Netsurion | EventTracker®

Two-factor Authentication (2FA) using Google Authenticator

EventTracker v9.3

Publication Date: May 12, 2020

Abstract

This guide helps users in configuring and using the Two-factor authentication (2FA) supported via Google Authenticator App on the phone (Android and IOS). This document also covers 2FA configuration by Admins in EventTracker v9.3. 2FA is also know as 2 Step Verification.

This guide shows you how you can secure the EventTracker v9.3 account by using password as well as Google Authenticator PIN. The Authenticator configured on your phone provides an additional level of security to the EventTracker Login.

It is an effective yet a simple way to authenticate and protect the users from the hackers. With 2FA enabled, hackers would not be able to log in even if the password is known.

Audience

EventTracker v9.3 users who want to setup additional level of security and configure 2FA.

Table of Contents

1. Configuring 2FA using Google Authenicator App

Install the Google Authenicator App on your phone.

Note: The Google Authenicator screens may vary on IOS devices. The screen references given are from Android phone.

1. Launch the Google Authenicator app. The following screen opens.

Note: If Google Authenticator App is already installed on your phone and configured for any other application, this screen will not be displayed.

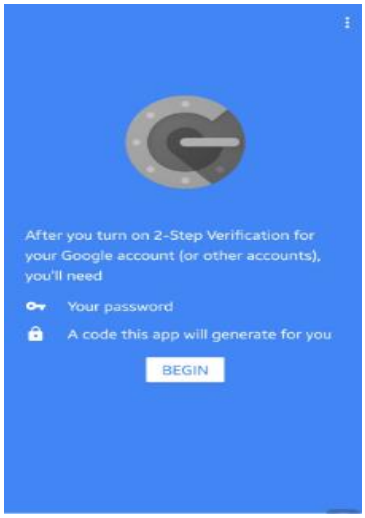

Figure 1

2. Click **Begin** to proceed further. **Add an account** screen opens.

Figure 2

You can select either of the two options to add an account

- **Scan a barcode**
- **Enter a provided key**.

1.1 Option 1: Scan a barcode

1. Login to the EventTracker from your computer with the user name and password.
   Two-factor Authentication Using Google Authenticator page opens. **QR Code** option is selected by default.

   Note: This page is displayed only when your administrator has enabled 2FA for your account.

2. On Google Authenticator App, select "Scan a barcode" option and capture the QR code availiable on the screen.

   Note: By default, the Account name is captured as your EventTracker domain. If you wish to change it, please enter the name of your choice and reload the QR code and scan the same to proceed further.

