

# Two-factor authentication (2FA)

## Summary

This article provides summary on how you can configure Two Factor authentication (2FA) in MachPanel.

## Applies To

This article applies to MachPanel Build v6 and above.

## Two Factor Authentication (2FA):

Two Factor Authentication, also known as 2FA, two step verification or TFA (as an acronym), is an extra layer of security that is known as "multi factor authentication" that requires not only a password and username but also something that only, and only, that user has on them, i.e. a piece of information only they know.

1. To Configure 2FA settings in MachPanel, navigate to the following path: Home » System Configuration » Authentication. Select Two Factor Authentication Settings tab.
2. Check Enabled All sorts of options are possible to entertain different scenarios about enabling/disabling 2FA on different levels (Staff/Resellers/Customers) using the checkboxes highlighted below:
  - a. **Enabled:** Enabled will enable the option globally without affecting any users. It is up to the user to enable/disable the option for himself/herself.
  - b. **Enable by default for new (i) Customers (ii) Resellers (iii) Staff Users:** This means that after saving configuration having this checkbox enabled, the respective new Customer/Reseller/Staff will have the option to use 2FA enabled by default.
  - c. **Update Existing Users:** This option will update existing users based on the previous settings.
    - i. If only "a" is Checked and "b" is Unchecked, the option will be disabled for existing Customers/Resellers/Staff.
    - ii. If "a" and "b" both are Checked, it means that option will be enabled for existing Customers/Resellers/Staff.

The screenshot shows the 'Two Factor Authentication Settings' page in MachPanel. The breadcrumb trail is 'Home > System Configuration > Authentication'. The page has two tabs: '3rd Party Authentication' and 'Two Factor Authentication Settings', with the latter being active. The settings include: a checked 'Enabled' checkbox; three checkboxes for 'Enabled by default for new customers', 'Enabled by default for new resellers', and 'Enabled by default for new staff users', all of which are checked and highlighted with a red box; and a checked 'Update Existing Users' checkbox. Under 'Authenticate Using:', there are four radio button options: 'PIN through Email', 'PIN through SMS', 'Authenticator App' (which is selected), and 'Duo Authentication'. A note at the bottom states: 'Use your mobile authenticator app to generate 2-Step verification code on your phone. Please note that to display QR code images a 3rd party API is used, see details. The API must be accessible.' A 'Save Settings' button is at the bottom left.

## Two-factor authentication (2FA)

For 2FA Settings **Authenticate Using** following:

1. Send PIN through Email
2. Send PIN through SMS
3. Authenticator App

**Send PIN through Email:**

Select PIN expires in Minutes. **Save** Settings

The screenshot shows the 'Two Factor Authentication Settings' page. The breadcrumb trail is 'Home > System Configuration > Authentication'. There are two tabs: '3rd Party Authentication' and 'Two Factor Authentication Settings', with the latter being active. The settings include: 'Enabled' (checked), 'Enabled by default for new customers' (checked), 'Enabled by default for new resellers' (unchecked), 'Enabled by default for new staff users' (unchecked), and 'Update Existing Users' (checked). Under 'Authenticate Using:', 'PIN through Email' is selected with a radio button. Other options are 'PIN through SMS', 'Authenticator App', and 'Duo Authentication'. The 'PIN expires in:' field is set to '10' minutes. A green 'Save Settings' button is at the bottom.

