Two-factor authentication (2FA)

Summary

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

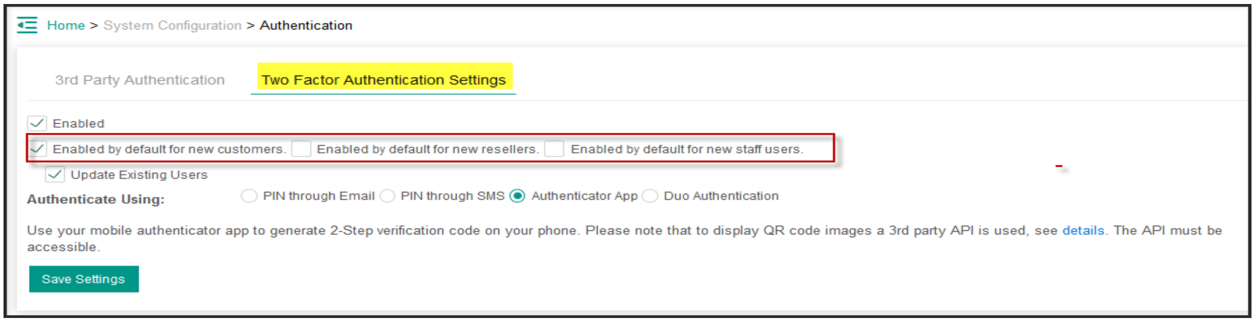
Applies To

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.



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

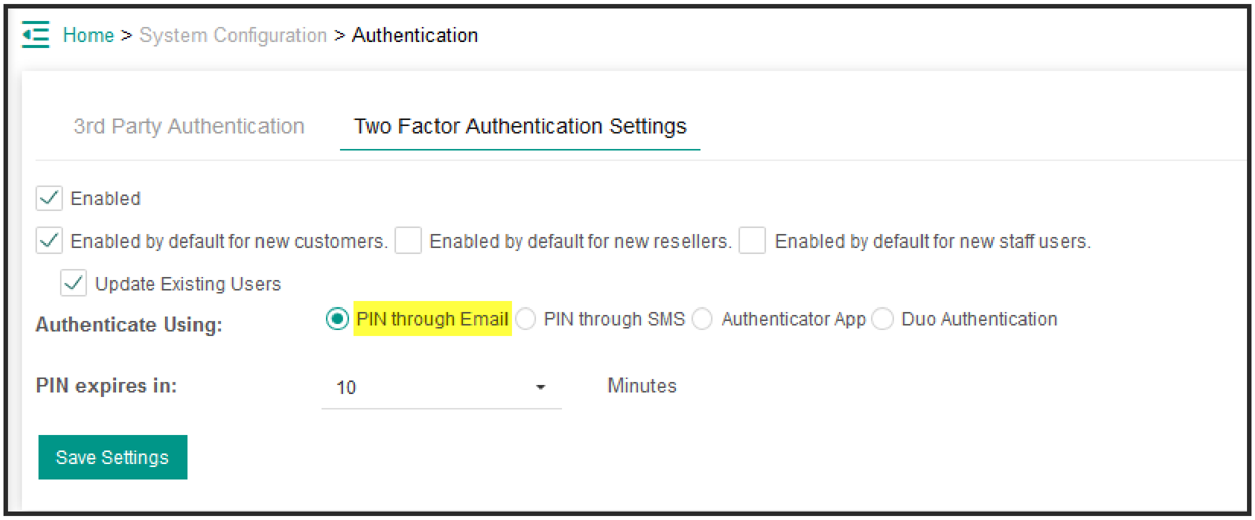
Two-factor authentication (2FA)

