore, a PM-LOGON Runtime instance can be used both as a logon device and as a logon provider with PM-LOGON Server. This means that the logon to a PM-LOGON Runtime instance can also be propagated to other PM-LOGON Runtime instances.

PM-LOGON Server supports all Logon Devices, which are also supported by PM-LOGON Runtime.
Furthermore, all Logon Providers of PM-LOGON Runtime are supported except SIMATIC Logon. Since PM-LOGON Server is operated exclusively as a service and an interactive user is required to log on to SIMATIC Logon, it is not possible to log on to SIMATIC Logon via PM-LOGON Server itself.
PM-LOGON Server must be licensed via a corresponding hardware or software license.

9.2 Application Window

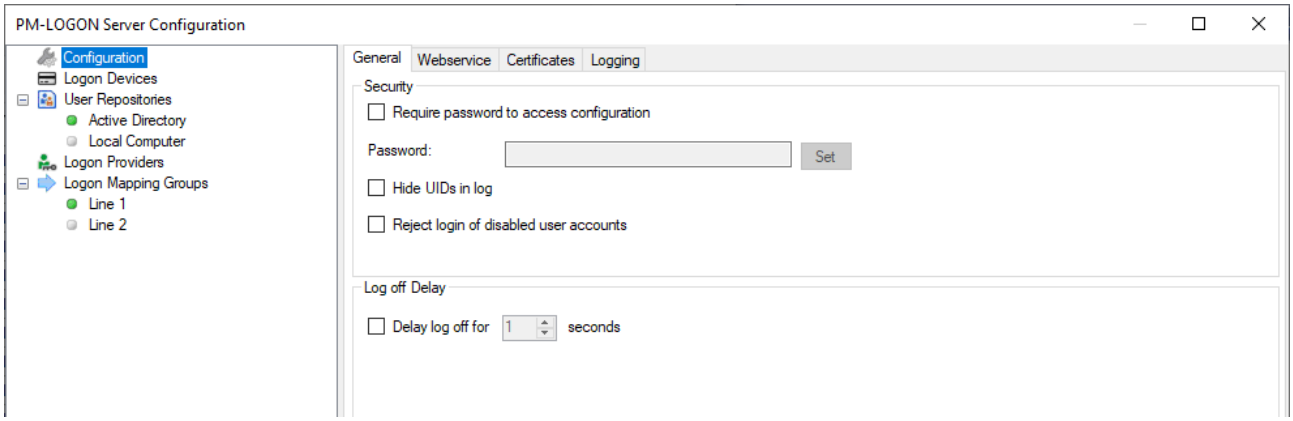


The user interface of PM-LOGON Server can be accessed via the corresponding entry in the start menu.

In the main window of the application program runtime information of PM-LOGON Server is displayed. Using the individual buttons in the toolbar PM-LOGON Server can be started ("Start") and stopped ("Stop") and the list of program flow information can be cleared ("Clear Log").
Via the button "AutoScroll" the AutoScroll function can be activated/deactivated.

9.3 Configuration

Open the configuration of PM-LOGON Server via the menu
File->Configuration. The configuration dialog of PM-LOGON Server will be opened.



Via the tree structure on the left side of the configuration dialog you can navigate within the different configuration sections.

Via the "Configuration" element you reach the general configuration of PM-LOGON Server.

The configuration of "PM-LOGON Server" can be protected against unauthorized access. If the checkbox "Require password to access configuration" is activated, a password can be assigned, which must be entered when opening the configuration. The password can be changed using the "Set" button.

Since read UIDs from RFID cards can represent information that is worth protecting, these UIDs are made unrecognizable in the diagnostic output if the "Hide UIDs in log" checkbox has been selected.

If the "Reject disabled users" checkbox is selected, PM-LOGON will reject logins for user accounts that are disabled in the user repository (e.g. Active Directory).

Using the "Delay log off for x seconds" setting in the "Log off Delay" section, the log off can be delayed for up to 15 seconds after the card is removed from the reader field. To delay the logoff, the option "Log off current user" has to be selected as "Log off behavior" in the respective Logon Provider and the PM-LOGON reader used signals the removal of the card from the field. If the card leaves the reader field and returns within the set time period, the log off process is aborted and the previously logged on user remains logged on. If another card is brought into the field within the set time period after leaving the reader field of a card, the logout process is also aborted and the user is logged in to this card.

Via the "Webservice" tab you can configure the web service of PM-LOGON Server, which is especially necessary for logging on to panels via PM-LOGON Runtime for Panels.

Via the "Certificates" tab you can manage the security certificates that PM-LOGON Server uses for secure data exchange with OPC UA servers and other PM-LOGON Runtime instances.

The "Logging" tab can be used to activate the output of program flow information in log files for diagnostic purposes.

The "Logon Devices" element takes you to the configuration of the connected readers.

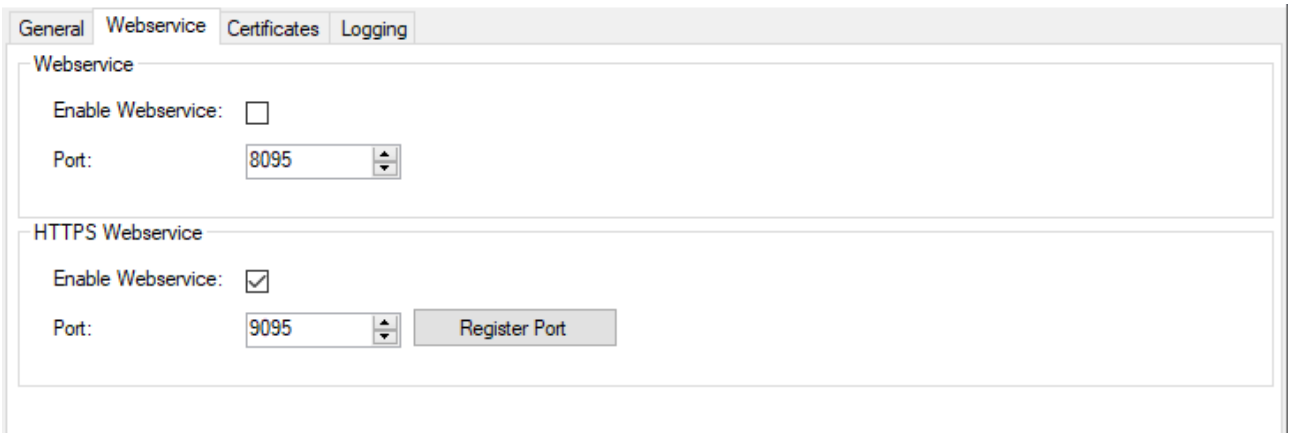
The "User Repositories" element takes you to the overview of the supported user administrations, below which are the configuration sections of the individual user repositories.

The "Logon Providers" element takes you to the configuration of the connected logon services.