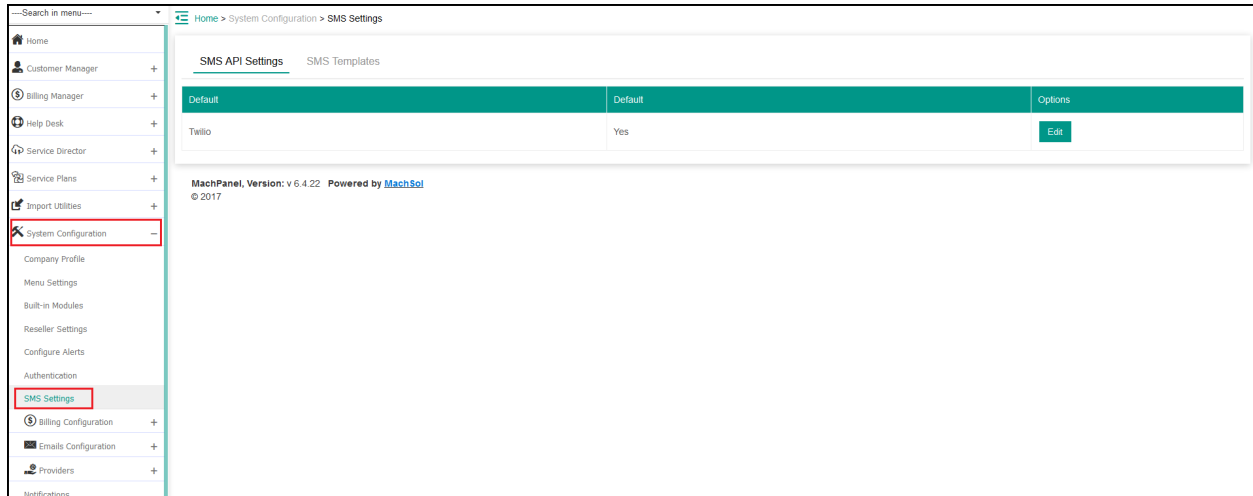
You can configure Email address at following path: **Home > System Configuration > Emails Configuration > Email Templates**

The screenshot shows the 'Email Templates' configuration page. The breadcrumb trail is 'Home > System Configuration > Emails Configuration > Email Templates'. The left sidebar shows the navigation menu with 'Email Templates' highlighted. The main content area is titled 'Password Notification Emails'. It contains fields for 'Email from name', 'Email from address', 'Email CC address', 'Reply-To name', 'Reply-To Address', and 'Email BCC address'. A red box highlights the 'Email from name', 'Email from address', and 'Reply-To name' fields, with a tooltip saying 'Configure Email address here.' pointing to the 'Email CC address' field. Below these fields are several email templates listed with 'Edit Template' buttons: 'Password Update (CP)', 'Password Recovery', 'Password update notification.', 'Account Information', 'Active Directory user setup information', 'Two Factor Authentication - PIN Email' (highlighted), and 'Password Update (Client)'.

## Two-factor authentication (2FA)

### Send PIN through SMS

For this option you have to navigate to **System Configuration > SMS Setting**



Provide **Twilio API Settings**.

1. **Account SID:** Here provide the twilio Account SID.
2. **Auth Token:** Provide twilio account authentication token
3. **Number:** Provide your number.
4. **Twilio API URL:** Provide the Twilio API URL.

The screenshot shows the 'Twilio API Settings' form. It has four input fields: '\*Account SID:', '\*Auth Token:', '\*Number:', and '\*Twilio API Url:'. The '\*Twilio API Url:' field is pre-filled with 'https://api.twilio.com/2010-04-01/'. There are two buttons: 'Save Settings' at the bottom left and 'Send Test SMS' next to the '\*Twilio API Url:' field.

## SMS Templates

Navigate to **System Configuration > SMS Setting > SMS Template** Add "Templates" for the PIN SMS to be sent. See snapshot below:

## Two-factor authentication (2FA)



SMS API Settings SMS Templates

Add Template

\*Template Name:

\*SMS Body:

