Multi-Factor Authentication: Admin

Table of Contents

Introduction

To better protect data security and customer information, Total Expert allows you to set up multi-factor authentication (MFA) for your organization's users. This requires them to provide a securely generated code in addition to their user name and password to log in. This extra proof of identity makes it much less likely that a compromised password can be used to access sensitive information stored in a user account.

Your organization can make MFA required for all users, optional for all users, or unavailable to any users.

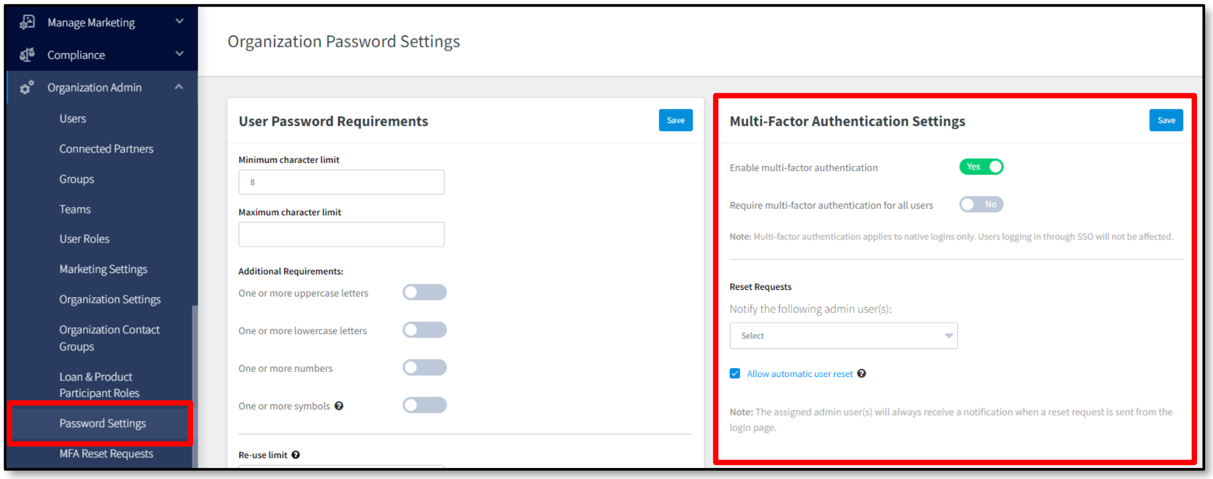
Note
If a given person uses a single sign-on (SSO) service to log in to Total Expert, then that service uses its own authentication steps and bypasses Total Expert's MFA (even if MFA is active for their Total Expert account).

Organization Setup

After you complete the following steps, each individual user is responsible for associating their own account with an authenticator app by using a QR code. See *Multi-Factor Authentication: User* for more information.

Note
Total Expert does not use codes sent by SMS. Authenticator apps are more secure.

1. Navigate to **Organization Admin → Password Settings** and locate the Multi-Factor Authentication Settings section.



Organization Password Settings

User Password Requirements

Minimum character limit: 8

Maximum character limit:

Additional Requirements:

One or more uppercase letters

One or more lowercase letters

One or more numbers

One or more symbols

Re-use limit

Multi-Factor Authentication Settings

Enable multi-factor authentication: Yes

Require multi-factor authentication for all users: No

Note: Multi-factor authentication applies to native logins only. Users logging in through SSO will not be affected.

Reset Requests

Notify the following admin user(s): Select

☑ Allow automatic user reset

Note: The assigned admin user(s) will always receive a notification when a reset request is sent from the login page.

©2024 Total Expert Inc. All Rights Reserved.