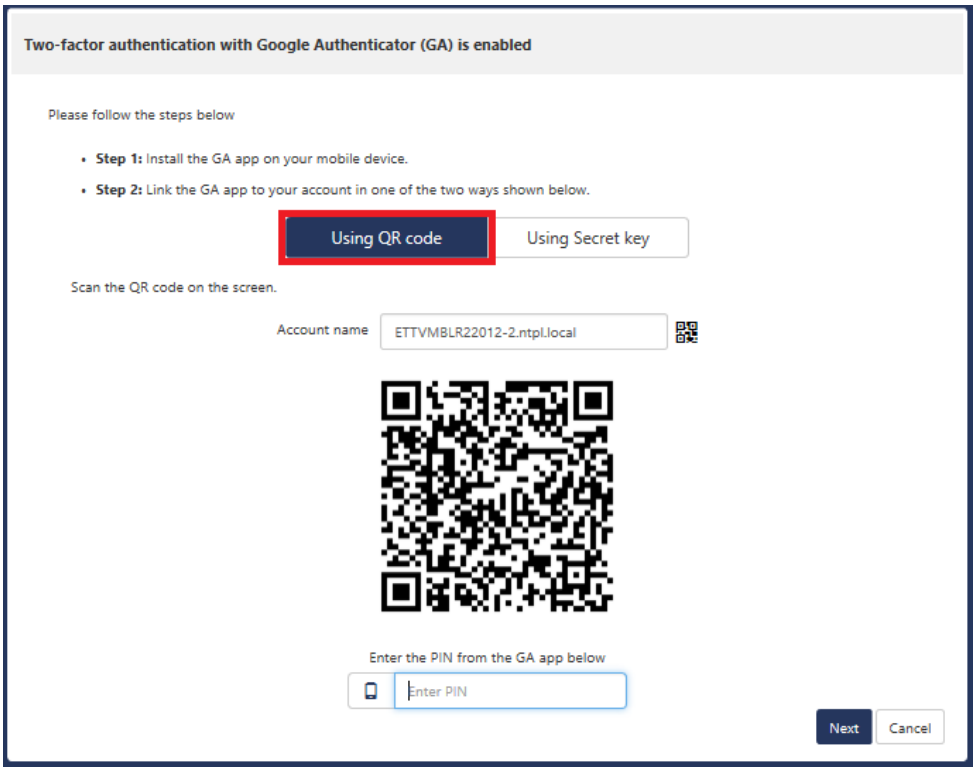

Figure 3

3. After the QR code is scanned **Account added** screen appears and PIN is generated.

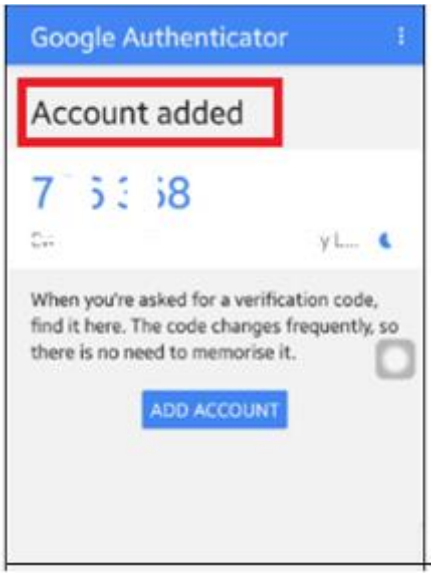

Figure 4

4. Enter the PIN (refer fig 4 for the PIN) and click **Next**. You will successfully log into EventTracker .

1.2 Option 2: Enter a provided key

1. Login to the EventTracker from your computer with user name and password.
   Two-factor Authentication Using Google Authenticator page opens.

   Note: This page is displayed only when your administrator has enabled 2FA for your account.