%PINCode%  
%UserName%  
%CompanyName%

\*Insert Variable: --Select--

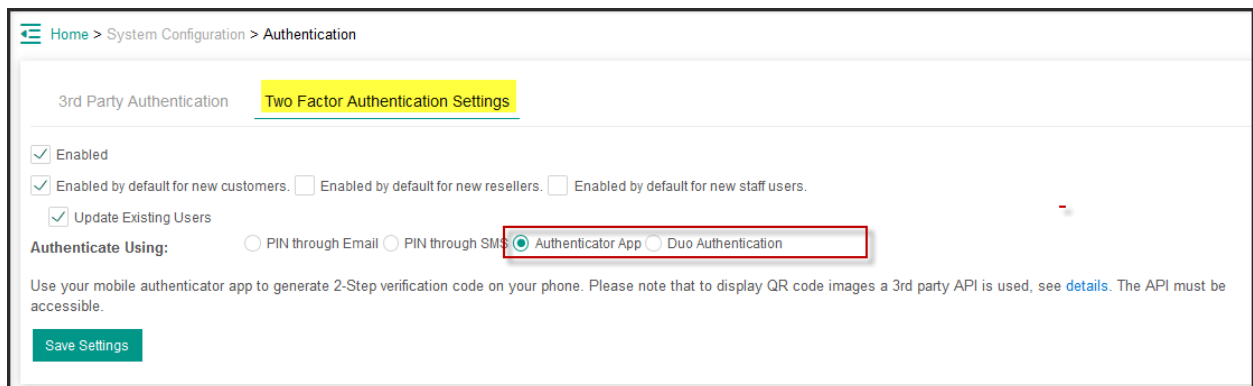
\*Language: English

\*Purpose: Two Factor Authentication

Save Cancel

### Authenticator App

Mobile Authenticator App can be used to enable **App Authentication** in MachPanel. The **Duo Authentication** is also supported.



Home > System Configuration > Authentication

3rd Party Authentication Two Factor Authentication Settings

☒ Enabled

☒ Enabled by default for new customers. ☐ Enabled by default for new resellers. ☐ Enabled by default for new staff users.

☒ Update Existing Users

Authenticate Using: ☐ PIN through Email ☐ PIN through SMS ☒ Authenticator App ☐ Duo Authentication

Use your mobile authenticator app to generate 2-Step verification code on your phone. Please note that to display QR code images a 3rd party API is used, see [details](#). The API must be accessible.

Save Settings

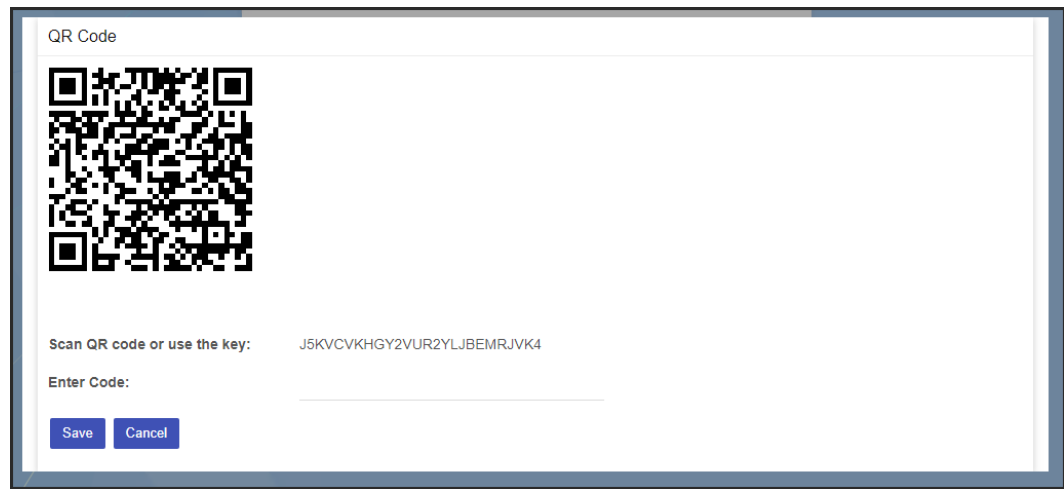
## How Login Works for Authenticator app?