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



Home > System Configuration > Authentication

☑ Enabled

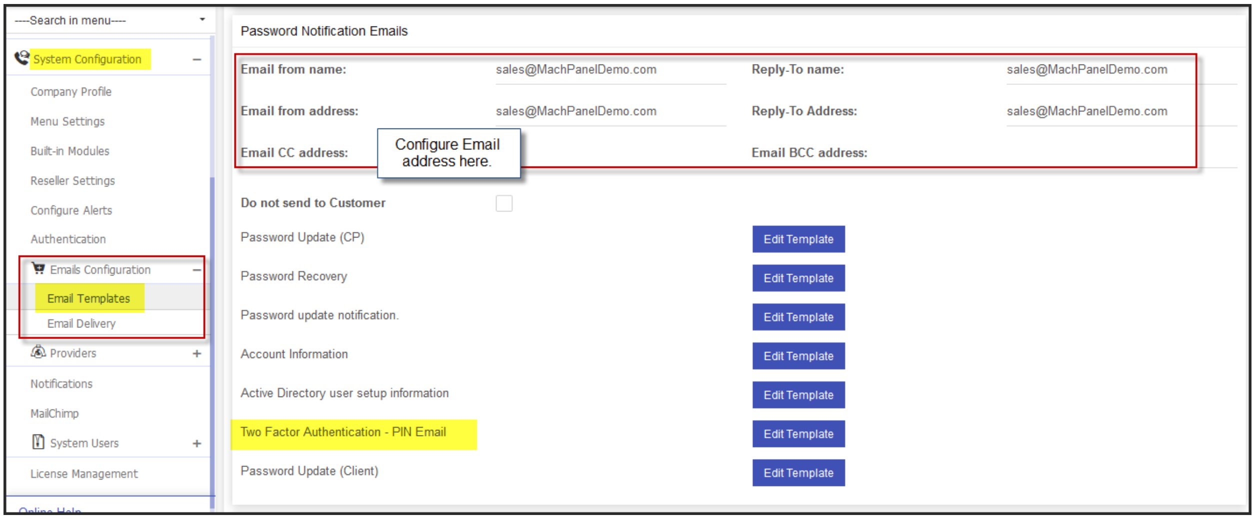
☑ Enabled by default for new customers. □ Enabled by default for new resellers. □ Enabled by default for new staff users.

☑ Update Existing Users

Authenticate Using: ● PIN through Email ○ PIN through SMS ○ Authenticator App ○ Duo Authentication

PIN expires in: 10 Minutes

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



Password Notification Emails

Email from name:	sales@MachPanelDemo.com	Reply-To name:	sales@MachPanelDemo.com
Email from address:	sales@MachPanelDemo.com	Reply-To Address:	sales@MachPanelDemo.com
Email CC address:		Email BCC address:	

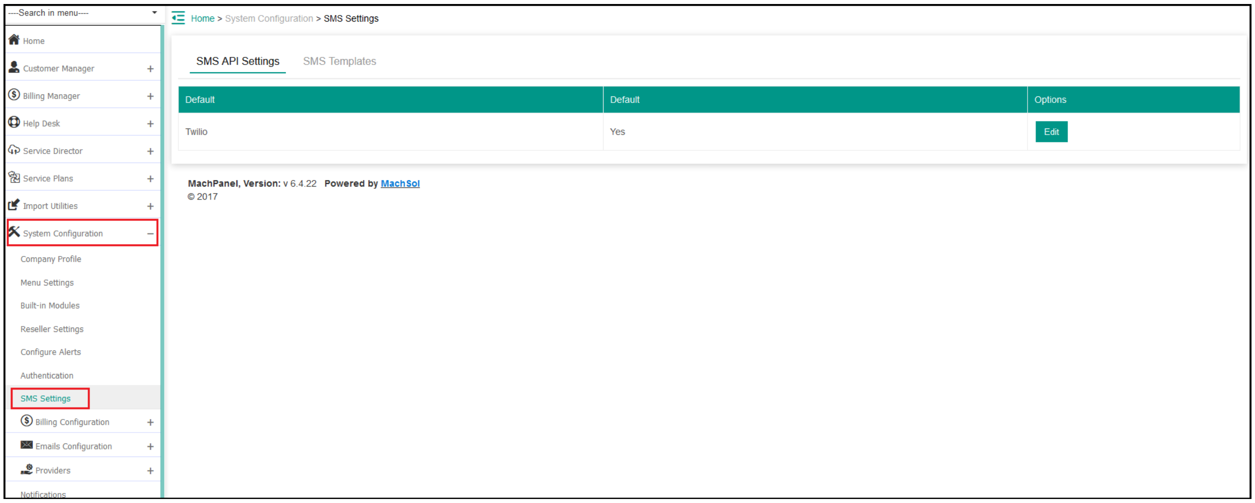
Configure Email address here.

