



## 2023 The IDmelon FIDO2 Passwordless Orchestration Platform

The IDmelon Passwordless Technologies: can be Deployed Overnight, have Lifecycle Credential Management, and allow BYOD (Smartphones, Security Keys, and/or Physical Access Cards). IDmelon also provides an additional option called "Simple Sign On for Single Sign On (SSO for SSO)" which provides your organization's Users with Passwordless for your Single Sign-On.

Companies can activate their Users for the IDmelon Passwordless with the IDmelon Account Setup Link, [panel.idmelon.com](https://docs.idmelon.com/docs/administration/introduction/) , and the Account Set Up Document at: <https://docs.idmelon.com/docs/administration/introduction/>

### Introduction

The IDmelon FIDO2 Orchestration Platform helps organizations simply and quickly deploy secure Passwordless Authentication for their users. Features like Security Key as a Service, FIDO2 managed security keys, and fully automated FIDO2 lifecycle are patented and unique approaches that help organizations enhance their workforce authentication security overnight. No more dealing with purchase and distribution of hardware FIDO security keys as organizations can use whatever device their users have as a FIDO2 security key. It can be an Access Card, a Key FOB or a smartphone.

### Setup is completed with these steps below:

1. Create a Workspace
2. Add Users
3. Assign Credential Formfactor
4. Create Credential Security Policies

**Please see the information and URL Links below.**

**\*Have Questions or Need Assistance? Please Contact:  
Sales@IDmelon.com**

#### 1. Create a Workspace

The IDmelon security key as a service solution can be managed from the IDmelon Admin Panel. You can enroll and activate users' security keys, grant, restrict and monitor their access, manage licenses, and more. The Admin Panel is

available Here. If it is your first try, you can create a workspace on behalf of your organization, or you can use your security key to experience a simple Passwordless login.

How to create a workspace: <https://docs.idmelon.com/docs/administration/createworkspace/>

## 2. Add Users

When the workspace has been created, the first step to take is adding users, which can be done in three ways:

- Add a single user
- Import from a CSV file
- Import from Azure AD

How to add users: <https://docs.idmelon.com/docs/administration/enrollment/>

## 3. Assign Credential Formfactor

While adding users, you can also assign security keys, which can be based on one of the three devices below:

A. Smartphone as a Security Key Device Formfactor: for which an email containing an activation link will be sent to the user's email address to let user activate their smartphone as a security key.

- Smartphone as a security key device: <https://docs.idmelon.com/docs/administration/enrollment/>

B. Contactless Card as a Security Key Device Formfactor: This type of device has two options for activation:

> Activate now: activate the card for your user if as an admin you have the card physically near you.

> Activate by user: send activation email to user if the card is not with you (the targeted user will receive registration link in an email).

- How to setup a Contactless card as a security key device:

<https://docs.idmelon.com/docs/administration/enrollment/#contactless-card>

C. Security Key as a Security Key Device Formfactor: This is if you want to use FIDO2 Hardware security keys. A registration link in your email, will let you set your hardware, as a FIDO2 hardware security key. From now on, your security key can be used for Passwordless logins based on FIDO standard wherever it is available.

- How to setup a FIDO2 hardware security key device:

<https://docs.idmelon.com/docs/administration/enrollment/#hardware-security-keys>

## 4. Create Credential Security Policies

> The organization can control access of users by setting authentication policies. An admin can create new authentication policies to apply to users' security keys to limit their access.

> The limitation can be based on multiple conditions such as time period, IP Address, RP (Relying Parties) that users are trying to reach out, and the location they are trying to login from.

- How create a security key policy: <https://docs.idmelon.com/docs/administration/skpolicy/#create-new-policy>

***\*Have Questions or Need Assistance? Please Contact: Sales@IDmelon.com***