EVIDEN

Identity and Access Management

DirX Identity

DirX Password Reset Client - User Interface Guide

Version 8.10.12, Edition August 2025

Table of Contents

Copyright ii
Preface 1
DirX Identity Documentation Set 2
Notation Conventions 3
1. DirX Password Reset Client - User Interface 5
2. Password Reset Procedure 7
  2.1. Multiple Options 7
  2.2. Smart Card Option 9
  2.3. Authentication Questions Option 11
  2.4. Mobile OTP Option 14
  2.5. Set New Password Step 17
  2.6. Get Status Step 19
Legal Remarks 23

Preface

This manual provides information about the DirX Password Reset Client User Interface.

DirX Identity Documentation Set

The DirX Identity document set consists of the following manuals:

- *DirX Identity Introduction*. Use this book to obtain a description of DirX Identity architecture and components.
- *DirX Identity Release Notes*. Use this book to understand the features and limitations of the current release. This document is shipped with the DirX Identity installation as the file **release-notes.pdf**.
- *DirX Identity History of Changes*. Use this book to understand the features of previous releases. This document is shipped with the DirX Identity installation as the file **history-of-changes.pdf**.
- *DirX Identity Tutorial*. Use this book to get familiar quickly with your DirX Identity installation.
- *DirX Identity Provisioning Administration Guide*. Use this book to obtain a description of DirX Identity provisioning architecture and components and to understand the basic tasks of DirX Identity provisioning administration using DirX Identity Manager.
- *DirX Identity Connectivity Administration Guide*. Use this book to obtain a description of DirX Identity connectivity architecture and components and to understand the basic tasks of DirX Identity connectivity administration using DirX Identity Manager.
- *DirX Identity User Interfaces Guide*. Use this book to obtain a description of the user interfaces provided with DirX Identity.
- *DirX Identity Application Development Guide*. Use this book to obtain information how to extend DirX Identity and to use the default applications.
- *DirX Identity Customization Guide*. Use this book to customize your DirX Identity environment.
- *DirX Identity Integration Framework*. Use this book to understand the DirX Identity framework and to obtain a description how to extend DirX Identity.
- *DirX Identity Web Center Reference*. Use this book to obtain reference information about the DirX Identity Web Center.
- *DirX Identity Web Center Customization Guide*. Use this book to obtain information how to customize the DirX Identity Web Center.
- *DirX Identity Meta Controller Reference*. Use this book to obtain reference information about the DirX Identity meta controller and its associated command-line programs and files.
- *DirX Identity Connectivity Reference*. Use this book to obtain reference information about the DirX Identity agent programs, scripts, and files.
- *DirX Identity Troubleshooting Guide*. Use this book to track down and solve problems in your DirX Identity installation.
- *DirX Identity Installation Guide*. Use this book to install DirX Identity.
- *DirX Identity Migration Guide*. Use this book to migrate from previous versions.

Notation Conventions

Boldface type
In command syntax, bold words and characters represent commands or keywords that must be entered exactly as shown.

In examples, bold words and characters represent user input.

Italic type
In command syntax, italic words and characters represent placeholders for information that you must supply.

[ ]
In command syntax, square braces enclose optional items.

{ }
In command syntax, braces enclose a list from which you must choose one item.

In Tcl syntax, you must actually type in the braces, which will appear in boldface type.

|
In command syntax, the vertical bar separates items in a list of choices.

...
In command syntax, ellipses indicate that the previous item can be repeated.

userID_home_directory
The exact name of the home directory. The default home directory is the home directory of the specified UNIX user, who is logged in on UNIX systems. In this manual, the home pathname is represented by the notation *userID_home_directory*.

install_path
The exact name of the root of the directory where DirX Identity programs and files are installed. The default installation directory is *userID_home_directory*/**DirX Identity** on UNIX systems and **C:\Program Files\DirX\Identity** on Windows systems. During installation the installation directory can be specified. In this manual, the installation-specific portion of pathnames is represented by the notation *install_path*.

dirx_install_path
The exact name of the root of the directory where DirX programs and files are installed. The default installation directory is *userID_home_directory*/**DirX** on UNIX systems and **C:\Program Files\DirX** on Windows systems. During installation the installation directory can be specified. In this manual, the installation-specific portion of pathname is represented by the notation *dirx_install_path*.

dxi_java_home
The exact name of the root directory of the Java environment for DirX Identity. This location is specified while installing the product. For details see the sections "Installation" and "The Java for DirX Identity".

tmp_path

The exact name of the tmp directory. The default tmp directory is /tmp on UNIX systems. In this manual, the tmp pathname is represented by the notation *tmp_path*.

tomcat_install_path
The exact name of the root of the directory where Apache Tomcat programs and files are installed. This location is defined during product installation.

mount_point
The mount point for DVD device (for example, **/cdrom/cdrom0**).

1. DirX Password Reset Client - User Interface

Used abbreviations in this document:

DPRS: DirX Password Reset Server (backend server connected to the customer Active Directories)

DPRC: DirX Password Reset Client (Windows credential provider on customer client PC)

Supported modes:

DPRC supports two different functional modes:

- Kiosk mode: In this mode the user is logged into a special local account to do the password setting. This mode supports corporate and Internet LAN/WLAN environments (no hotel scenarios).
- Pure credential provider mode: In this mode no local account is used. The difference to the kiosk mode is that special VPN requirements must be met. This mode also supports corporate and Internet LAN/WLAN environments (no hotel scenarios). This mode can also be configured that it works in corporate networks only.

These functional modes are set by installation and cannot be changed.

The DPRC offers three operational modes that can be combined:

- Smart card option (in corporate networks only)
- Authentication questions option
- Mobile OTP (one-time password) option
- A combination of these 3 options

Which option is used is defined by installation.

The dialog language is according to the Windows 10 system language setting. If password reset client the current Windows 10 language is not supported by the password reset client, then the dialogs are displayed in English.

Preconditions:

- The user has a valid AD account
- The PC is a Windows 10 or Windows 11 system.
- The user’s PC is connected to the LAN (corporate/Internet) or to a pre-configured WLAN (corporate/Internet)
- The user is not logged in with his account
- In case smart card option is used:
    - A smart card reader is available, and the required smart card software is installed.

    - The user has a valid smart card
- In case Internet option is activated:
    - The required VPN software is installed.