The "Logon Mapping Groups" element takes you to the configuration of the logon groups.

PM-LOGON Server can be extended by additional readers, user administrations and logon services via a plugin system.

9.3.1 Configuration of the Webservices



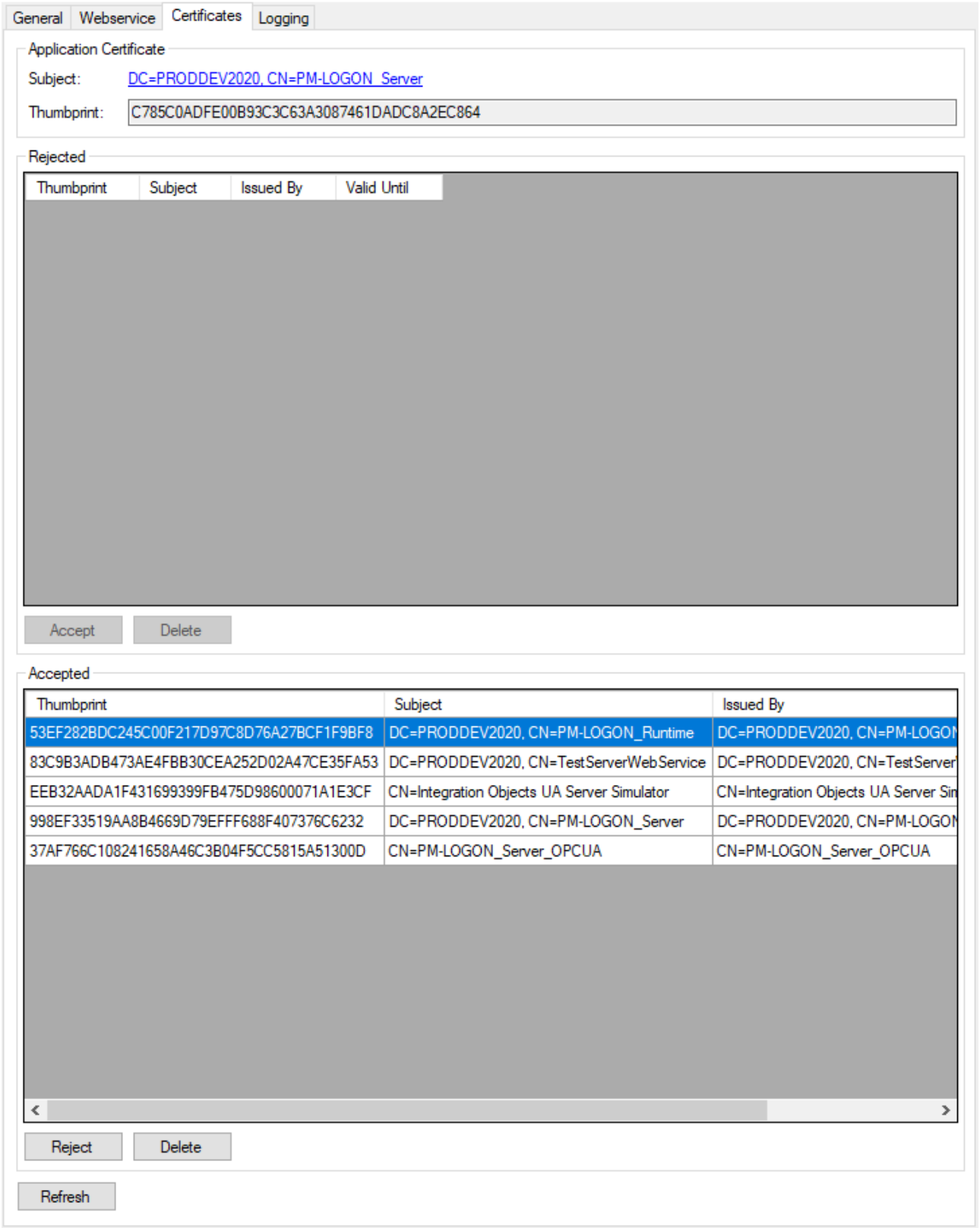
The PM-LOGON Server web service is required if it is operated together with other remote PM-LOGON Runtime or PM-LOGON Runtime for Panels instances.

PM-LOGON Server provides both HTTP and HTTPS web service.
PM-LOGON for Panels instances always use HTTP web service, for connection between PM-LOGON Runtime and Server instances only HTTPS web service is supported.

To establish an HTTPS connection, a port must be reserved to link it to the PM-LOGON application certificate. The default port is already reserved by the installation of PM-LOGON Server, so that the port only needs to be reserved via the "Register Port" button when a change is made.

Activate the respective web service via the corresponding checkbox.

9.3.2 Certificate management



Via the configuration section "Certificates" you can manage the security certificates, PM-LOGON Server uses for secure data exchange with OPC UA servers and other PM-LOGON Runtime instances.

In the "Application Certificate" section the subject and thumbprint of the application certificate of PM-LOGON Server are specified.

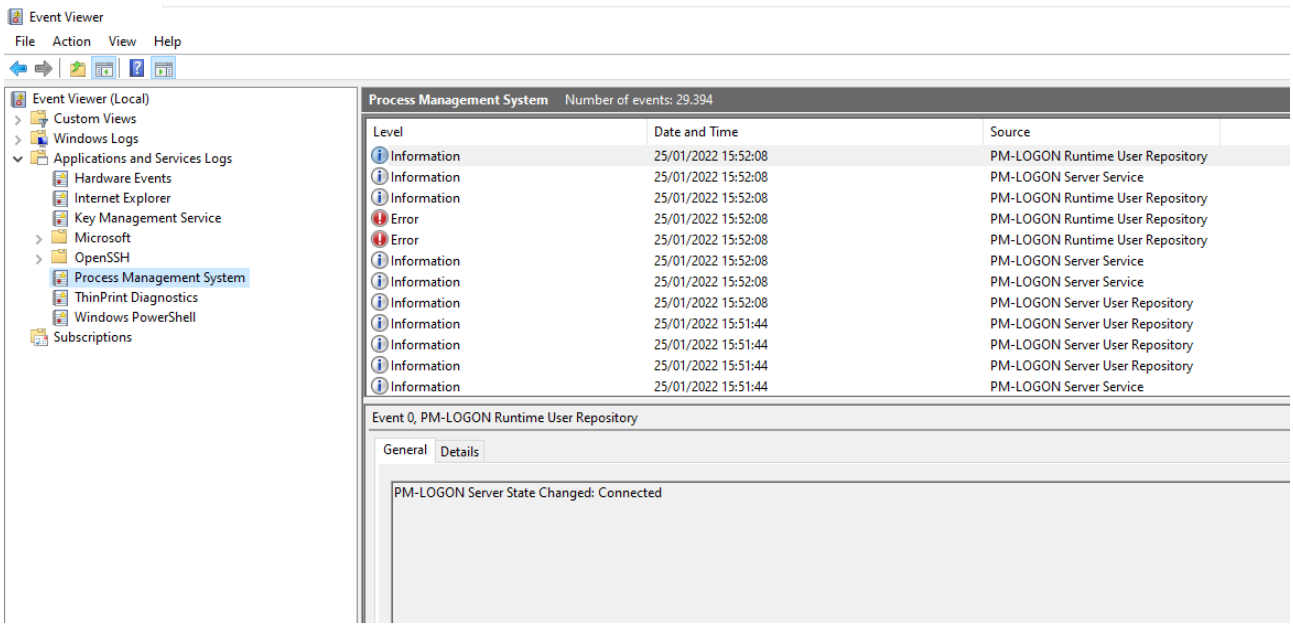
In the section "Rejected" all certificates of communication partners are listed, which have not yet been accepted by PM-LOGON Server and thus have been classified as trustworthy.
Via the buttons "Accept" these certificates can be accepted and thus transferred to the section "Accepted".