1. 1st time login
  - a. After password is verified
  - b. User is shown a QR code
  - c. User will scan QR code using any app, suggested apps are (Google Authenticator, Microsoft Authenticator, Authy 2-Factor Authentication)
  - d. When QR code is scanned, user will get 6-digit auth code in application.

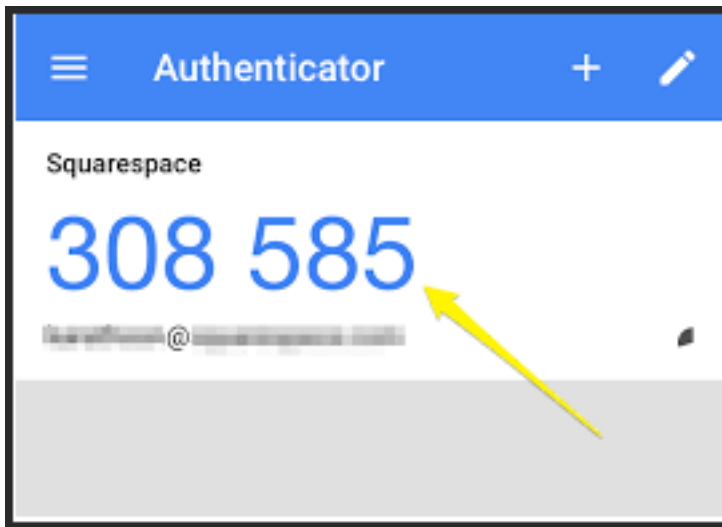


## Two-factor authentication (2FA)

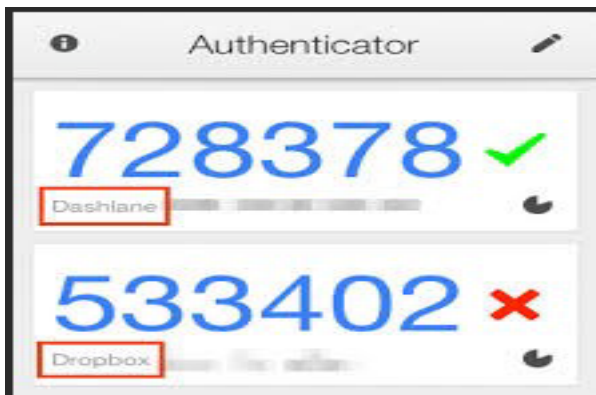
- i. Warning: Code changes in 30 seconds.