2. Password Reset Procedure

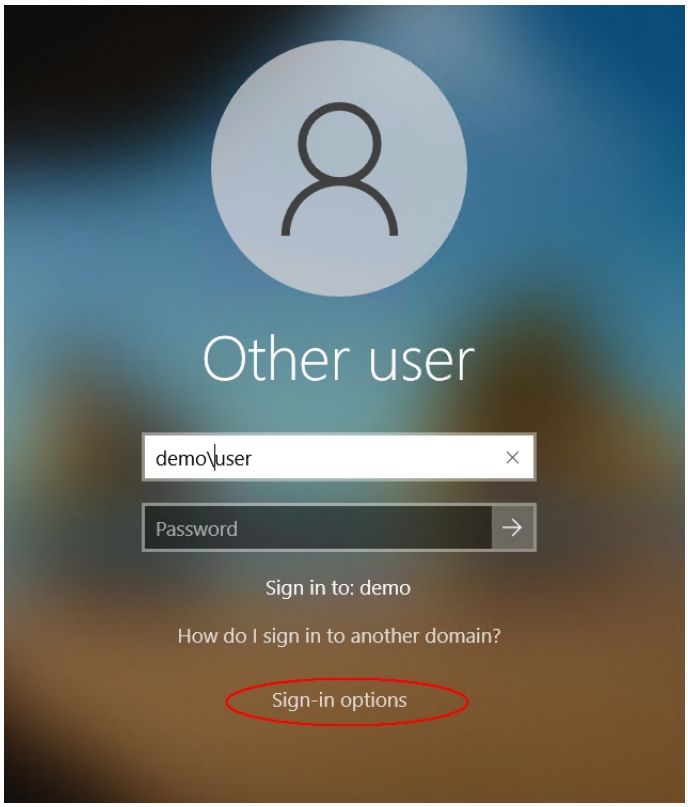
The reset procedure depends on the set option mode of the DPRC.

2.1. Multiple Options

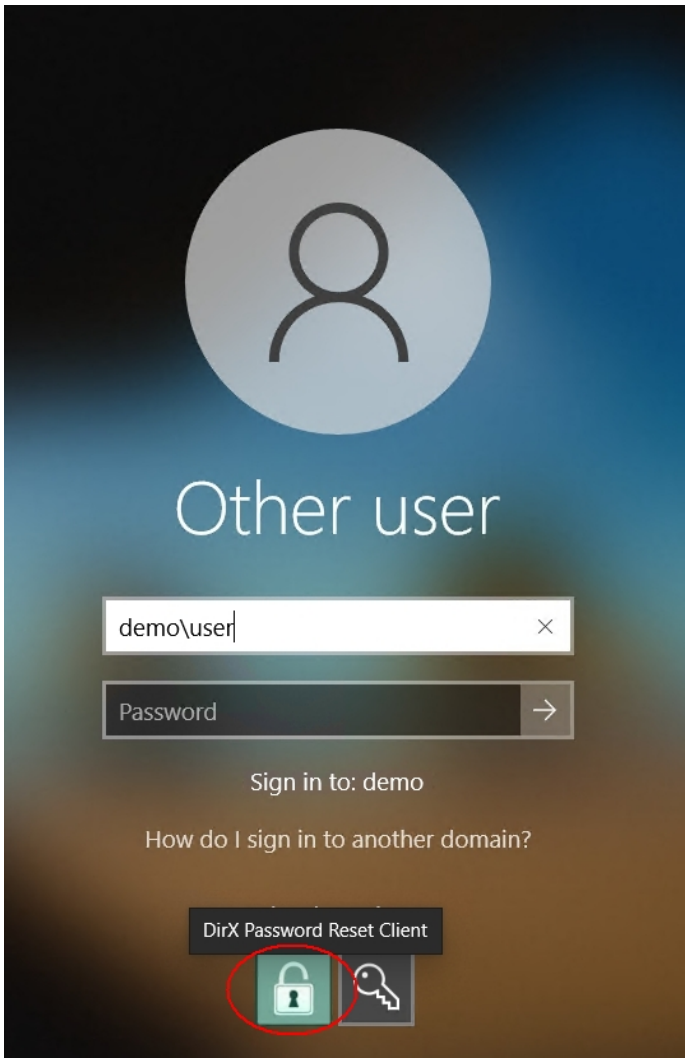
If multiple options are configured the user has to choose which option he will use to reset her or his password.

Windows login screen

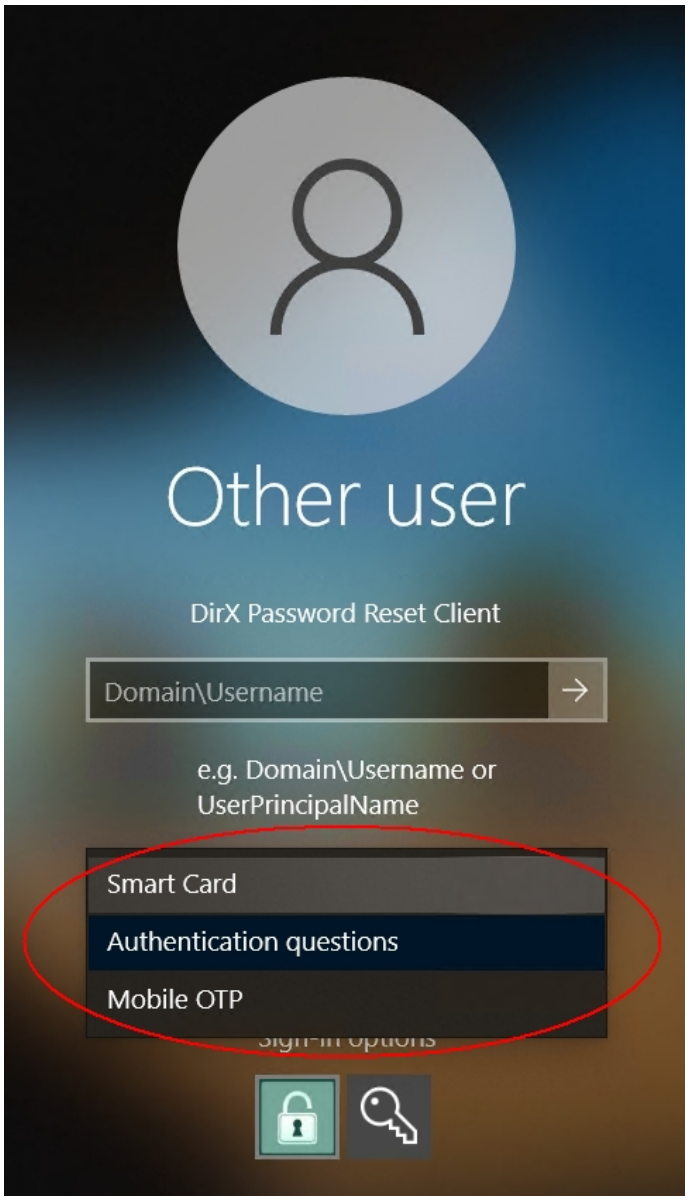
1. The user starts the PC and gets the Windows login screen.Here the user has first to switch to “Sign-in options":