2. Select **Using Secret key** option**.** Secret key is generated.

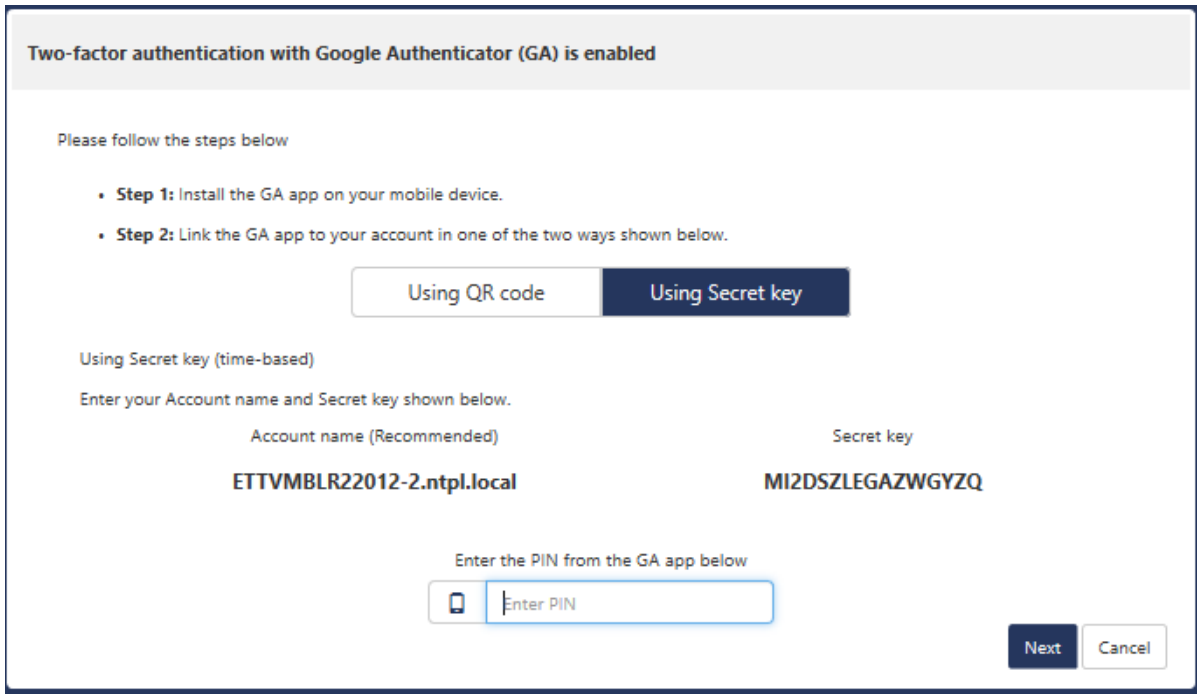

Figure 5

3. On Google Authenticator App, tap the **Enter a provided key** option on your phone.

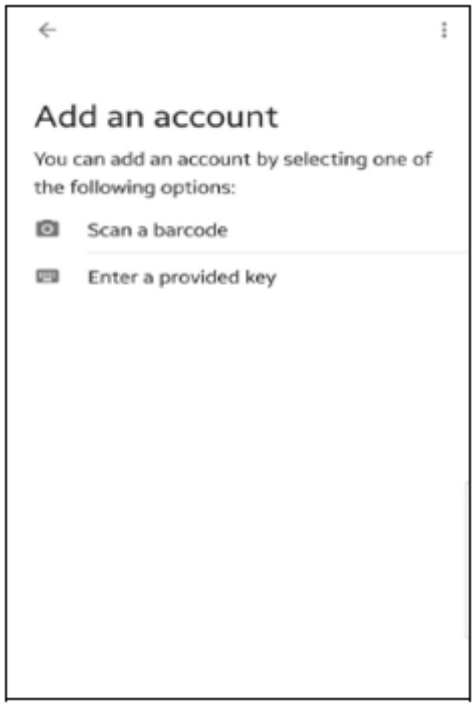

Figure 6

4. **Enter account details** screen opens. Provide the Account name of your choice and the key. once the account name of your choice and the key is entered click **Add**.

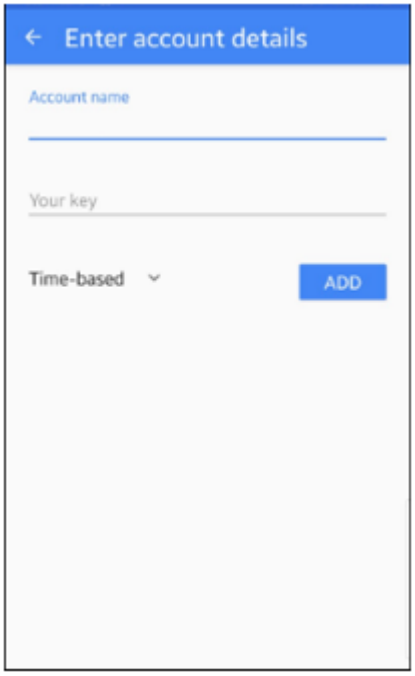

Figure 7

The following screen opens and a PIN is generated.

