Passkeys for Enterprises

Last updated: March 2023

Deploy passwordless authentication to protect your organization's data.

Security is a major concern for organizations alike and passwords are the primary means of protecting sensitive information, but it does not means they are secure enough. This lack of security can be solved through passkeys.

Using enterprises' passkeys, organizations are able to not only facilitate the authentication journey for employees, but also manage users and access, enhancing the security and protecting sensitive internal data.

Benefits

- Increased security,
- Simplified password management,
- Improved user experience,
- Reduced risk of human error,
- Increased control.

Management and Protection

The major benefit of using passkeys for enterprises is the possibility of control over passkeys, including management of users, devices, and permissions.

Another advantage of passkeys for enterprises is the access policy creation, which allows admins to set security key policies according to the organization's needs.
Passkeys can be used in a variety of scenarios, including web applications, mobile applications, and IoT devices.

They can also be used for single sign-on (SSO) to simplify access to multiple applications and services.

All of these solutions can be quickly deployed and easily managed through IDmelon Passwordless Orchestration Platform, which offers an easy-to-use admin dashboard with a variety of allowances and tools to help enterprises to manage all of their users and access.

Benefits of Passkeys

Increased Security

Passwords can be hacked or stolen, but managed passkeys use advanced encryption techniques to protect sensitive data. The cryptographic keys used in managed passkeys are much harder to crack than traditional passwords, making them a more secure option.

Simplified Password Management

Users can use a single managed passkey to access multiple applications and services. This eliminates the need to remember multiple passwords, which can be a time-consuming and frustrating task.

Improved User Experience

Managed passkeys can provide a more seamless user experience than traditional passwords. Users can log in quickly and easily without having to remember complicated passwords or go through the hassle of resetting forgotten passwords.

Increased Control

Managed passkeys allow administrators to control access to sensitive information. They can revoke or modify passkeys if necessary, which gives them more control over who has access to sensitive data.

Reduced Risk of Human Error

Human error is a common cause of security breaches. Passkeys can reduce the risk of human error by eliminating the need for users to create and remember passwords. This also reduces the risk of users writing down passwords or storing them in insecure locations.

Phising-resistant
Passwordless Authentication.
Superior security for workforce authentication with existing devices as FIDO security keys.