The "Accepted" section lists all certificates that have been accepted by PM-LOGON Server and thus classified as trustworthy. Already accepted certificates can be rejected by clicking the "Reject" button.

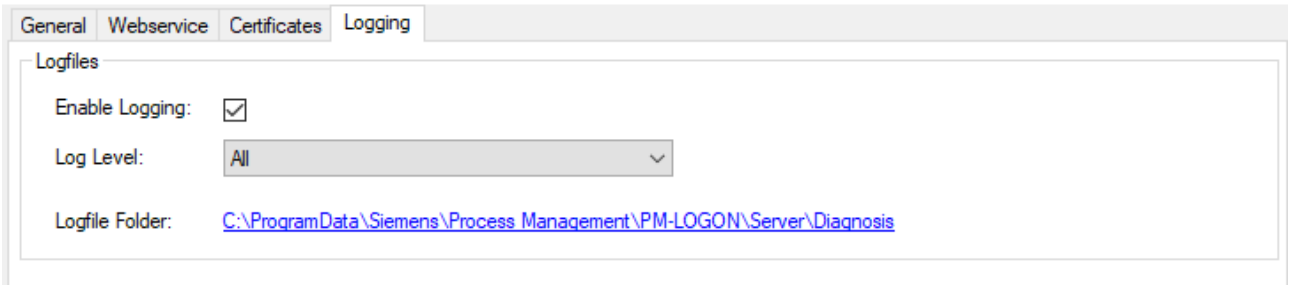
Via the button "Delete" certificates can be deleted from the sections "Rejected" and "Delete".

9.3.3 Diagnosis

PM-LOGON Server logs events during the program execution to the Windows event log. The events are logged under the Event Log "Process Management" system.



The "Logging" tab in the configuration can be used to additionally activate the logging of program run information in log files ("Enable Logging").

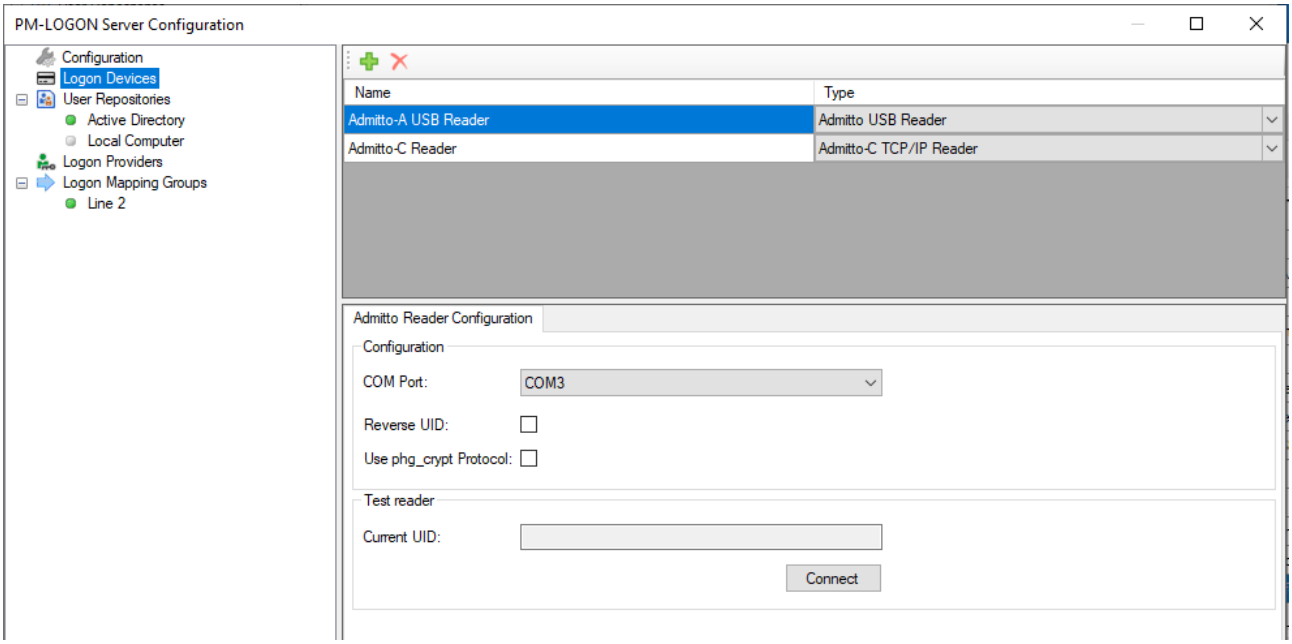


The scope of the logged program run information can be set via the "Log Level" drop-down list:

- All:
  All messages
- Error:
  Only errors
- Warning:
  Warnings and errors
- Information:
  Information messages, warnings and errors
- Verbose:
  Detail information, Information messages, warnings and errors

File logging should only be activated for diagnosing problems and should not be activated permanently. The size of the log files is limited to 10MB and the log files are automatically deleted after 7 days. The folder where the log files are stored can be opened by clicking the link to the right of the label “Logfile Folder”.