2. Now the user will see the “DirX Password Reset Client” tile.



3. If the user clicks on the tile “DirX Password Reset Client” he gets the following tile with an input field which must be filled with the correct domain and account name and a drop-down list to choose the authentication mode.
   The drop-down list contains the configured options (in the picture three options):



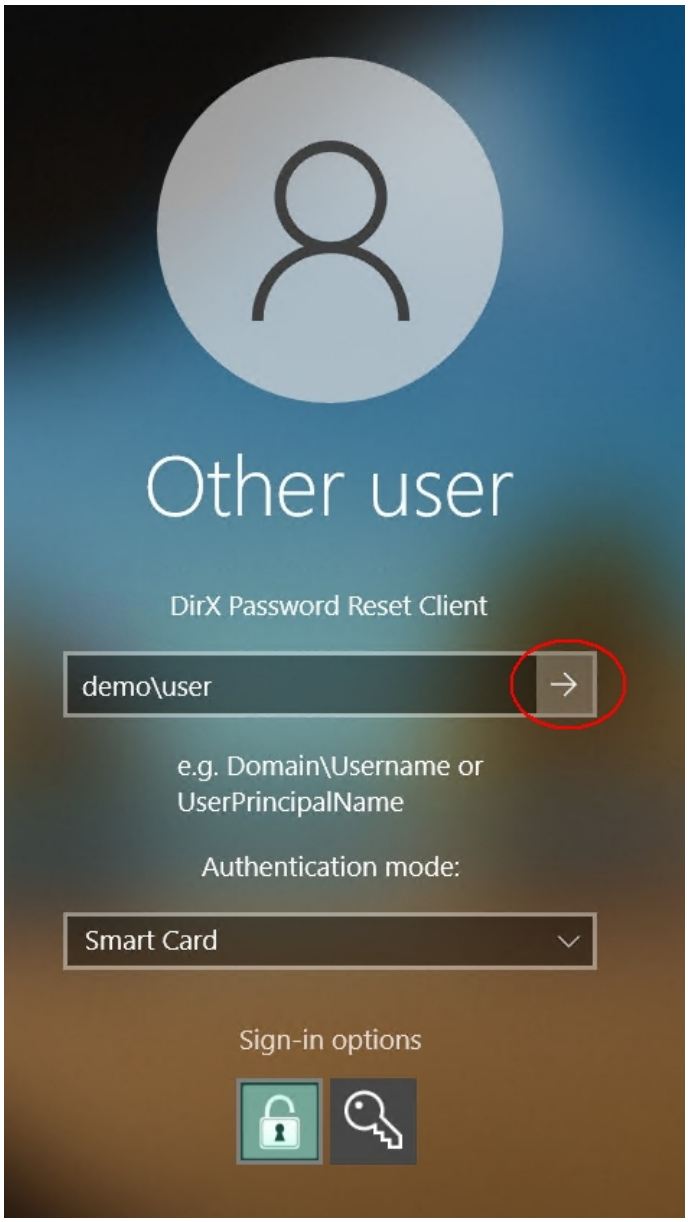
4. The user chooses his/her mode to reset and clicks on the submit button (the arrow right to Domain/Username)

The subsequent procedure is described in the chapter for smart card option, in the chapter for authentication questions option or the chapter for mobile OTP option.

2.2. Smart Card Option

Domain and account name

1. The user is asked to enter the account name and domain name for the password reset



2. The user must press the “right arrow” (submit) button to finish the domain\account input

Smart Card validation

3. The password reset client now looks up the smart card for suitable certificates.(An animation is shown as the access can take a while)

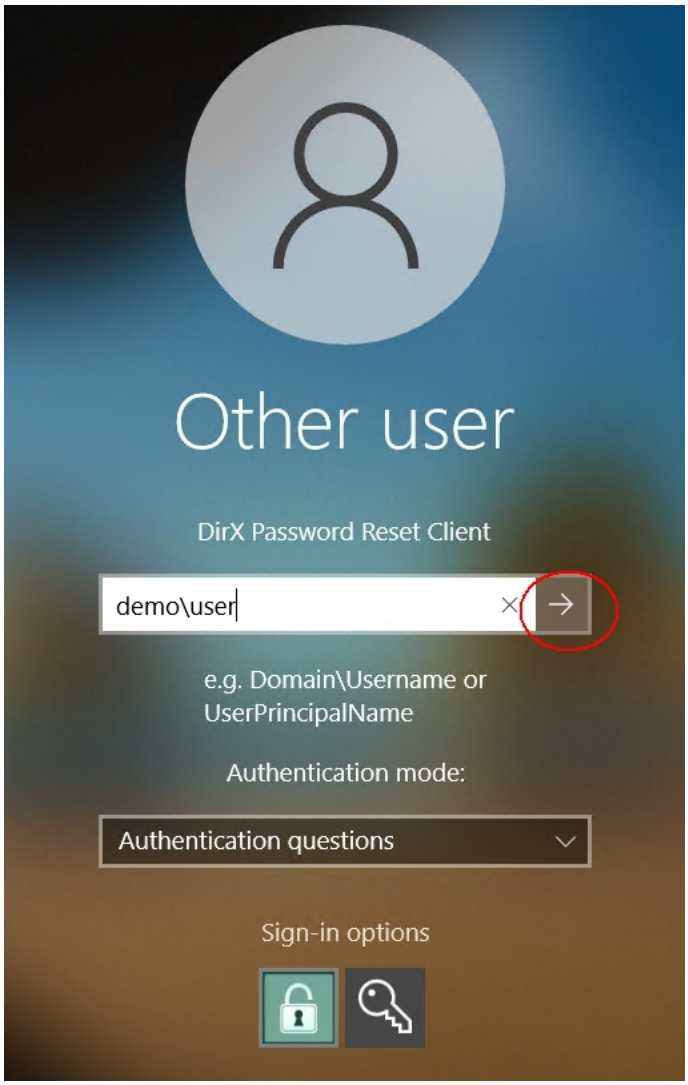
4. In general, the client will show a list of suitable certificates (also from multiple smart cards)
5. When the certificate is selected the user is asked to enter the smart card PIN
6. If the user clicks on the more information link an additional dialog box is presented:
7. The password reset client validates the smart card PIN.In case of an invalid PIN the user is asked to try again from step 3 after clicking ok

The subsequent procedure is described in the chapter Set New Password Step.

