Multi factor authentication

Introduction

TDS platform is utilizing SSO solution based on Keycloak. That is usually standalone and users can use basic authentication procedure using username and password or multi factor authentication (MFA) with time based OTP token.

Enabling MFA

For specific user

MFA can be enabled by user via user profile on portal or via OTP token reset from TDS SSO login page.

- Go to User profile
- Enable *Enable Multi-factor Authentication (MFA)* feature

For area/project

Following steps will enable Multi Factor authentication on area/project level. Members of area/project will be required to set up TDS OTP tokens during next sign-in using TDS password or AzureAD/ADFS integration unless they already use MFA in TDS. TDS OTP token is then required every time when signing in using TDS password.

- Go to Area/Project configuration
- Enable *Enforce MFA for all area/project members* feature

Customers using AzureAD/ADFS integration only configure OTP token if they do not have it. They are not required to use TDS OTP token for sign in as they already utilize MFA capable SSO integration.

OTP token reset/enable

- Go to TDS Portal login screen
- Click on *Reset or enable OTP token for TDS Multi Factor Authentication (MFA)*

OTP token configuration

Following steps need to be executed during the first login with MFA enabled or after resetting your OTP token.

1. Install time based OTP tokens capable application. One of the following applications is recommended:
    - Browser extensions
        - Chrome
            - Authenticator by authenticator.cc
        - Edge
            - Authenticator: 2FA Client by mymindstorm
        - Firefox
            - Authenticator by mymindstorm
    - Android
        - Microsoft Authenticator blocked URLRecommended for Tietoevry users
        - Google Authenticator
        - Twilio Authy 2-Factor Authentication
        - FreeOTP Authenticator
    - iOS
        - Microsoft Authenticator blocked URLRecommended for Tietoevry users
        - Google Authenticator
        - Twilio Authy by Authy Inc.
        - Authenticator by Matt Rubin
    - Windows
        - WinAuth
    - Password Managers

    - Bitwarden
    - 1Password
2. Open the application and scan the QR code displayed
    a. Key code may be used in case of inability to scan the QR code. Click on *Unable to scan?* to get the key.
3. Enter the one-time code provided by the application and click submit to finish the setup.
4. Optionally you can enter device name if asked, for example "My Windows work laptop".
5. Click Submit.

OTP token is always provided only once. It is either QR code or code visible under *Unable to scan?* button. In case of the OTP token loss, use TDS OTP token reset functionality available on TDS SSO login page - see *OTP token reset/enable* section

Troubleshooting

One time code is not accepted

Possible reasons and solutions:

- in case of device change or application/plugin change for OTP tokens
    - Solution - go back to log in screen and reset OTP token from there - see *OTP token reset/enable* section
- date/time could be out of sync on the device generating one time codes
    - Solution - make sure device or application/plugin has time in sync
        - Google Authenticator - tap on hamburger menu () in the top right corner > Settings > Time correction for codes > Sync now.
- if OTP does not work after time sync
    - Solution - go back to log in screen and reset OTP token from there - see *OTP token reset/enable* section