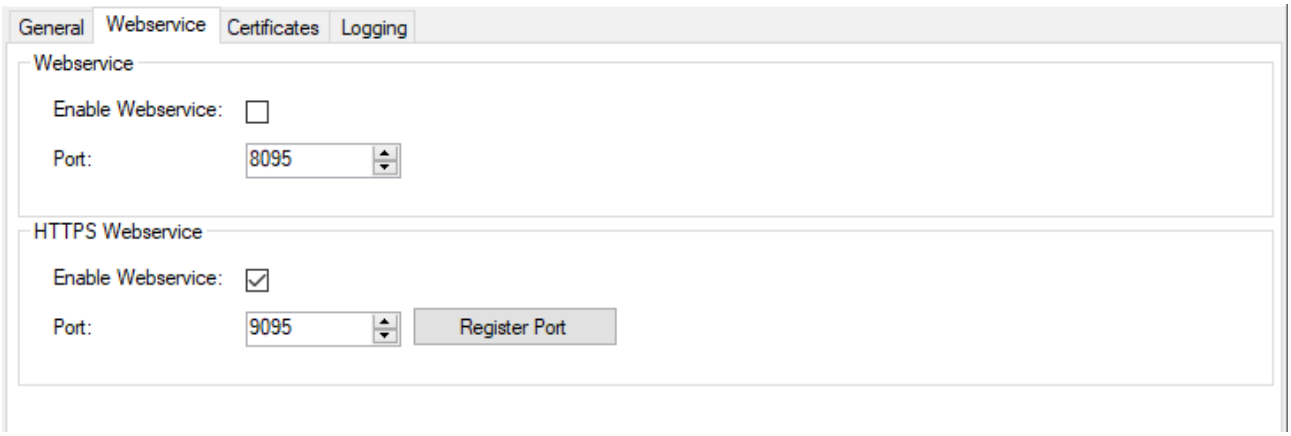
9.3.4 Configuration of Logon Devices



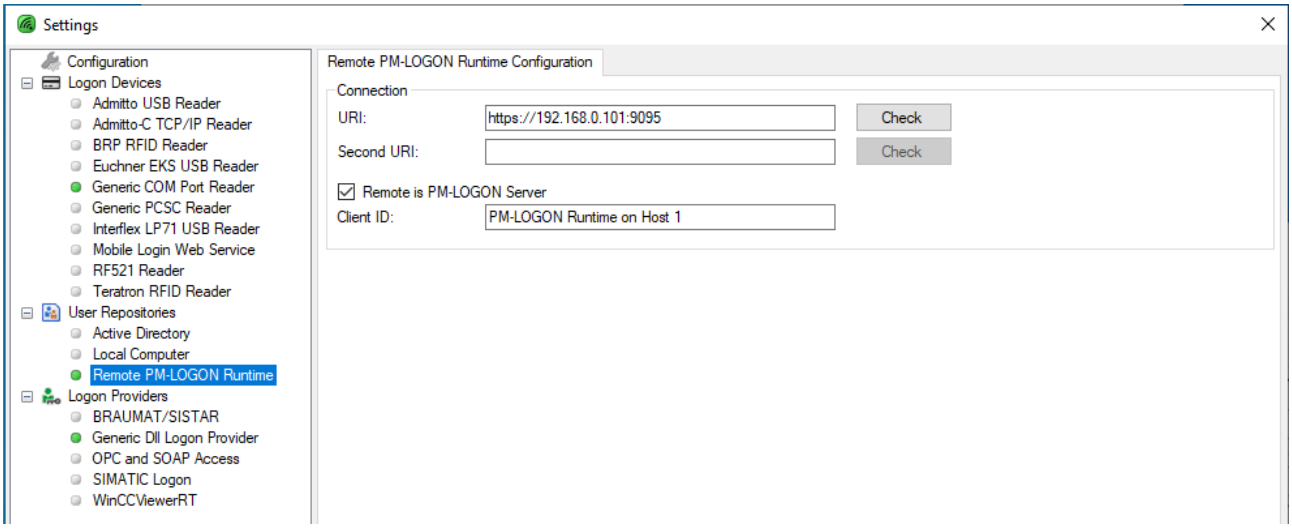
The "Logon Devices" section in the tree structure of the configuration interface takes you to the overview of configured readers. You can use the buttons in the upper section of the list to add further readers or delete existing readers.
Assign a unique designation for the Logon Device in the "Name" field of the corresponding line.
Use the drop-down list in the "Type" column to specify the type of the Logon Device
Below the list of Logon Devices the configuration interface corresponding to the type of Logon Device is displayed, which can be used to configure the plugin for the reader.
The configuration for the respective Logon Device types can be taken in detail from chapter 3.2.3 ff.

9.3.4.1 PM-LOGON Runtime as a Logon Device

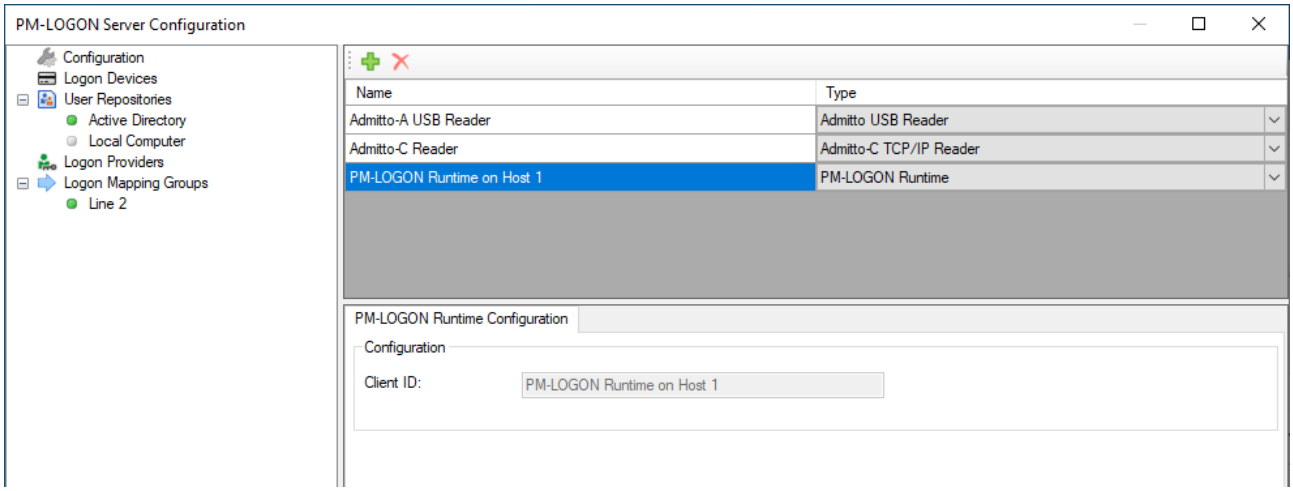
A PM-LOGON Runtime instance can also be used as a Logon Device. This allows e.g. the reader at the local PM-LOGON Runtime to be connected to PM-LOGON Server or a logon at a PM-LOGON Runtime to be passed on to further Logon Providers.
For this purpose, the HTTPS web service of PM-LOGON Server must be activated and configured first (see chapter 9.3.1).



After that the PM-LOGON Runtime instance must be connected to PM-LOGON Server.
For this purpose, the remote repository must be used as the user repository in the configuration of PM-LOGON Runtime (see chapter 4.3.14).