- ii. 6-digit TOTP Code in application

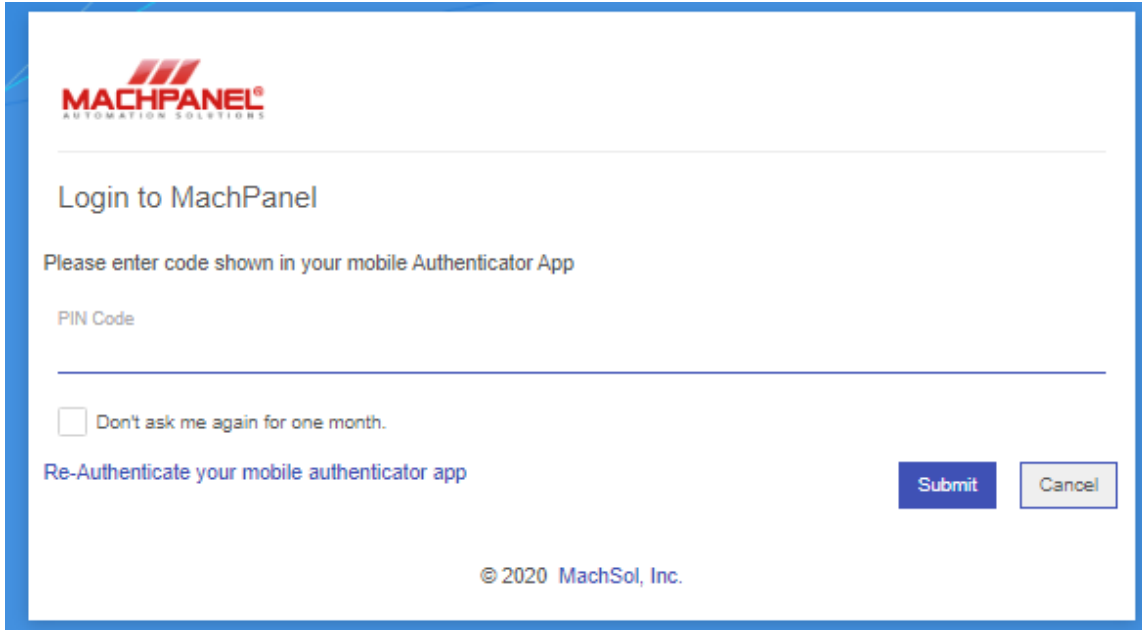


3. In case user account is duplicated, then latest one will be valid.



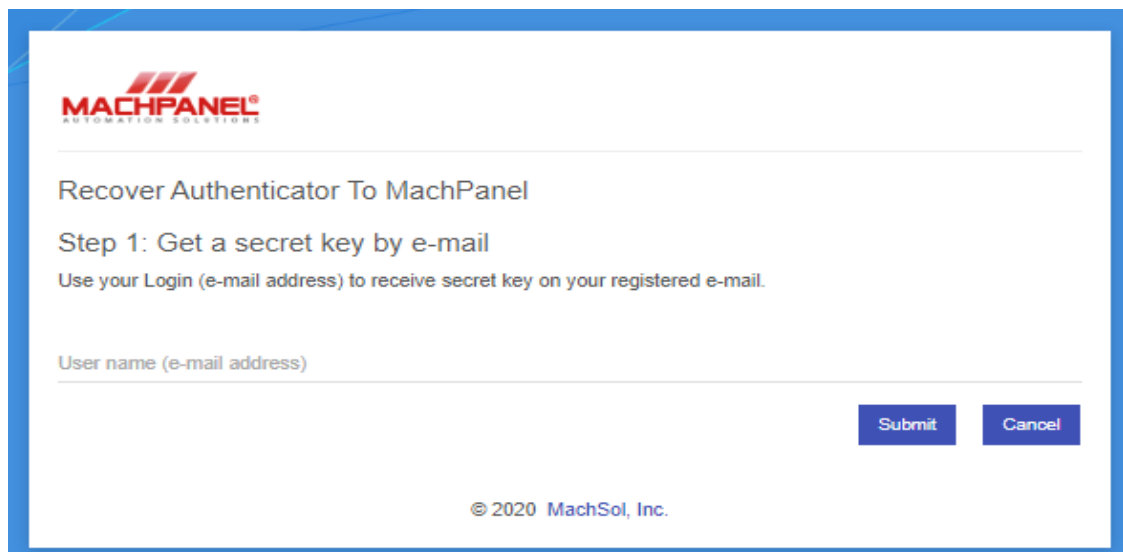
## Two-factor authentication (2FA)

- e. User will input code, if code is accepted user is logged in.
- 2. Returning user login
  - a. Same as 1st time login but no need to scan QR code.
  - b. User just needs to enter code from his mobile app.



The screenshot shows the MachPanel login interface. At the top is the MachPanel logo with the tagline 'AUTOMATION SOLUTIONS'. Below the logo is the heading 'Login to MachPanel'. A message states: 'Please enter code shown in your mobile Authenticator App'. There is a text input field labeled 'PIN Code'. Below the input field is a checkbox with the text 'Don't ask me again for one month.' and a link that says 'Re-Authenticate your mobile authenticator app'. At the bottom right are two buttons: 'Submit' and 'Cancel'. At the bottom center is the copyright notice '© 2020 MachSol, Inc.'.

