Logo ID Presentation Document

You may need to use multiple Logo applications simultaneously throughout the day. Creating and storing separate usernames and passwords for each application takes your time and makes your tasks more difficult. Instead of searching for the application - username and password matching to enter the application you need, you can now carry out your tasks much faster and easier by using Logo ID.

What is Logo ID?

Logo ID; is a unique username and password created individually by users and provides common access to all Logo Solutions*.

- **Single, common username and password for all products**
  - With Logo ID, you no longer need to create and store different passwords when logging into different applications. With the creation of a central username and password, you will have a single username and password that integrates systems at entry to all Logo Solutions*. Logo ID, which allows you to be simultaneously connected to numerous Logo Solutions with your common username and password, is a practical feature that offers ease of use.
- **Simplified integrated user experience**
  - With Logo ID, you can connect between multiple applications. With the Logo ID you create, your username and password becomes unique, and access and synchronization between applications become possible. It allows you to holistically manage all the solutions and platforms you use within the wide Logo solution family; from corporate business software to Logo Portal, with the same username and password, and you can perform your support requests and ticket follow-ups without re-entering password and username while using your Logo solution. In this way, business processes gain speed and efficiency.
- **Increased security**
  - Logo ID enables you to minimize potential security risks and strengthen the security of your business with the need for strong password use and the end-to-end multi-factor authentication (MFA) structure. With the uniqueness and password management, your systems work securely while your business processes gain efficiency.
- **Central user management**
  - With Logo ID, which allows central management of the users in your business, it becomes easier to manage user changes. In addition, users can manage their user information that is common in all solutions for themselves from a single place.

"Create your user information with simple steps with Logo ID, simplify all your accesses by unifying the username and password of your software, and make your user management more secure."

*İşbaşı application is excluded.

What are the Logo ID password rules?

IDM password rules have been created in accordance with the password policy created by Logo Software.

Rules

- If the user makes 10 incorrect login attempts, the user's account is locked for 30 minutes.
- Passwords for user accounts should be changed at least every three (3) months.

Password Selection Obligations

- Must be at least 8 digits.
- It must include at least 3 criteria from capital letters, lowercase letters, numbers, and special characters.
- Cannot include username and surname.
- The new given password cannot be the same as the last 3 used passwords.
- 4 numbers cannot be consecutive in year format (like 1984, 2021)

Password Selection Recommendations:

- Not using Turkish characters (ç, ğ, İ, ı, ö, ş, ü)
- Not containing words that express meaning to the user (relative/friend's name, car model, year/date of birth)

What is multi-factor authentication (MFA)? How does Logo ID's multi-factor authentication support work?

Multi-factor authentication (MFA) is a method that allows the user to confirm his identity with other information in addition to the password during the login process to the product and protects his account even if his password is compromised.

Logo ID offers the multi-factor authentication option optionally to its users. Users who wish can log into the Logo ID management screen, complete the installation process of the multi-factor authentication options they find suitable, and put them into use, or they can remove them from use via the same screen. Two-factor authentication can be activated with Google Authenticator or Duo Mobile applications to be installed on mobile devices supported by Logo ID.