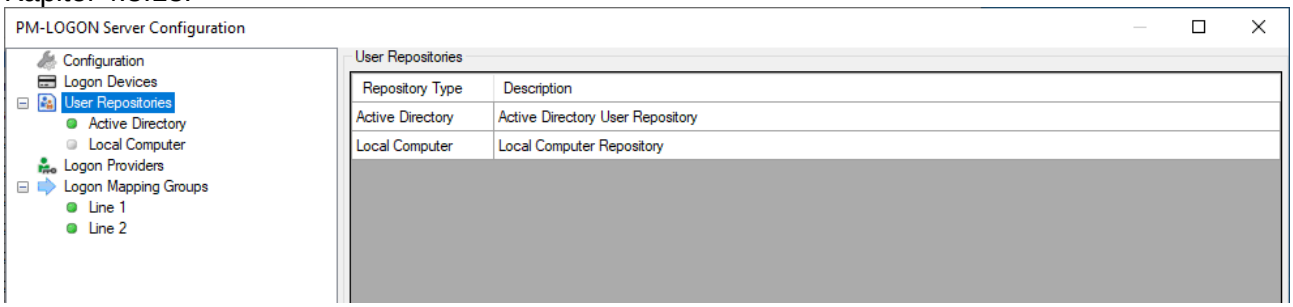


After a successful connection the PM-LOGON Runtime instance registers itself with PM-LOGON Server. In the list of Logon Devices the PM-LOGON Runtime instance is automatically added as a new entry.

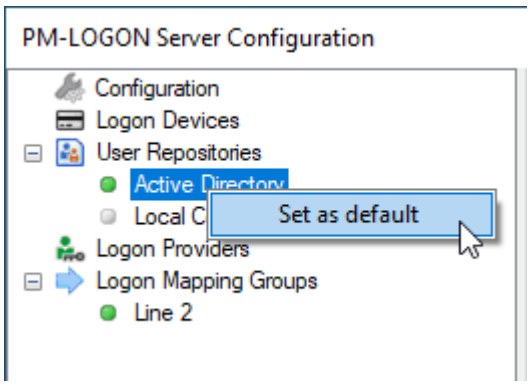


9.3.5 Configuring the User Repository

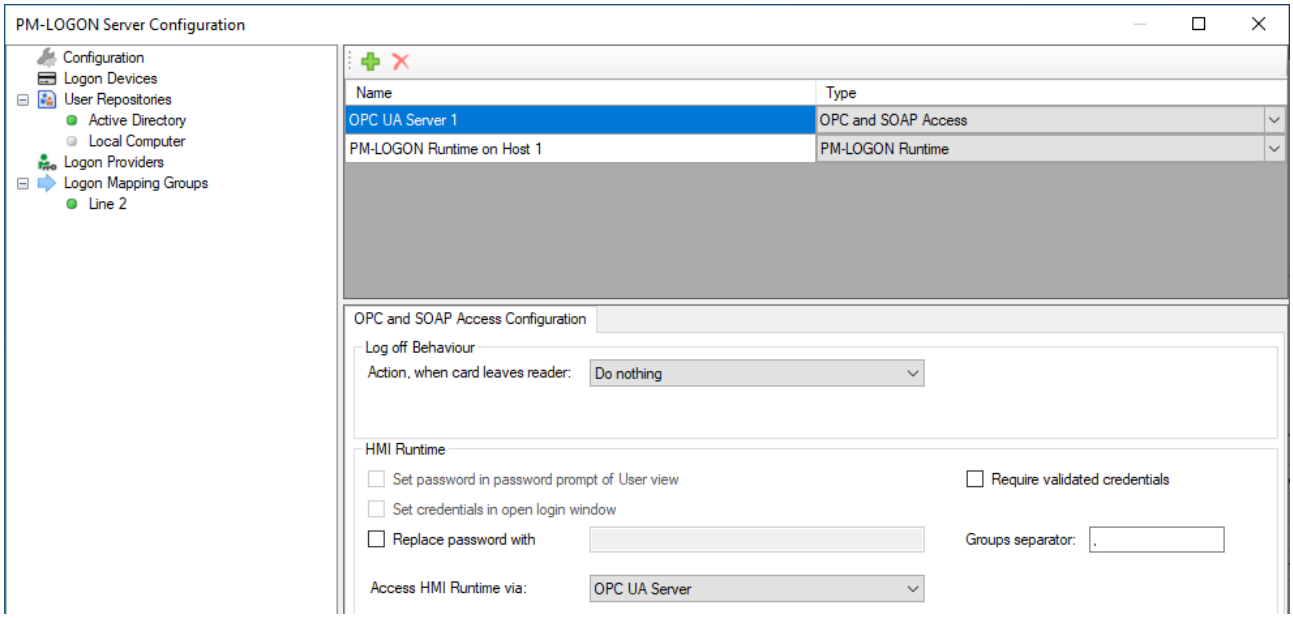
PM-LOGON Server supports Active Directory or local user management as a user repository. Details about the configuration of the respective user repository can be found in chapter 4.3.12 and Kapitel 4.3.13.



The user repository to be used must be activated through the context menu of the respective plugin.



9.3.6 Configuration of the Logon Providers

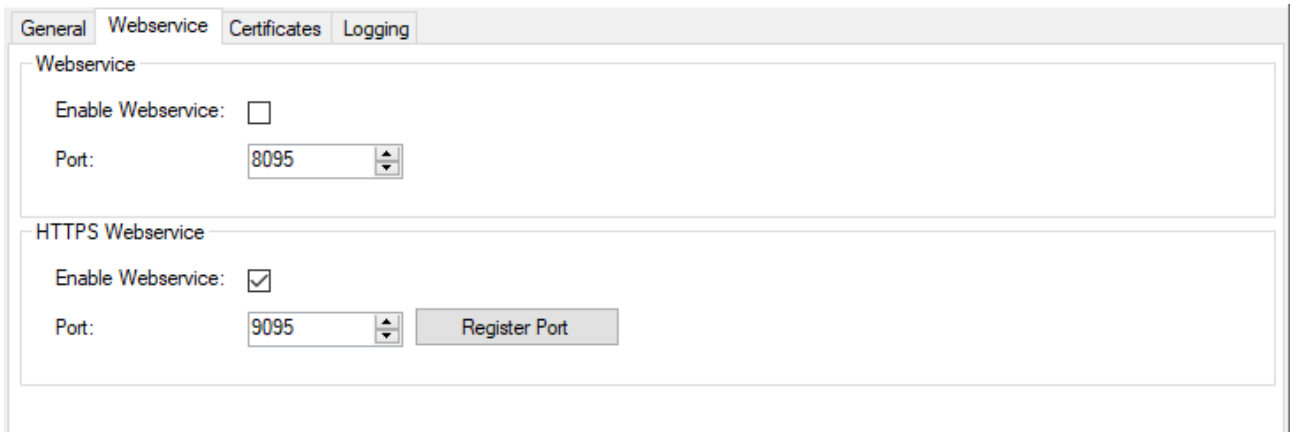


The "Logon Providers" section in the tree structure of the configuration interface takes you to the overview of configured logon providers. You can use the buttons in the upper section of the list to add further logon providers or delete existing logon providers.
Assign a unique name for the logon device in the "Name" field of the corresponding configuration line.
Use the drop-down list in the "Type" column to specify the type of logon provider.
Below the list of Logon Providers, the configuration interface corresponding to the type of Logon Provider is displayed, which can be used to configure the plugin for the Logon Provider.
The configuration for the respective logon provider types can be found in detail in chapter 4.3.17 ff.