Do not send to Customer □

Password Update (CP)	Edit Template
Password Recovery	Edit Template
Password update notification.	Edit Template
Account Information	Edit Template
Active Directory user setup information	Edit Template
Two Factor Authentication - PIN Email	Edit Template
Password Update (Client)	Edit Template

Send PIN through SMS

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

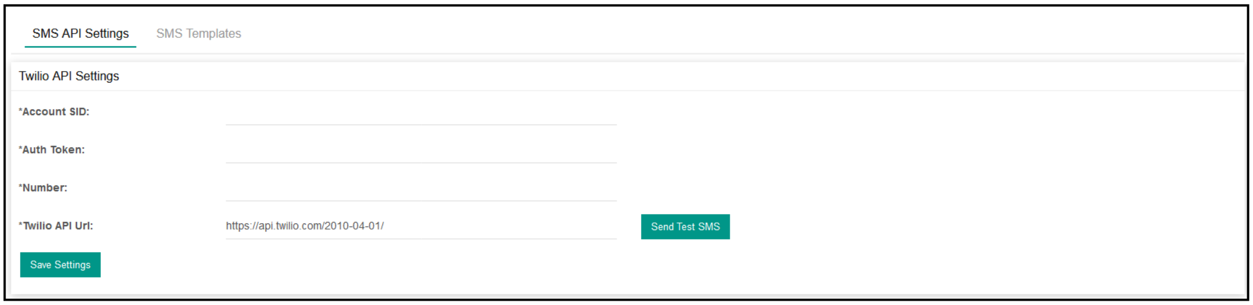


Default	Default	Options
Twilio	Yes	Edit

MachPanel, Version: v 6.4.22 **Powered by** MachSol
© 2017

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.



Twilio API Settings

*Account SID:

*Auth Token:

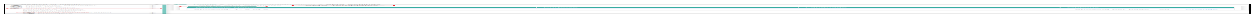
*Number:

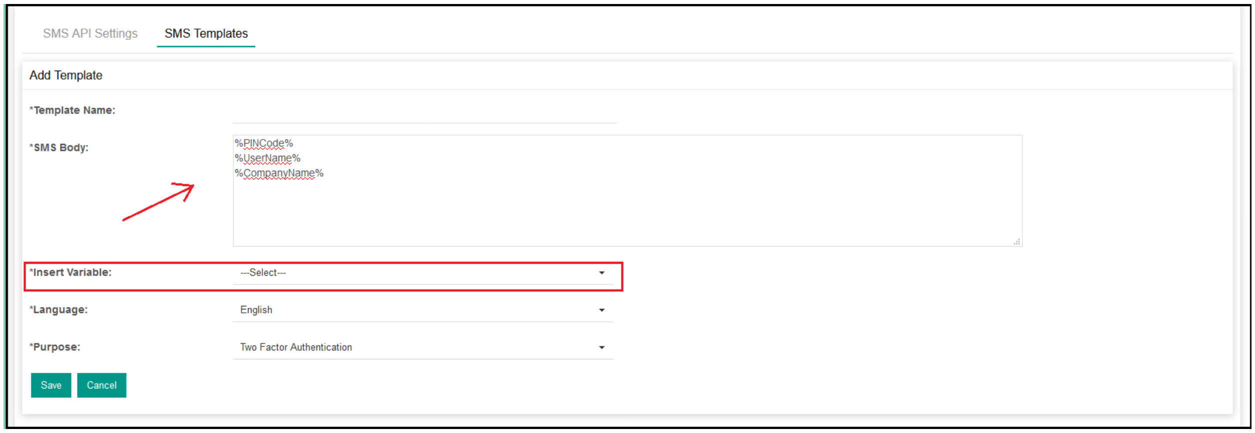
*Twilio API Url: https://api.twilio.com/2010-04-01/