2.3. Authentication Questions Option

Domain and account name

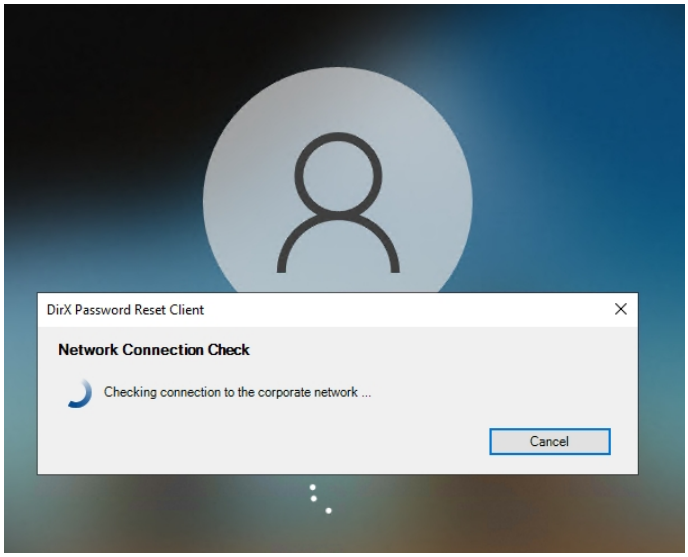
1. The user is asked to enter the account name and domain name for the password reset:



The user has to click the “right arrow” **Submit** button to finish the domain\account input

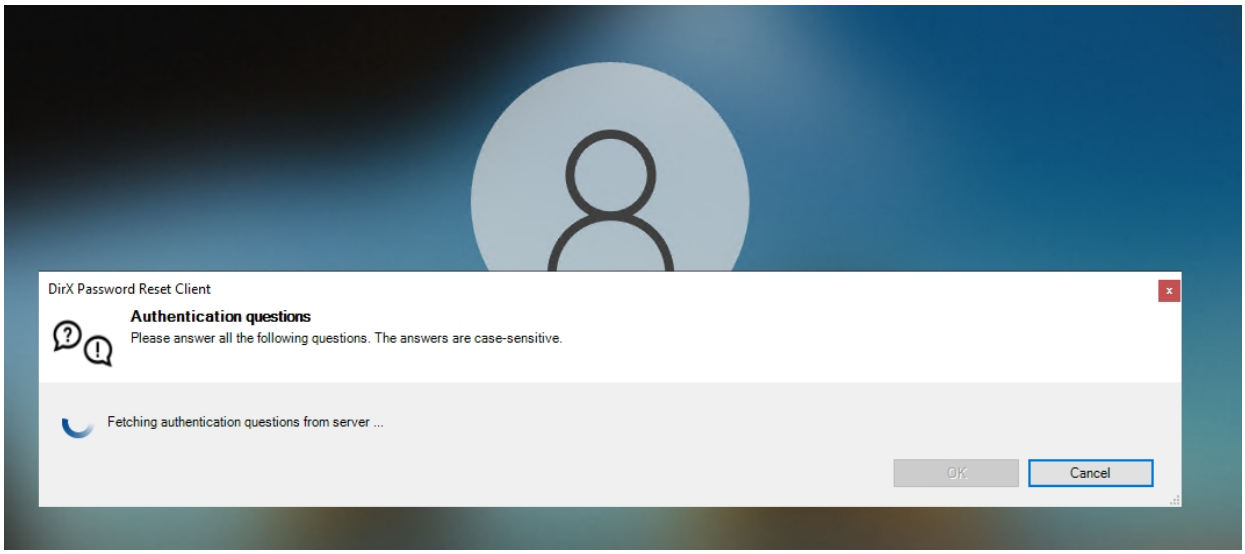
Network Connection Check

2. The password reset client now checks the network connection of the PC to check if in corporate or Internet environment.

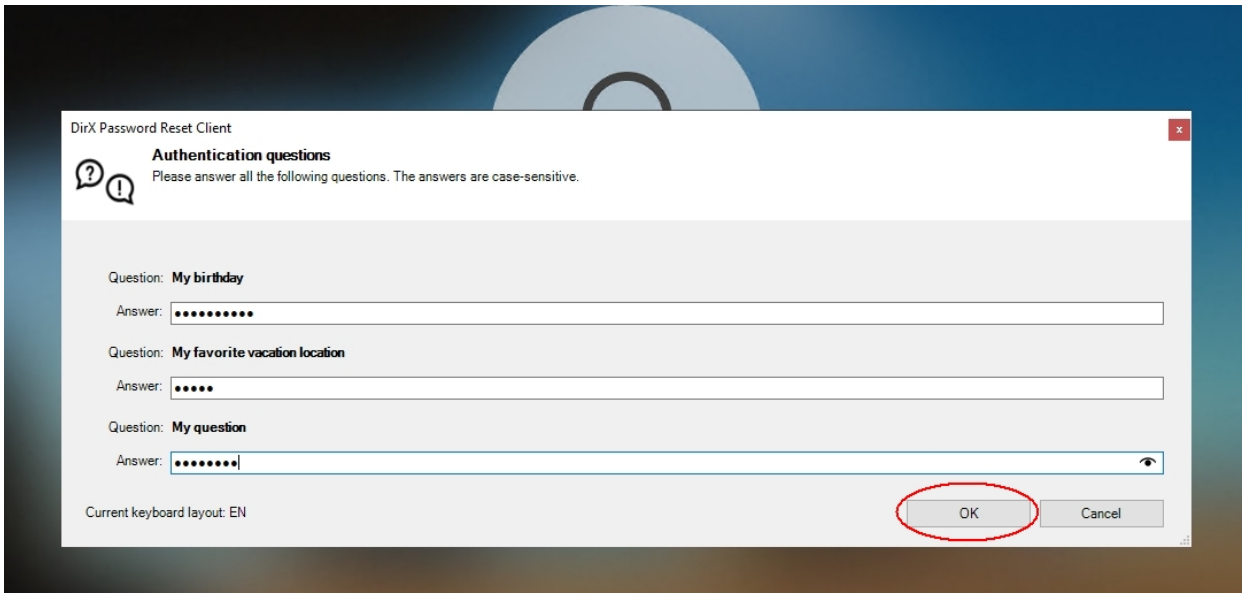


Fetching authentication questions

3. It then looks up the authentication questions for the given account. (An animation with different messages is shown as the network check and access can take a while)