Figure 8

5. Enter the PIN and click **Next** . You will successfully log into EventTracker.

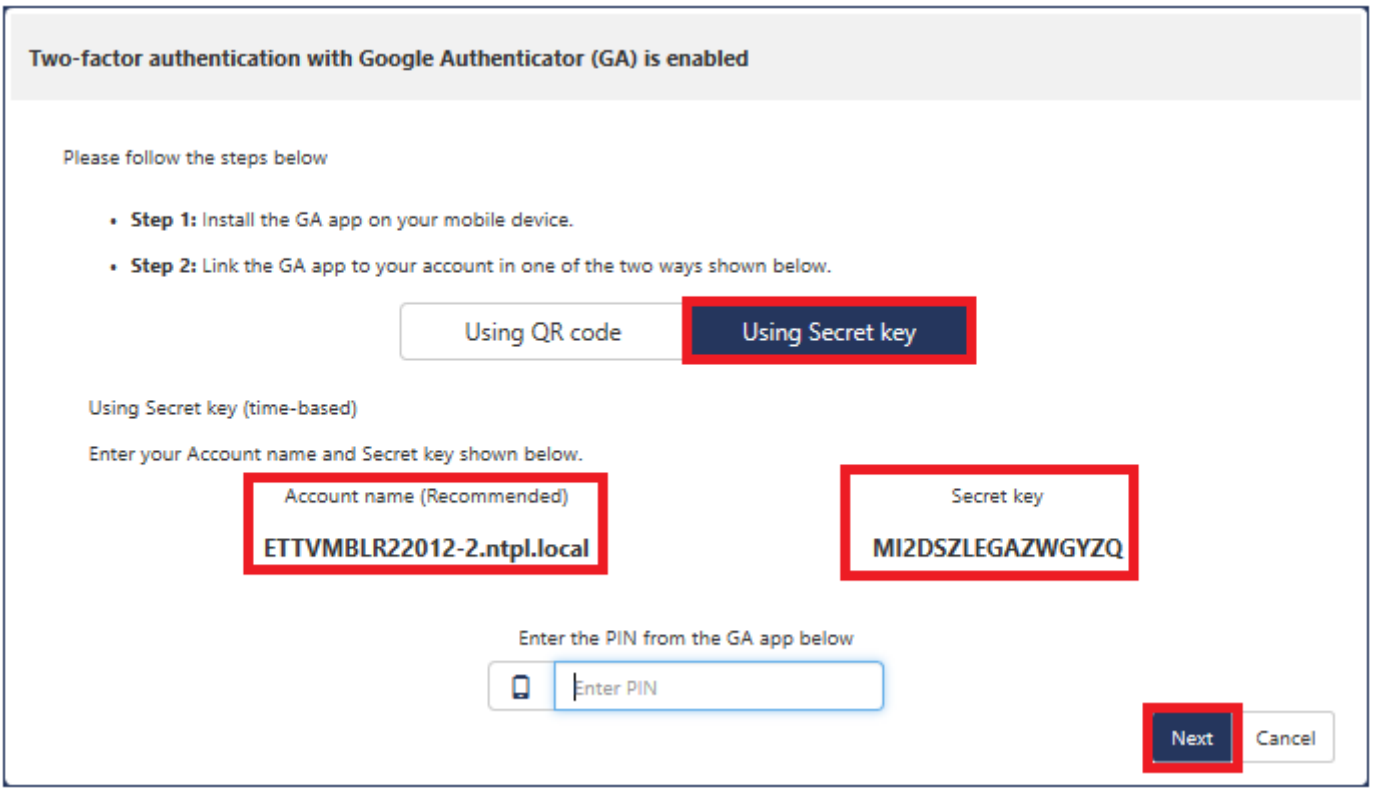

Figure 9

2. Logging into EventTracker after setting up 2FA

Now, each time when you login to the EventTracker with the username and password, you are prompted to enter the Google authentication PIN available on Google Authenticator app.

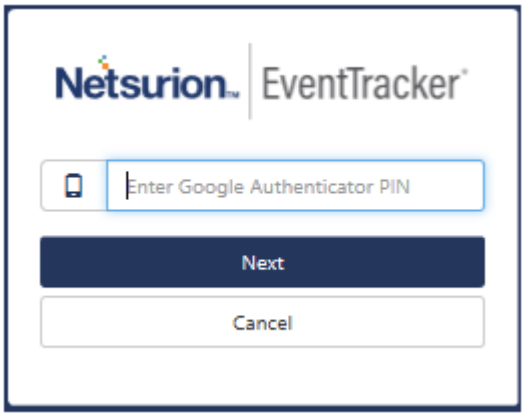

Figure 10

3. Enabling 2FA option in EventTracker v9.3

Note: This section is for EventTracker Admins and User Management admins who manages the users in EventTracker.

To enable 2FA option in EventTracker v9.3.

1. Log into EventTracker and click **Admin** and then click **Manager.**
2. The **Manager page** opens. Scroll down and enable 2FA authentication.