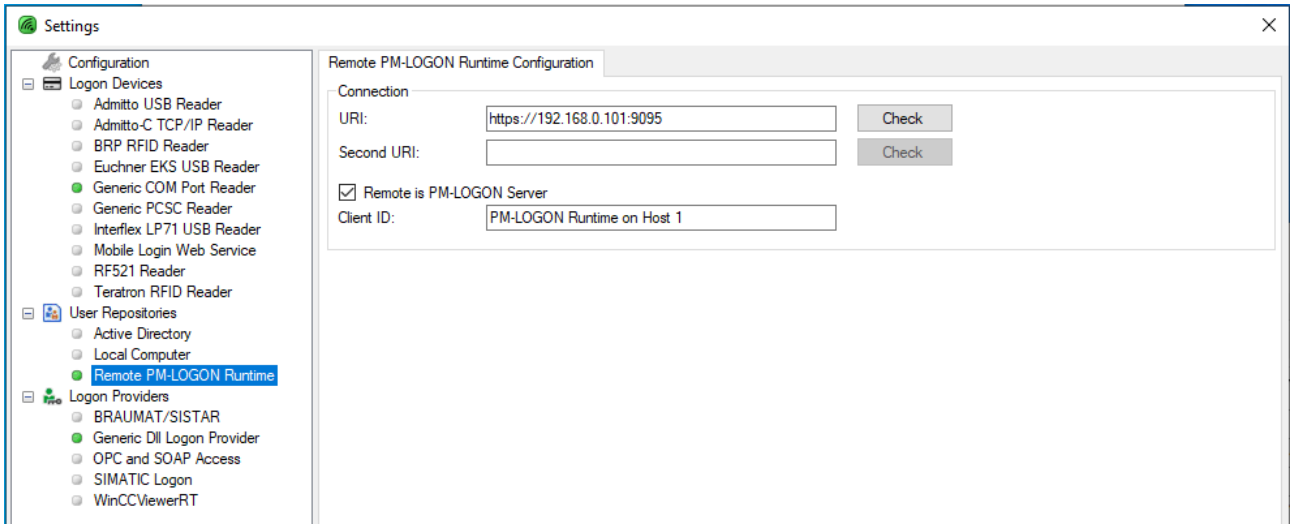
9.3.6.1 PM-LOGON Runtime as a Logon Provider

A PM-LOGON Runtime instance can also be addressed as a Logon Provider. This can be used, for example, to propagate a logon to a reader or another PM-LOGON Runtime instance.

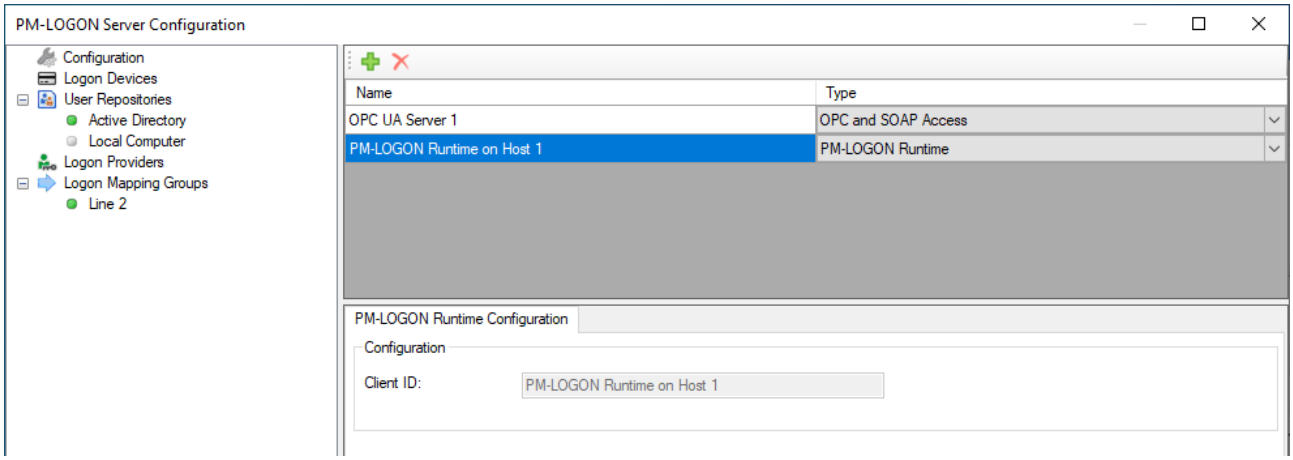
For this purpose, the HTTPS web service of PM-LOGON Server must first be activated and configured (see Chapter 9.3.1).



After that the PM-LOGON Runtime instance must be connected to PM-LOGON Server.
For this purpose, the remote repository must be used as the user repository in the configuration of PM-LOGON Runtime (see chapter 4.3.14).

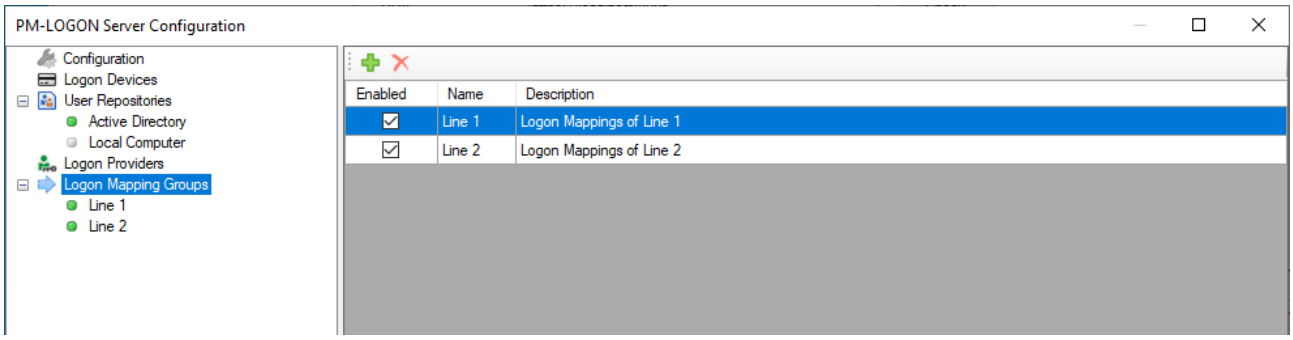


After a successful connection the PM-LOGON Runtime instance registers itself with PM-LOGON Server. In the list of logon providers the PM-LOGON Runtime instance is automatically added as a new entry.