2. Click the **Enable multi-factor authentication** toggle switch to move it to the **Yes** position.
   - With this switch set to Yes, MFA is enabled for all users in your organization.
   - With this switch set to No, MFA is disabled and cannot be used by anyone in your organization.
3. (optional) Click the **Require multi-factor authentication for all users** toggle switch to move it to the **Yes** position.
   - With this switch set to Yes, every user is required to set up MFA for their account.
   - With this switch set to No, each user in your organization can decide whether or not to set up MFA for their individual account (assuming the first switch is toggled to Yes).
4. In the **Reset Requests** field, select 1 or more users who should be notified when a user requests to reset the MFA setup for their account. The drop-down list includes only active users designated by permission as administrators in your organization

Note
You must select at least 1 user in this field, or you cannot save your changes in this section.

5. (optional) Check the **Allow automatic user reset** box to allow users to reset the MFA setup for their account.
   - If this is selected, a user can reset their MFA setup after logging in with the existing setup. This allows a user who gets a new device to use their old device to log in, then create a new setup using a new device.
   - If this is not selected, one of the selected administrator(s) must manually reset the user's MFA setup, even if it is requested after the user logs in.
6. Click the **Save** button in the upper-right corner of the section.

Warning
If you do not click the Save button, your changes will be lost.

If you disable MFA for your organization as a whole, individual users who have already set up MFA for their accounts are no longer challenged after providing their user name and password. If you later re-enable MFA for the organization, the existing setup for those users takes effect again automatically.

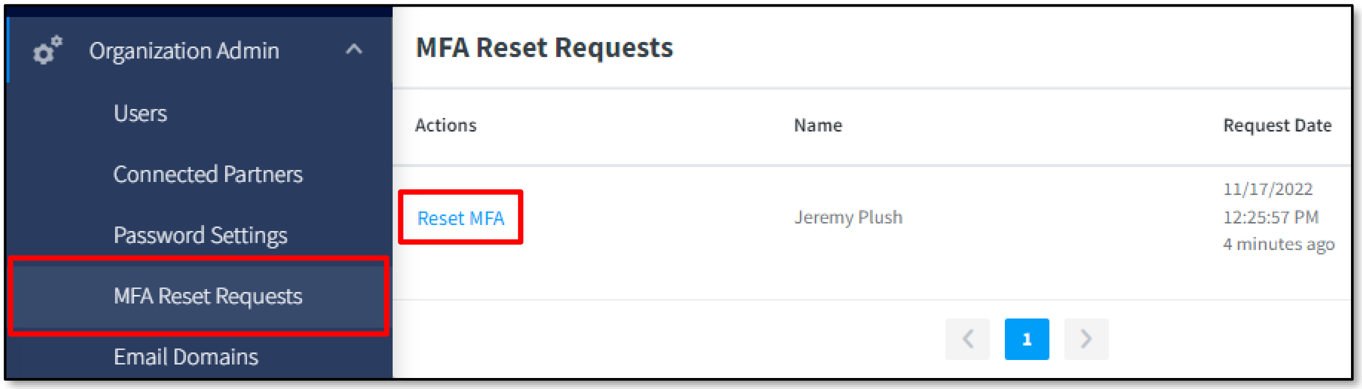
Handling a User's Reset Request

When a user has lost access to their authentication information (for example, by losing their device), they can request to have an admin reset the MFA for their account. When this happens, any admin users indicated in the Reset Requests field are notified by email that a reset has been requested.

Warning
The notification email tells you which user requested the reset. You should reach out to this user by trusted means to determine whether the request is legitimate. Do not proceed with the following steps until this is verified.

1. If the request is legitimate, click the **View Reset Requests** link in the email or navigate to **Organization Admin → MFA Reset Requests** in the platform.
2. Locate the relevant request in the list. The user for each request is listed along with the date and time of the request.
3. Click **Reset MFA** in the Actions column.

©2024 Total Expert Inc. All Rights Reserved.



MFA Reset Requests

Actions	Name	Request Date
Reset MFA	Jeremy Plush	11/17/2022 12:25:57 PM 4 minutes ago

A success message appears, and the request is removed from the list. Additionally, the affected user is notified by email that the MFA setup for their account has been disabled.