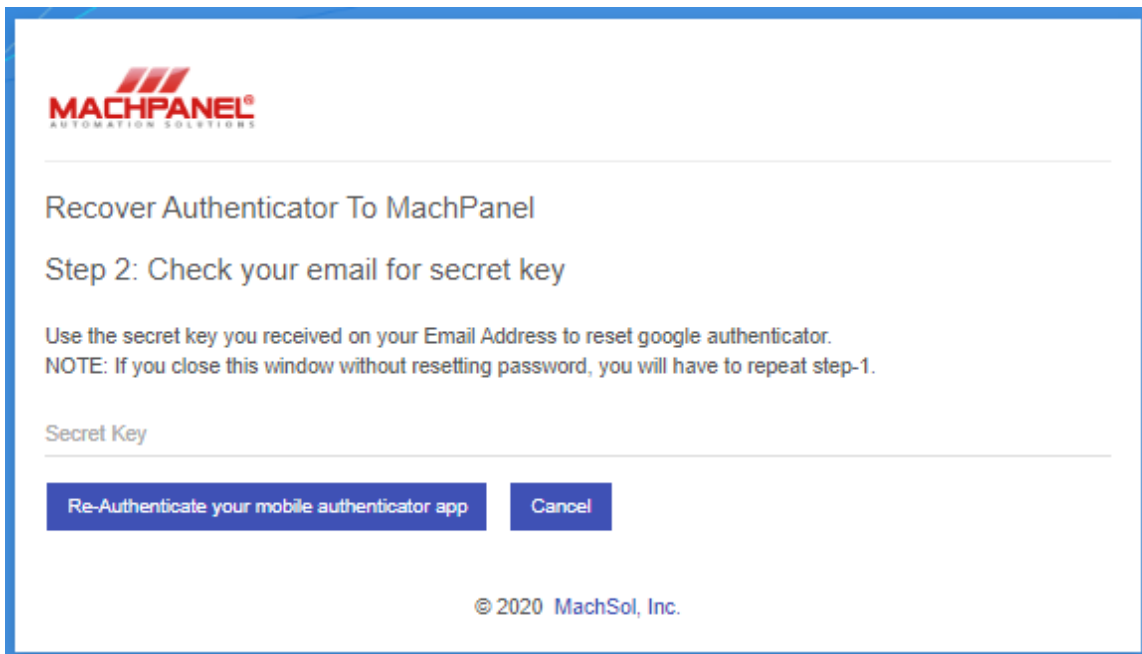
- 3. Reset Authenticator App.
  - a. Needed in case user lost his device, or reinstalled app and does not have code available.
  - b. Click on [Re-Authenticate your mobile authenticator app](#) link.
  - c. Enter registered email address and hit **Submit** to get secret key on your registered email address:



The screenshot shows the MachPanel 'Recover Authenticator' interface. At the top is the MachPanel logo with the tagline 'AUTOMATION SOLUTIONS'. Below the logo is the heading 'Recover Authenticator To MachPanel'. Underneath is 'Step 1: Get a secret key by e-mail'. A message states: 'Use your Login (e-mail address) to receive secret key on your registered e-mail.' There is a text input field labeled 'User name (e-mail address)'. At the bottom right are two buttons: 'Submit' and 'Cancel'. At the bottom center is the copyright notice '© 2020 MachSol, Inc.'.