9.3.7 Configuration of Logon Mapping Groups

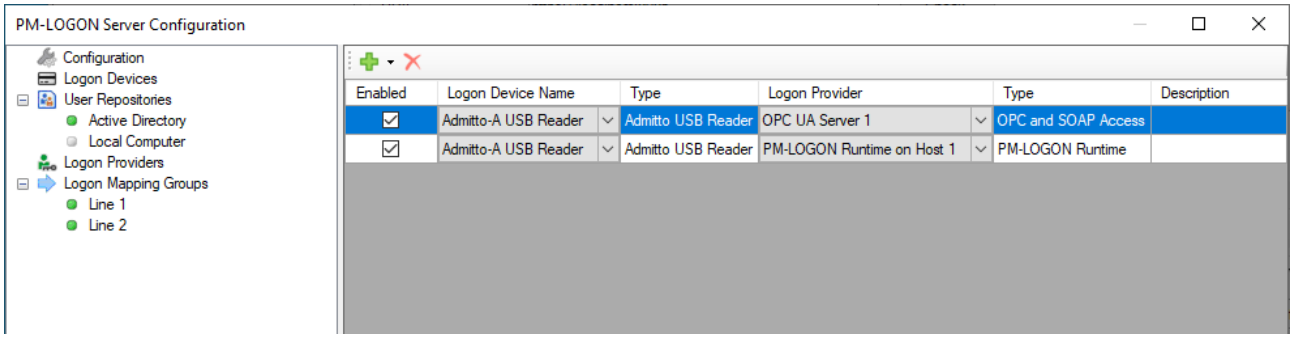
Logon Mapping Groups can be used to configure which logon events are transmitted to which logon providers.
Within a Logon Mapping Group it is defined which Logon Devices are connected to which Logon Provider(s).



The "Logon Mapping Groups" section in the tree structure of the configuration interface takes you to the overview of the defined logon mapping groups. You can use the buttons in the upper part of the list to add further logon mapping groups or delete existing logon mapping groups.
Assign a unique name for the logon mapping group in the "Name" field of the corresponding configuration line. In the "Description" field, you can enter a description for the logon mapping group.
Individual mapping groups can be activated or deactivated via the checkboxes in the "Enabled" column.

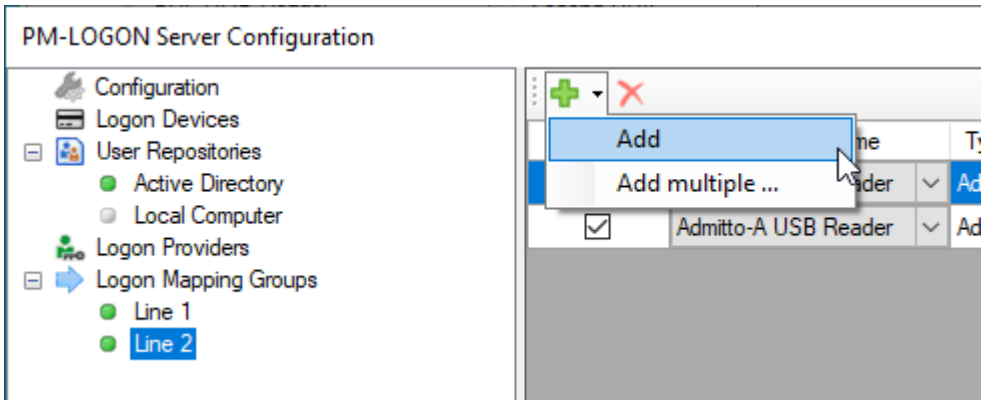
9.3.8 Configuration of Logon Mappings

To configure the logon mappings within a logon mapping group, select the corresponding entry of the logon mapping group in the tree structure below the "Logon Mapping Groups" section.



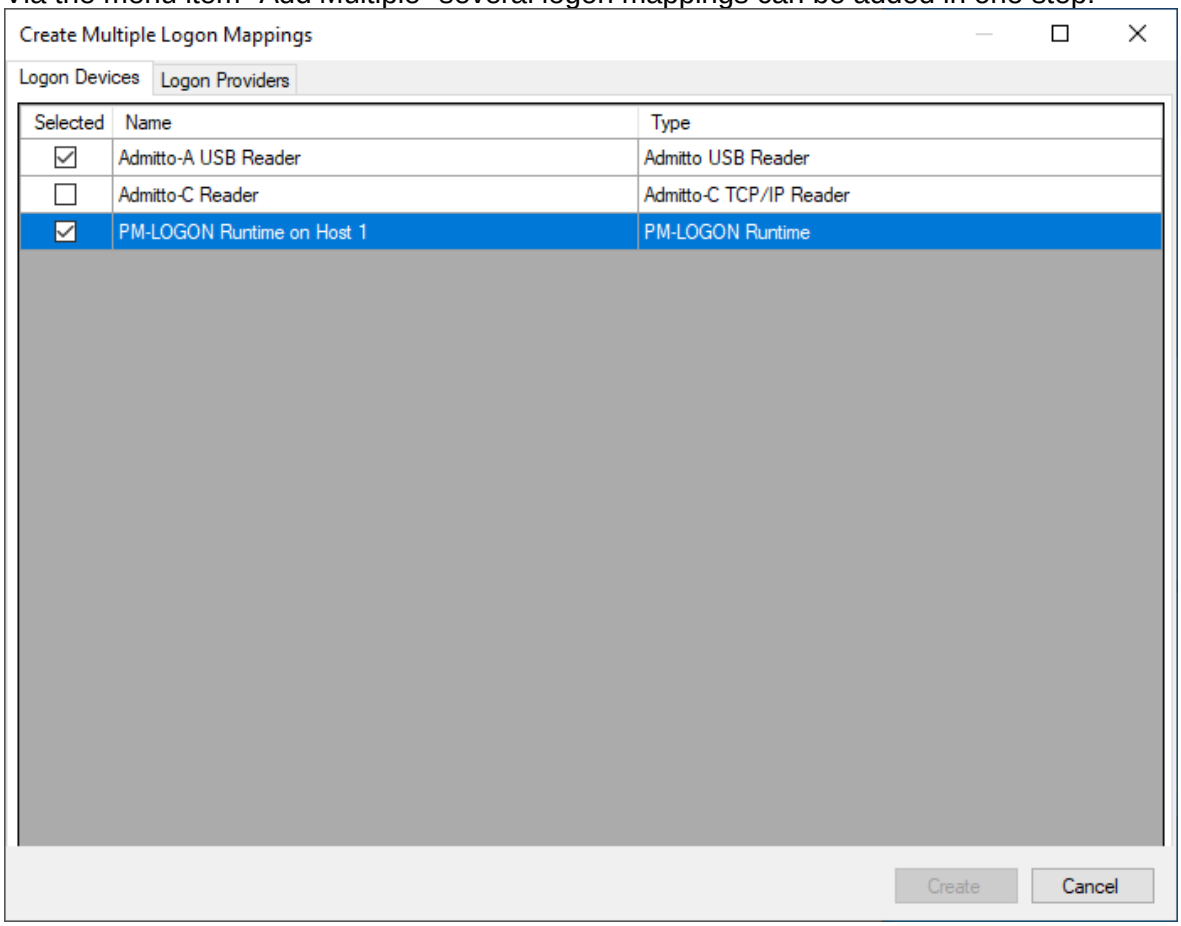
Using the buttons above the list of logon mappings you can add new logon mappings or delete existing logon mappings.