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%

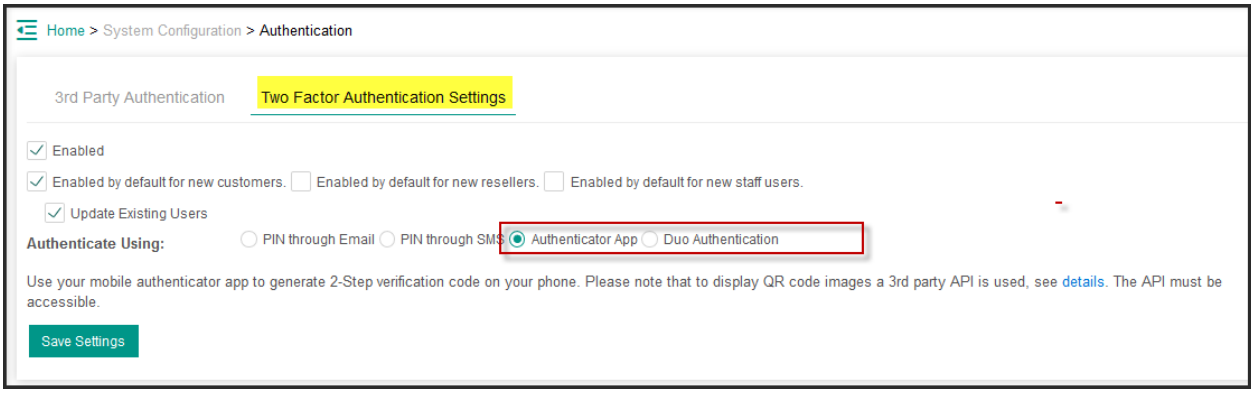
*Insert Variable: ---Select---

*Language: English

*Purpose: Two Factor Authentication

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

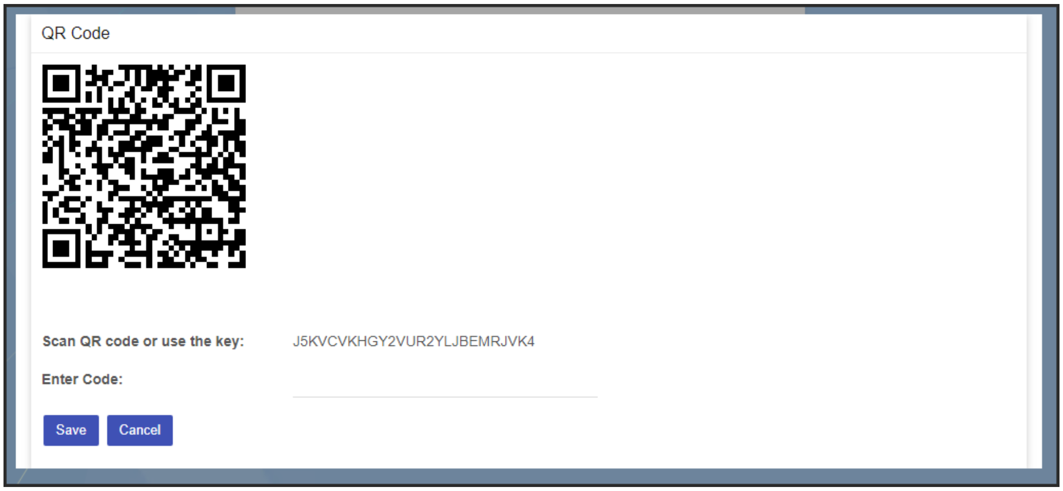
Use your mobile authenticator app to generate 2-Step verification code on your phone. Please note that to display QR code images a 3rd party API is used, see details. The API must be accessible.

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.

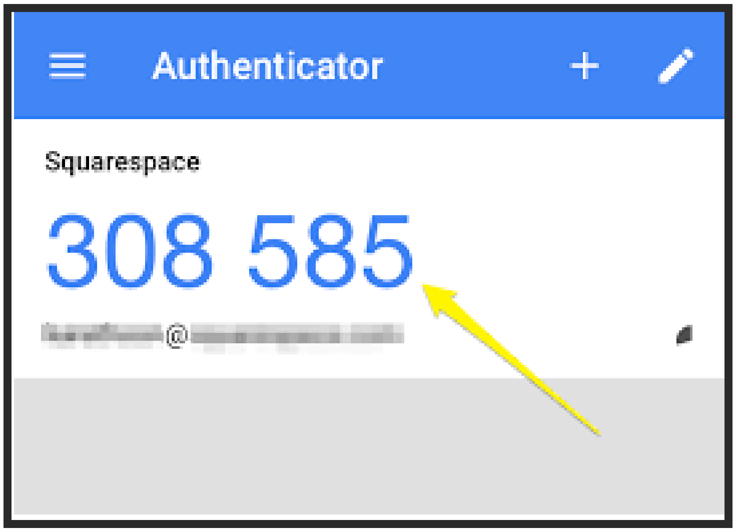


QR Code

Scan QR code or use the key: J5KVCVKHGY2VUR2YLJBEMRJVK4

Enter Code:

ii. 6-digit TOTP Code in application

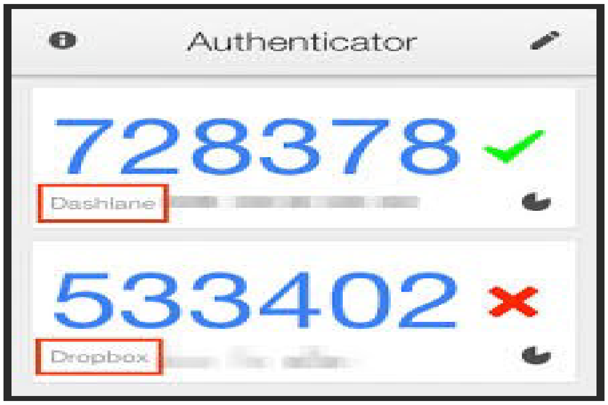


Squarespace

308 585

[redacted]

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



728378 ✓

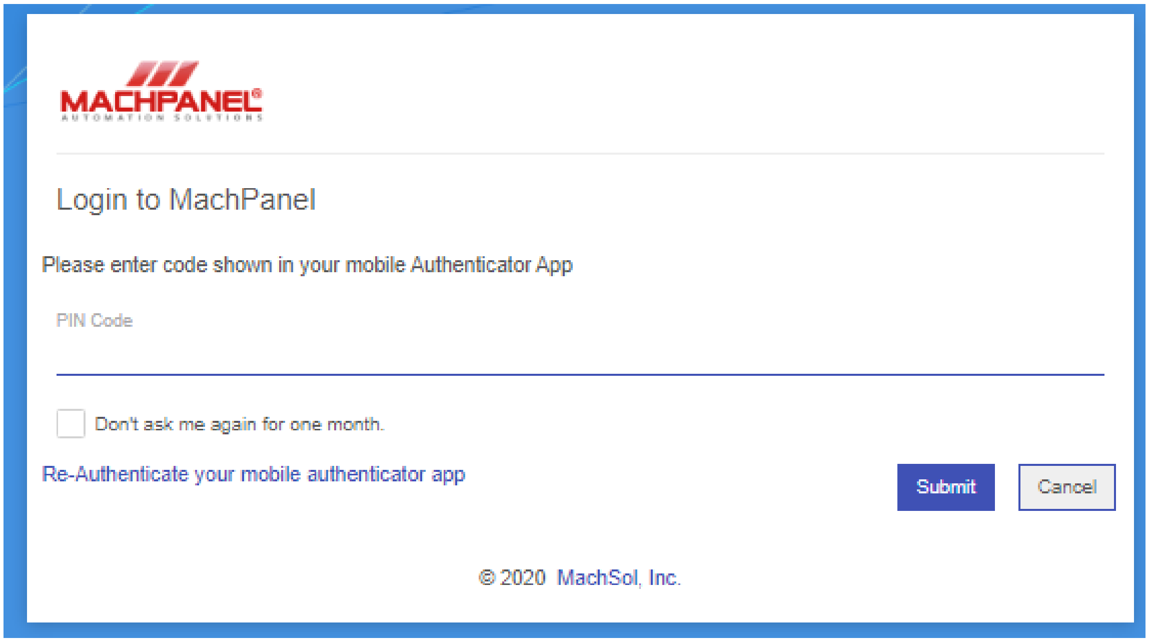
Dashlane [redacted]

533402 ✗

Dropbox [redacted]

   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.



