MachPanel PasswordLess Authentication

Summary

This article provides you information about MachPanel PasswordLess Authentication and how to configure it in MachPanel.

Applies to

Applies to MachPanel v7.2.11 and above.

Overview

Passwordless authentication is a method of authentication which enables users to authenticate into an application without providing password. Instead users can provide some other type of proof of identity that is linked with their device, such as fingerprint, retina/face scan, device pin code or a USB key.

In current era of IT, it has become very common to perform day-to-day business activities using different online apps where these apps require authentication of users for auditing purposes. Remembering authentication credentials (Username & Password) for different apps is very difficult.

Secondly in simple authentication methods, credentials are stored on servers, transmitted over network for client's validation and hence very vulnerable and attackers can make a guess and steal credentials and may get access to critical and sensitive information. These attacks may include Brute Force attack, Phishing, Network Packet sniffing, Trojan attack and credential stuffing.

Passwordless authentication decreases chances of credential theft and enhances the security by enabling users to use their device built security systems such TPM/TEE to validate user identity. Credentials never leave user's device and are never stored on server.

FIDO alliance has developed a standard for Passwordless authentication and is followed by big Tech Giants like Microsoft, Google and Apple. We have followed the FIDO alliance standard to provide Passwordless authentication for control panel end users.

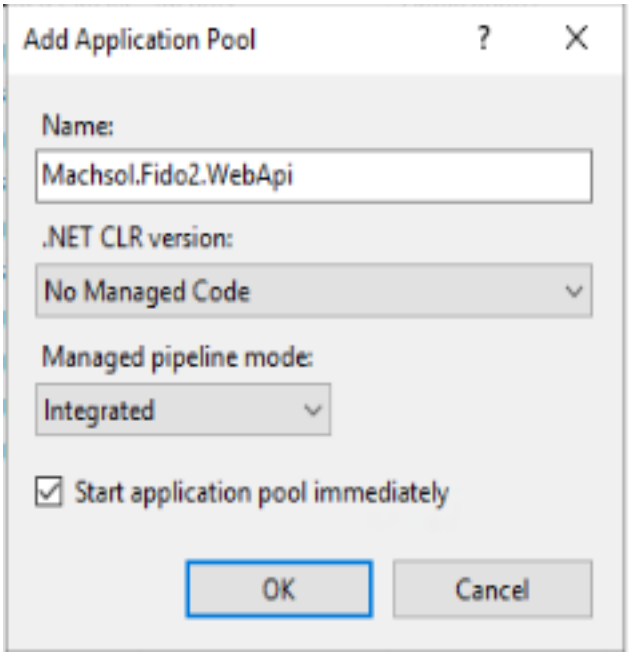
Reference: https://fidoalliance.org/fido2/

To make control panel Passwordless authentication aware, some installations and configurations are required. Below in this document we have described the details of installations and configurations required to enable Passwordless authentication in control panel.

Middleware App Installation and Configuration

To enable Passwordless authentication in control panel, it is required to install and configure a middleware application running on same IIS server as control panel and must be hosted with SSL certificate. It is not necessarily required for this App to be accessible outside the control panel server i.e. over the internet.

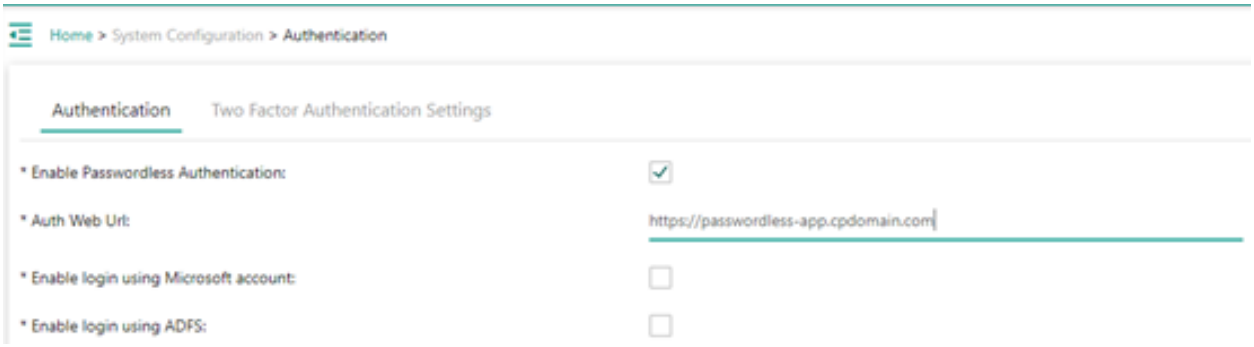
- For new middleware application, it is required to install 'Microsoft's ASP.Net Core 6.0.11 Windows Hosting Bundle' from this location
- Copy the directory 'MachSol.Fido2.WebApi' from 'Apps' directory inside Control Panel Web directory to the desired location for IIS.
- Create new application pool for 'MachSol.Fido2.WebApi' and select 'No Managed Code' in '.Net CLR Version' as depicted below.