Adding a Logon Mapping:



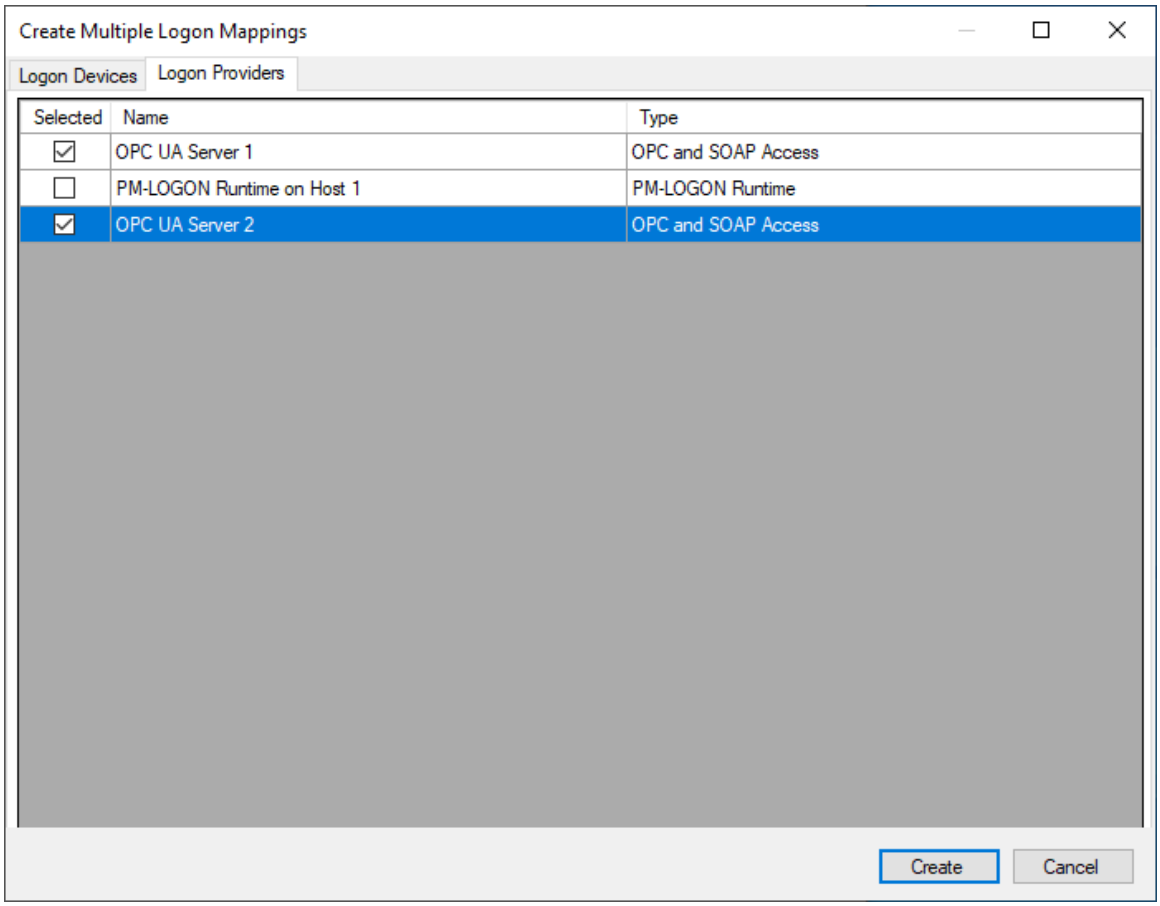
You can add a single logon mapping via the "Add" menu item. A new line is added to the list of logon mappings for the logon mapping.
The logon mapping determines which logon device is connected to which logon provider.
Via the selection lists in the column "Logon Device Name" and "Logon Provider" the corresponding Logon Device or the corresponding Logon Provider can be selected.

Via the menu item "Add Multiple" several logon mappings can be added in one step:

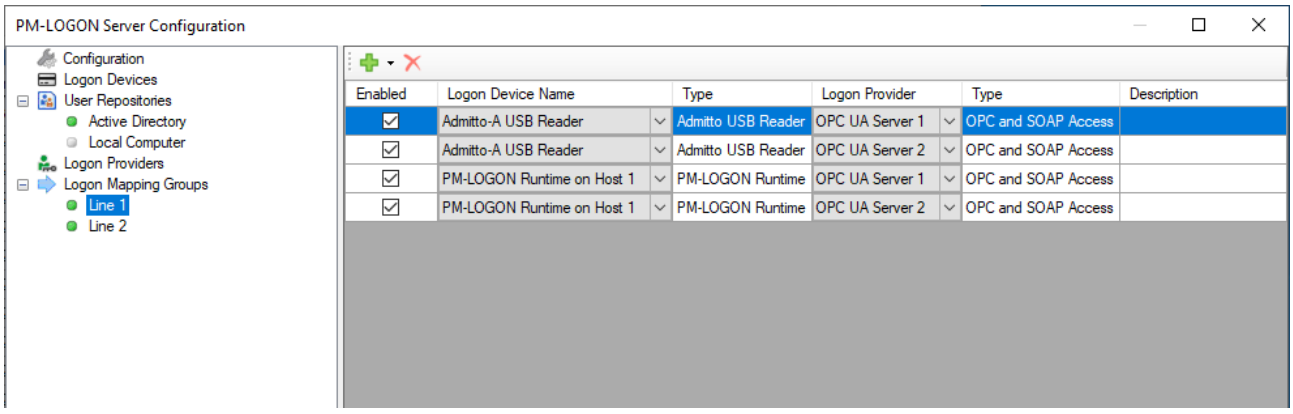


First, on the "Logon Devices" page, in the "Selected" column, select the logon devices that you want to connect to corresponding logon providers.

Then, on the Logon Providers page, select the logon providers to which you want to connect the previously selected logon devices.



When you confirm your selection with "Create", the associated Logon Mappings are created. Each selected logon device will be connected to each selected logon provider.



Individual mappings can be activated or deactivated via the checkboxes in the "Enabled" column.