Login to MachPanel

Please enter code shown in your mobile Authenticator App

PIN Code

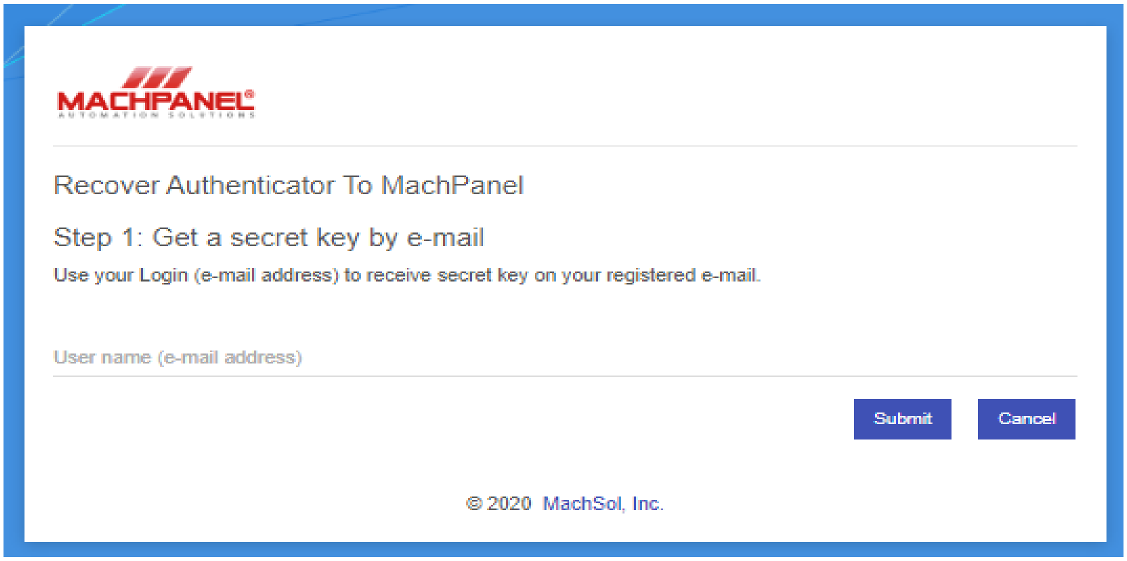
□ Don't ask me again for one month.

Re-Authenticate your mobile authenticator app

© 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:



Recover Authenticator To MachPanel

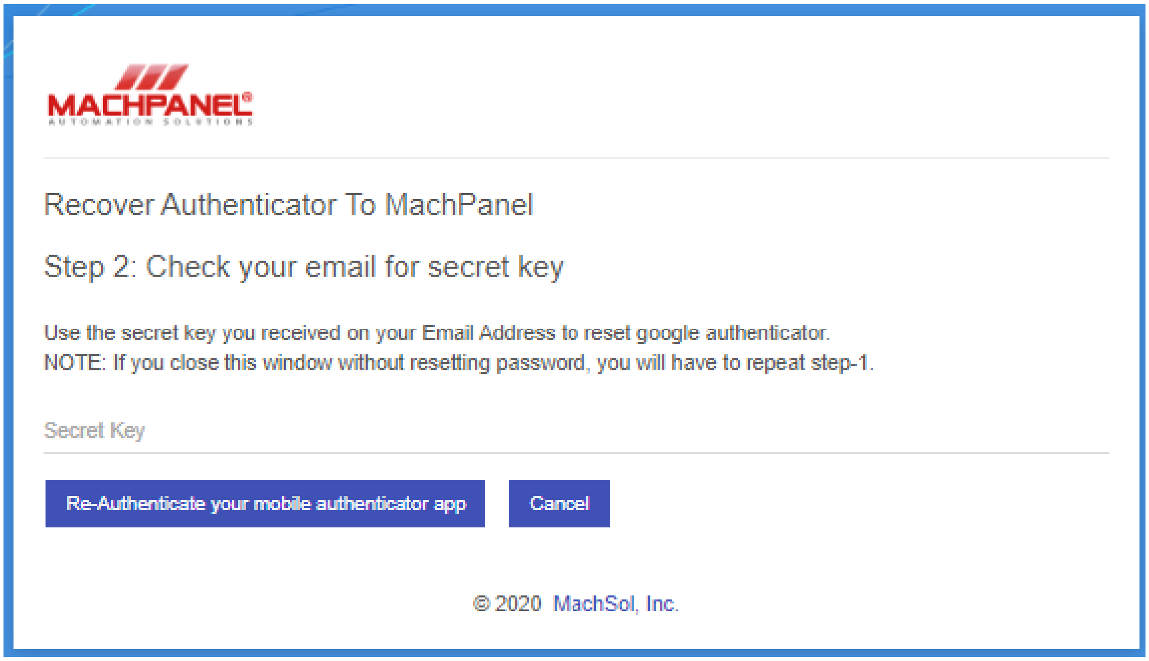
Step 1: Get a secret key by e-mail

Use your Login (e-mail address) to receive secret key on your registered e-mail.

User name (e-mail address)

© 2020 MachSol, Inc.

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:



Recover Authenticator To MachPanel

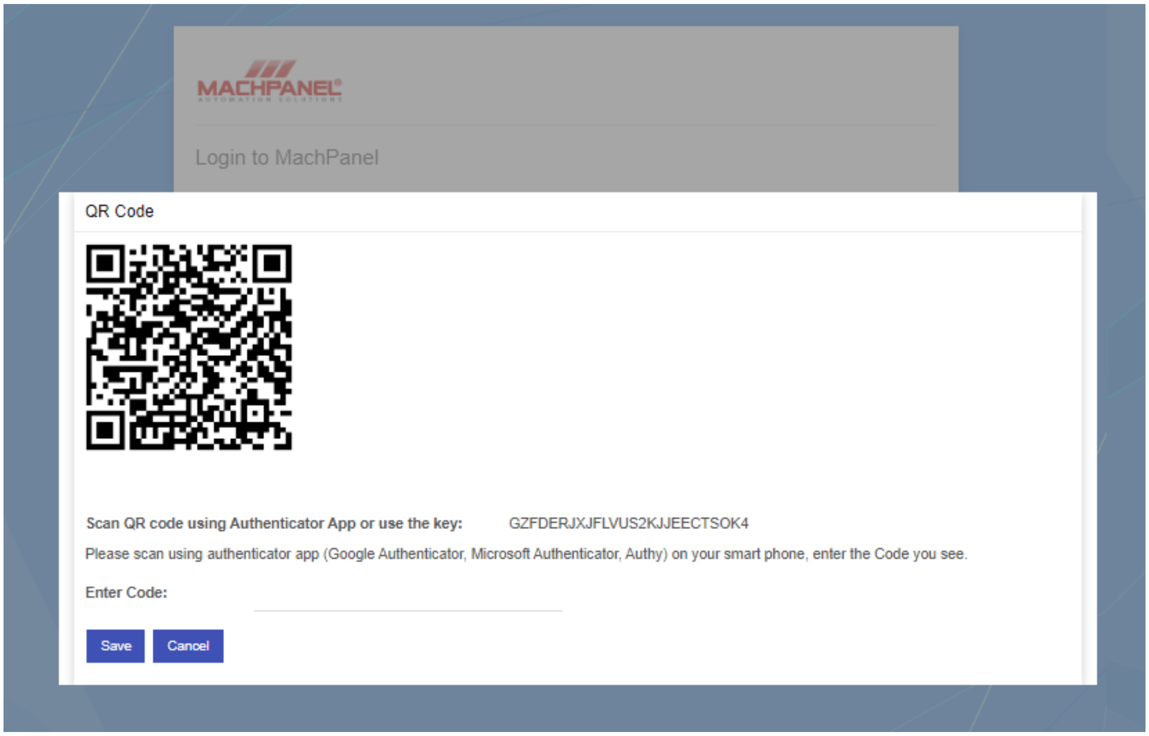
Step 2: Check your email for secret key

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.

Secret Key

© 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.



Scan QR code using Authenticator App or use the key: GZFDERJXJFLVUS2KJJEECTSOK4

Please scan using authenticator app (Google Authenticator, Microsoft Authenticator, Authy) on your smart phone, enter the Code you see.

Enter Code:

Two-factor authentication (2FA)

MachPanel Knowledgebase
https://kb.machsol.com/Knowledgebase/54540/Twofactor-authentication-2FA-