- Create a new website in IIS as ‘MachSol.Fido2.WebApi’ pointing to the ‘MachSol.Fido2.WebApi’ directory.
  - Select ‘MachSol.Fido2.WebApi’ in application pool
  - Assign bindings for accessibility and SSL certificate.
- Once application is configured and running try accessing a shake hand Uri to confirm that web API is running by typing in ‘https://passwordless-app.cpdomain.com/handshake. This request will result in a message on browser screen as ‘Handshake was successful, API is running’.

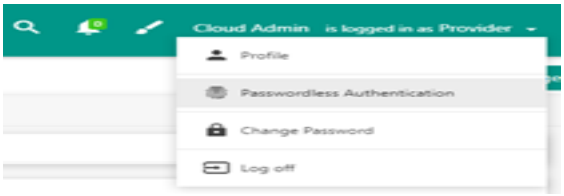
Enable and Configure PasswordLess Authentication in MachPanel

To enable Passwordless authentication in control panel login as ‘Service Provider’ and navigate to ‘System Configuration > Authentication’ and select option ‘Enable Passwordless Authentication’ to enable and provide Url for middleware app in ‘ Auth Web Url’ field as depicted below and press ‘Save’ button.

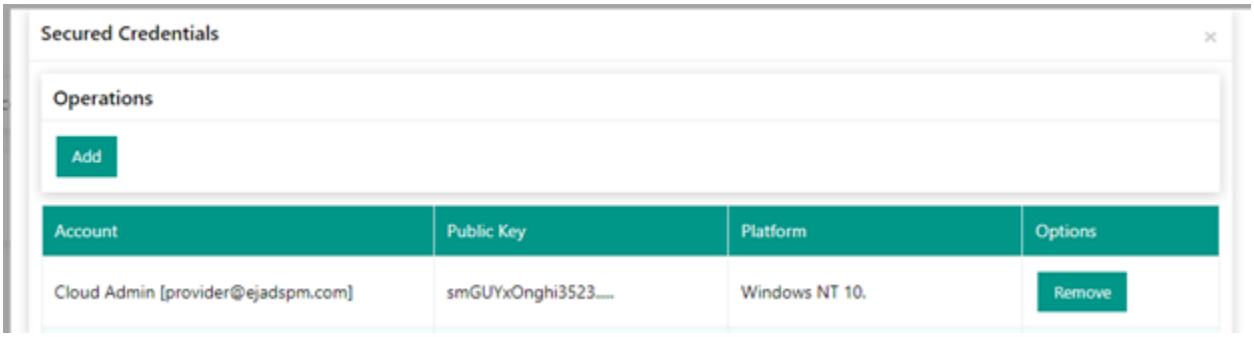


Secured Credentials Registration

When Passwordless authentication is enabled and browser supports device/platform credential authentication, option to configure platform/device authenticator appears on profile menu option for logged in account (staff/customer/contact) as depicted below.



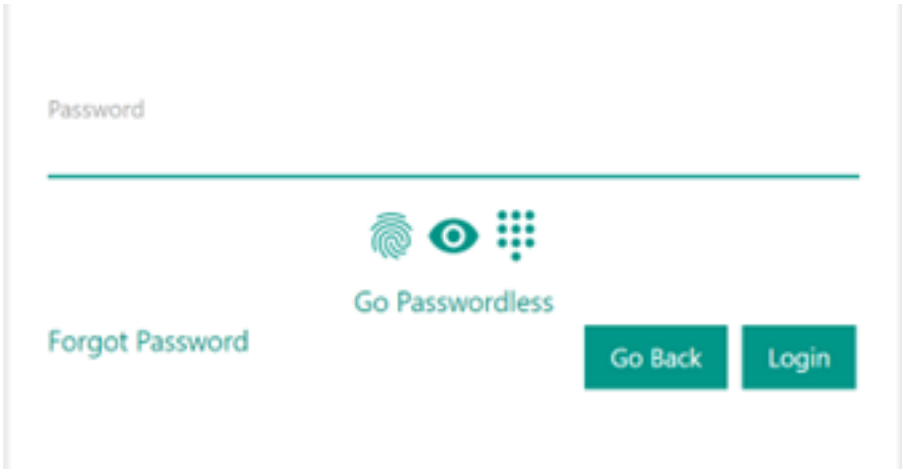
On clicking this option panel will show any existing registered platform credentials for logged in account (staff/customer/contact) and option to add new or remove existing credentials as depicted in below screenshot.



Any account can register one or more secured credentials referring to different authenticators such as from different devices, multiple biometric, or device pin.

Login With Secured Credentials

When an account which has registered secured credentials and Passwordless Authentication is enabled and also browser supports device/platform credential authentication then option to log in to control panel with device/platform credential appears at login password screen as depicted below.



User can login via both control panel password or can go Passwordless with device/platform registered secured credentials by clicking on ‘Go Passwordless’ option.

MachPanel PasswordLess Authentication

MachPanel Knowledgebase
https://kb.machsol.com/Knowledgebase/55733/MachPanel-PasswordLess-Authentic...