4. The password reset client then shows a randomized set of the authentication questions for the given account

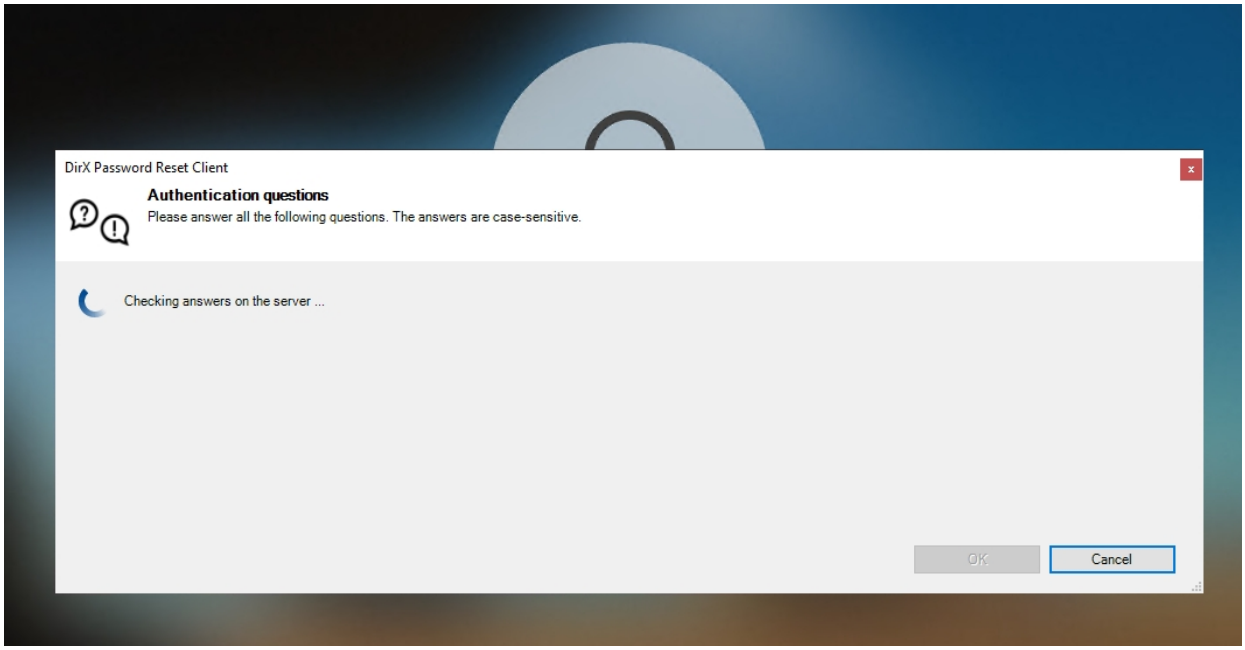


As long as an input box has the focus a so-called Password Reveal "Eye" button is visible in the right corner of the input box.This eye allows the user to see the password characters as he or she types them in.If the user moves the mouse pointer over the Password Reveal button then presses **and holds down** the left button of his mouse, the password (or anything that has typed in so far in the box) will be displayed.As soon as the user releases the mouse button, the password characters will go back to being “blobbed out” with asterisks again.
Note that the questions are displayed as defined in the Web Center (that is in the same language and in the same spelling as defined).

The user can now put his answers to the questions in:

The **OK** button will be enabled if all answers are typed in.

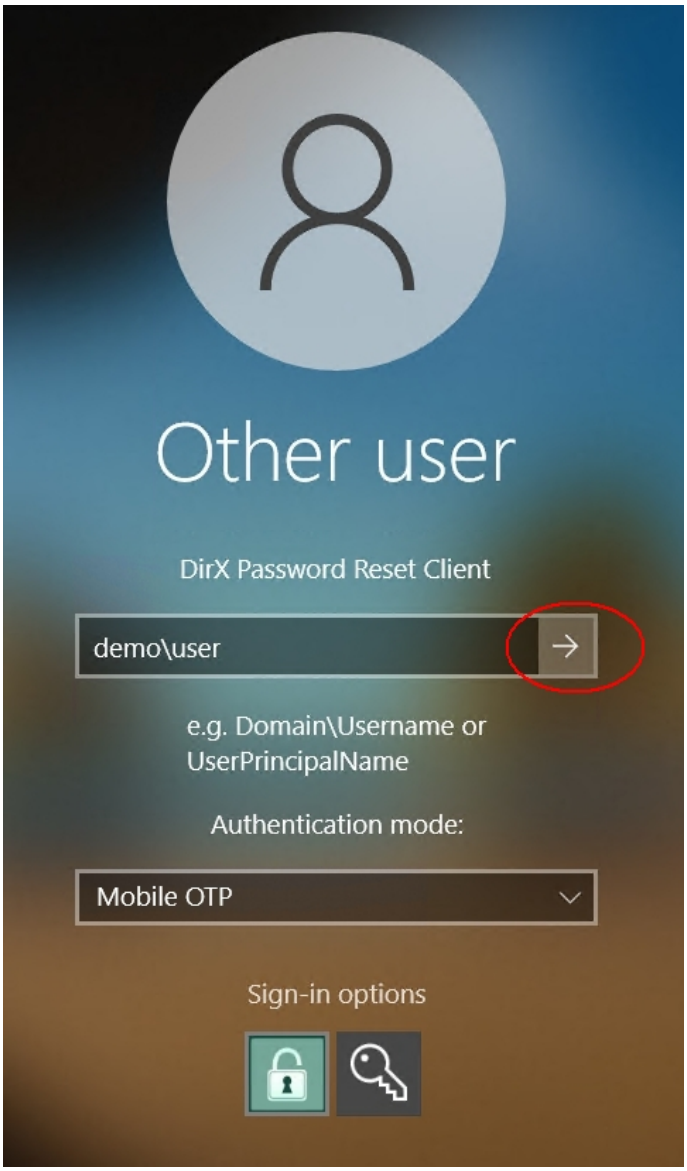
5. The answers are then checked on the server.If the answers are correct, then the subsequent procedure is described in the chapter Set New Password Step.If at least one of the answers is incorrect then the following dialog is shown:



The user can click on the **Try again** button to get a new randomized set of his authentication questions.To cancel the whole reset procedure the user can click on the **Cancel** button.

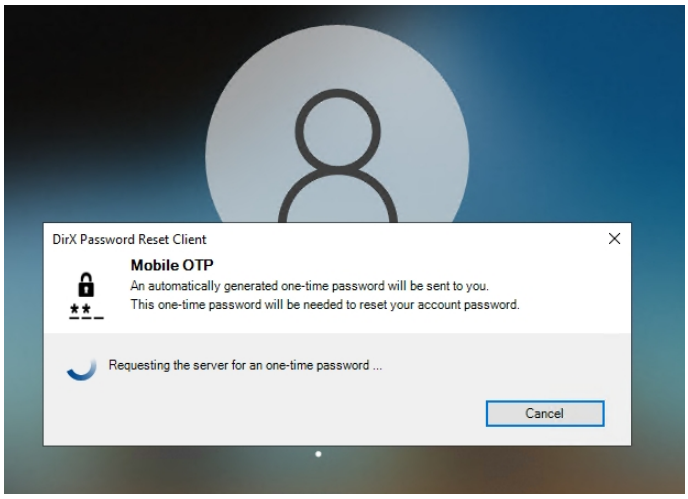
2.4. Mobile OTP Option

The login screen is the same as for Authentication Questions Option.The user has to give his domain and account name (steps 1. and 2.).