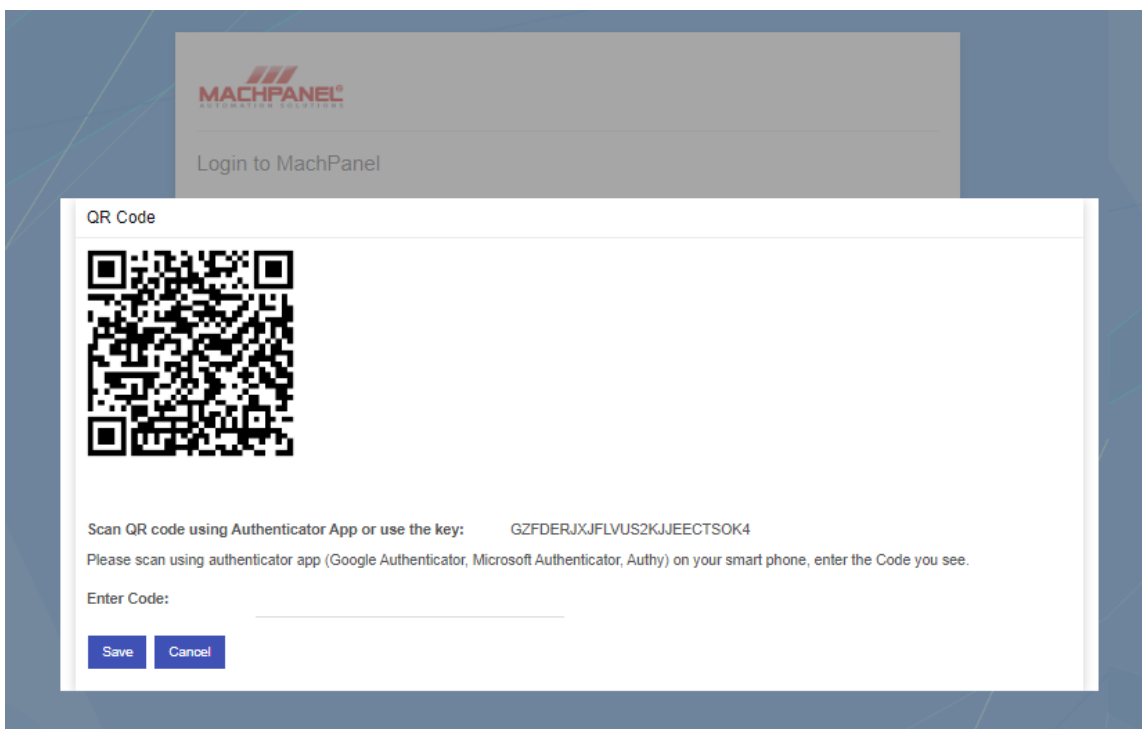
## Two-factor authentication (2FA)

- d. Check your email for secret key and enter the received secret key on Step 2 and hit "Re-Authenticate your mobile authenticator app" button:



The screenshot shows a web interface for MachPanel. At the top is the MachPanel logo with the tagline 'AUTOMATION SOLUTIONS'. Below the logo, the heading 'Recover Authenticator To MachPanel' is displayed. Underneath, 'Step 2: Check your email for secret key' is shown. A paragraph of text reads: 'Use the secret key you received on your Email Address to reset google authenticator. NOTE: If you close this window without resetting password, you will have to repeat step-1.' Below this text is a label 'Secret Key' followed by a horizontal line. At the bottom of the form are two buttons: 'Re-Authenticate your mobile authenticator app' and 'Cancel'. The footer of the page shows '© 2020 MachSol, Inc.'

- a. Finally you will be taken to login screen, where you can enter your login/password and then you will be asked to register a new authenticator app.



The screenshot shows the MachPanel login screen. The background is a dark blue gradient. In the center, there is a grey box with the MachPanel logo and the text 'Login to MachPanel'. Overlaid on this is a white modal window titled 'QR Code'. Inside the modal, there is a QR code. Below the QR code, the text reads: 'Scan QR code using Authenticator App or use the key: GZFDERJXJFLVUS2KJJEECTSOK4'. Below this, it says: 'Please scan using authenticator app (Google Authenticator, Microsoft Authenticator, Authy) on your smart phone, enter the Code you see.' There is a label 'Enter Code:' followed by a text input field. At the bottom of the modal are two buttons: 'Save' and 'Cancel'.

## Two-factor authentication (2FA)

MachPanel Knowledgebase

<https://kb.machsol.com/Knowledgebase/54540/Two-factor-authentication-2FA->