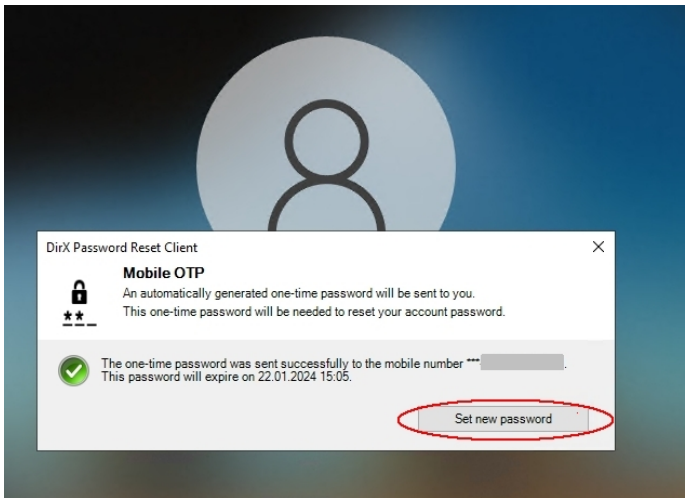
+ 

Sending text message

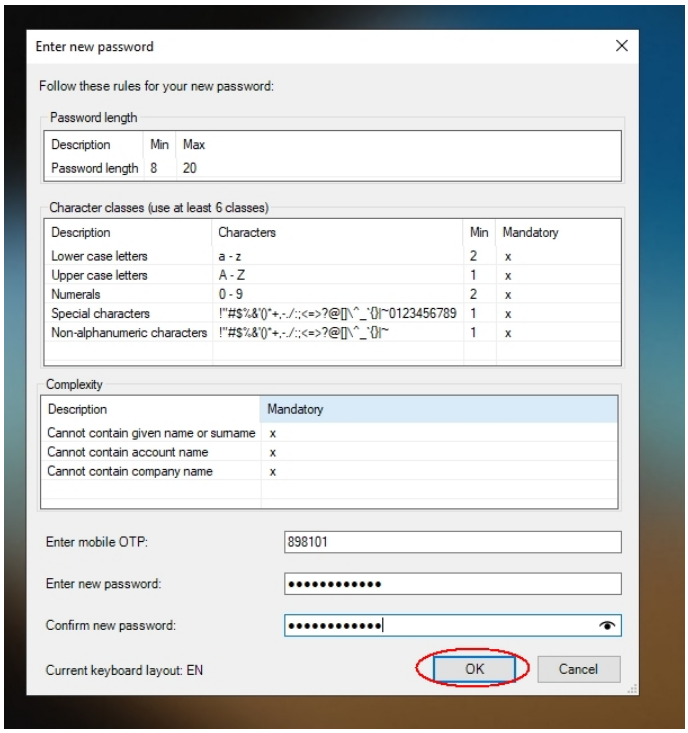
1. The password reset client now checks the network connection of the PC to check if in corporate or Internet environment.It then sends a request to the reset service to send a text message to the configured mobile phone number of the user.(An animation with different messages is shown as the network check and access can take a while)



2. The response (in an okay case) will give a hint to which number the message was sent (last 4 digits are given) and how long the generated one-time password is valid. If the user receives the one-time password on his or her phone, he can click **Set new password** button to continue.



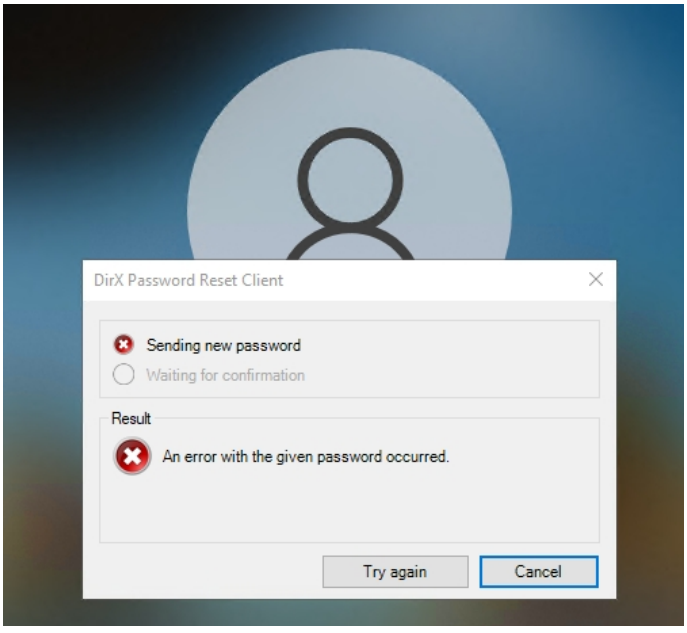
3. In the following Set New Password step the dialog box is slightly different.A further input field labeled "Enter mobile OTP" for the one-time password is shown:



Otherwise, the behavior is identical to chapter "Set New Password Step".

Note: The one-time password is valid only for one time.So if the new password is not compliant with the password history the user has to start over again so that he gets another one-time password.

In case of a wrong OTP, the user will see a failure:

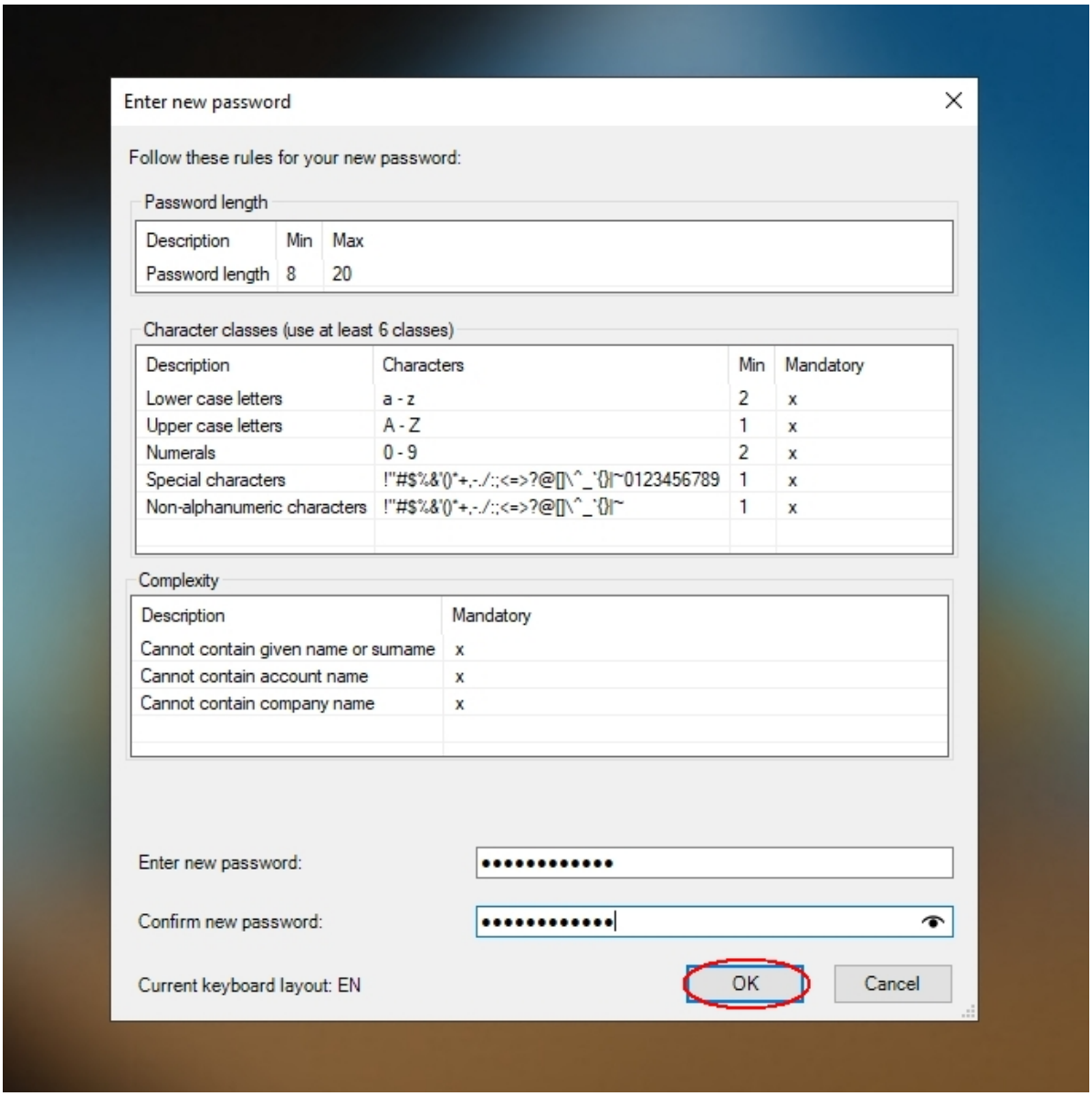
+ 

2.5. Set New Password Step

1. The password reset dialog is opened

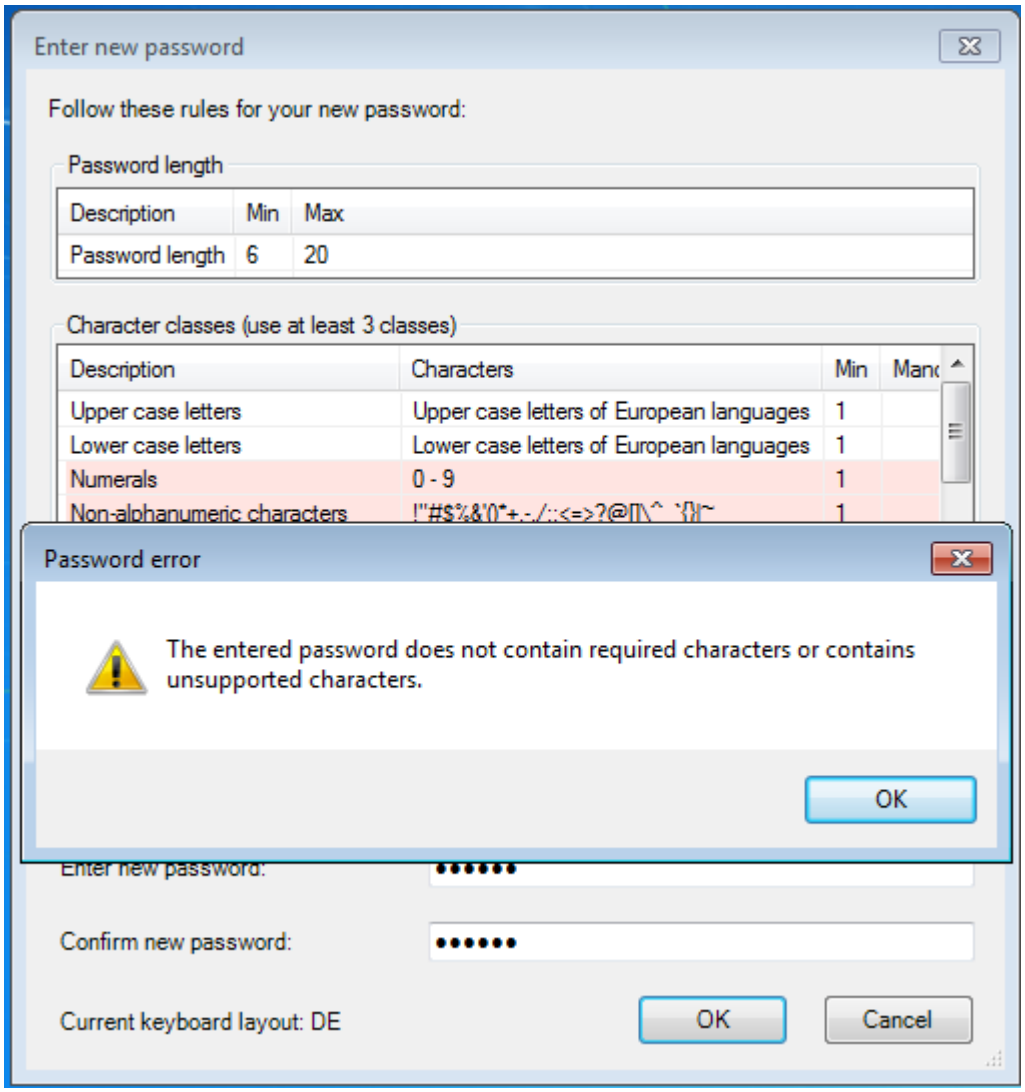
   The password policy is displayed and

- Two input boxes are given to enter the password two times



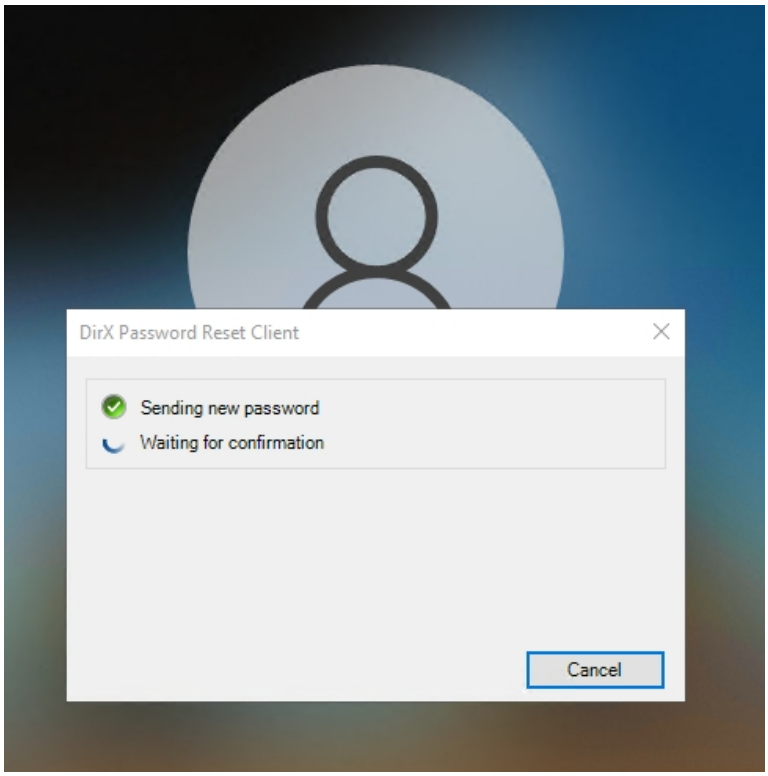
Note that these boxes also have a password reveal eye button.Additionally, the current keyboard layout is shown (current abbreviation of the user's/system's language setting).

2. The user's password input is validated based on the password policy.If the password policy criteria are not met (shown with red background), an error message is shown and the user is asked to try again from step 1



2.6. Get Status Step

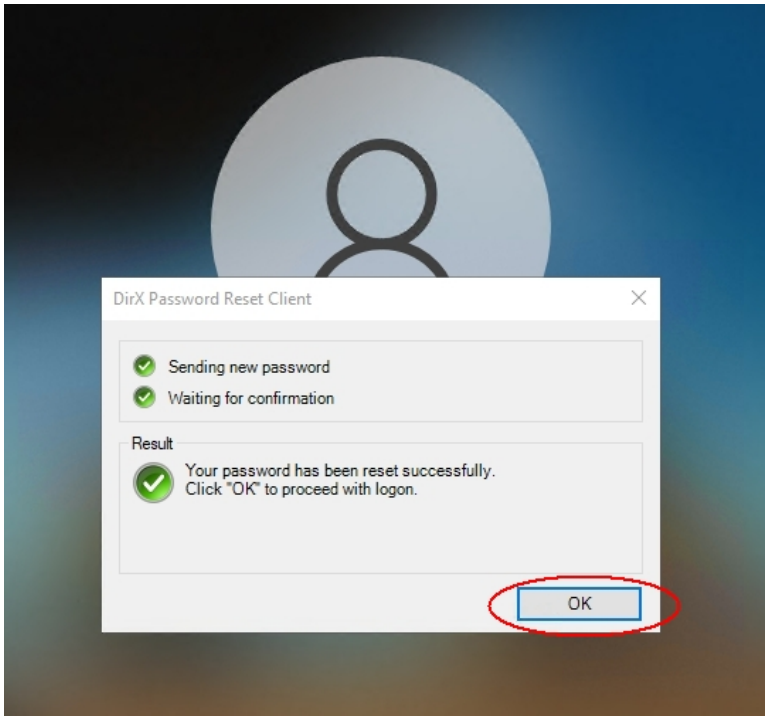
On successful validation of the password, the request is sent to the DPRS.



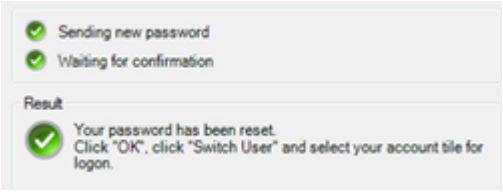
Status feedback

The server sends back the status on the password change request.

Success

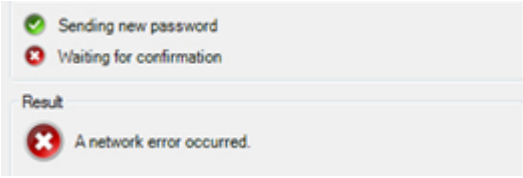


in corporate network or



in Internet network

or failure:



If the new password is not in accordance with the password policy of the Active Directory then a corresponding error message is shown. In both cases, with a click on the **Try again** button the user can repeat to enter a new password and to try over again.

Success means that the password has been set successfully in the connected Active Directory.
Corporate network: The user is directly logged in by clicking **OK** on the status box.
Internet network: The user is then directed back to the Windows 10 login screen by clicking **OK** on the status box. In the okay case the user must click “Switch User” to select the (domain account) password credential provider tile.

DirX Product Suite

The DirX product suite provides the basis for fully integrated identity and access management; it includes the following products, which can be ordered separately.

DirX Identity

DirX Identity provides a comprehensive, process-driven, customizable, cloud-enabled, scalable, and highly available identity management solution for businesses and organizations. It provides overarching, risk-based identity and access governance functionality seamlessly integrated with automated provisioning. Functionality includes lifecycle management for users and roles, cross-platform and rule-based real-time provisioning, web-based self-service functions for users, delegated administration, request workflows, access certification, password management, metadirectory as well as auditing and reporting functionality.

DirX Directory

DirX Directory provides a standards-compliant, high-performance, highly available, highly reliable, highly scalable, and secure LDAP and X.500 Directory Server and LDAP Proxy with very high linear scalability. DirX Directory can serve as an identity store for employees, customers, partners, subscribers, and other IoT entities. It can also serve as a provisioning, access management and metadirectory repository, to provide a single point of access to the information within disparate and heterogeneous directories available in an enterprise network or cloud environment for user management and provisioning.

DirX Access

DirX Access is a comprehensive, cloud-ready, scalable, and highly available access management solution providing policy- and risk-based authentication, authorization based on XACML and federation for Web applications and services. DirX Access delivers single sign-on, versatile authentication including FIDO, identity federation based on SAML, OAuth and OpenID Connect, just-in-time provisioning, entitlement management and policy enforcement for applications and services in the cloud or on-premises.

DirX Audit

DirX Audit provides auditors, security compliance officers and audit administrators with analytical insight and transparency for identity and access. Based on historical identity data and recorded events from the identity and access management processes, DirX Audit allows answering the “what, when, where, who and why” questions of user access and entitlements. DirX Audit features historical views and reports on identity data, a graphical dashboard with drill-down into individual events, an analysis view for filtering, evaluating, correlating, and reviewing of identity-related events and job management for report generation.

For more information: support.dirx.solutions/about

Legal remarks

On the account of certain regional limitations of sales rights and service availability, we cannot guarantee that all products included in this document are available through the Eviden sales organization worldwide. Availability and packaging may vary by country and is subject to change without prior notice. Some/All of the features and products described herein may not be available locally. The information in this document contains general technical descriptions of specifications and options as well as standard and optional features which do not always have to be present in individual cases. Eviden reserves the right to modify the design, packaging, specifications and options described herein without prior notice. Please contact your local Eviden sales representative for the most current information. Note: Any technical data contained in this document may vary within defined tolerances. Original images always lose a certain amount of detail when reproduced.