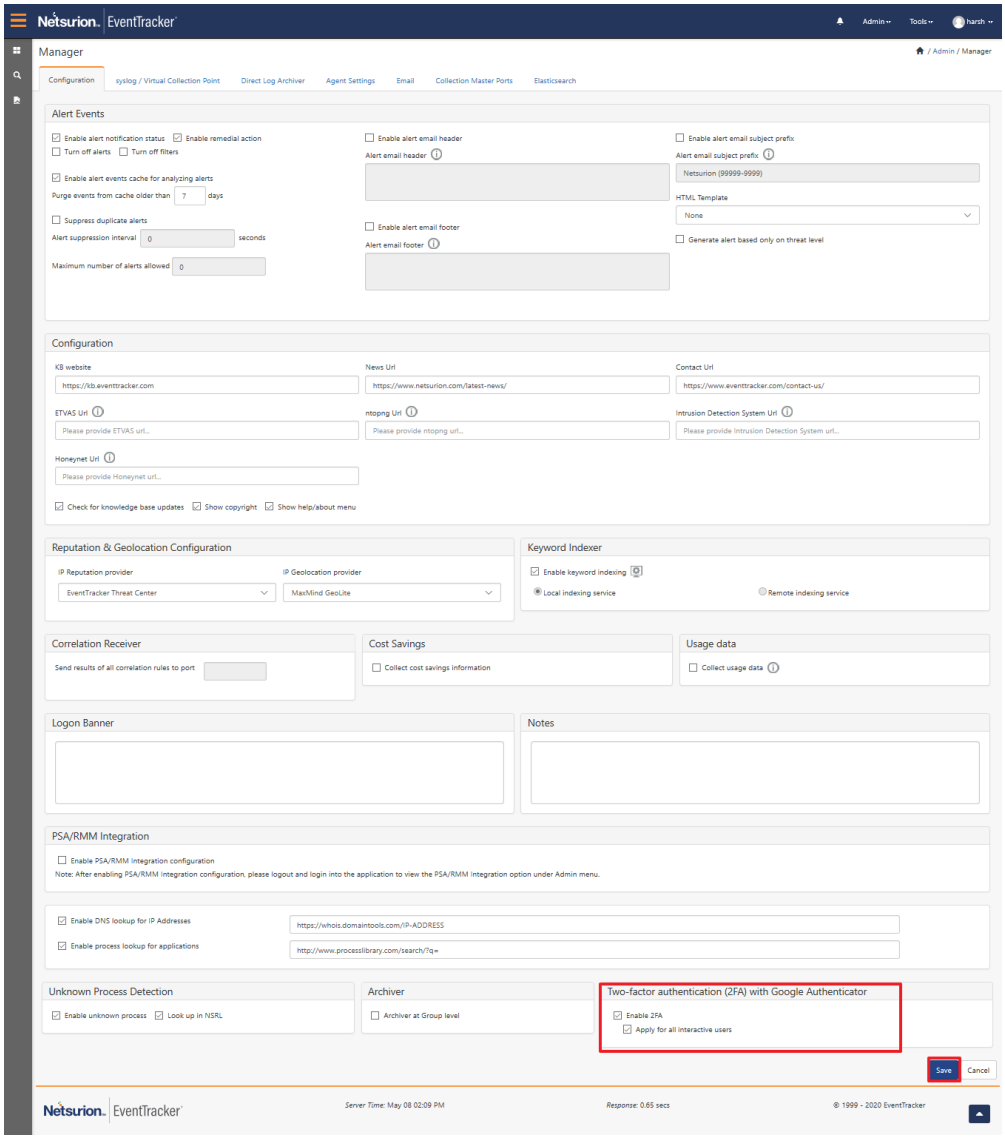

Figure 11

3. Enabling the 2FA option also enables the option **Apply for all interactive users**.

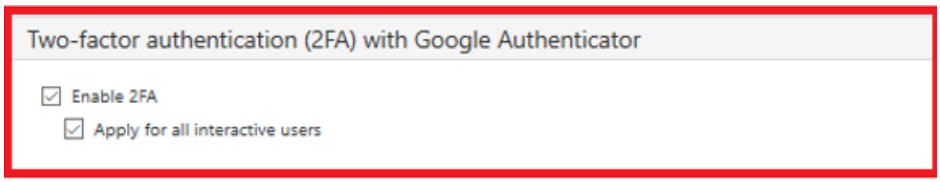

Figure 12

This will enable 2FA for all the interarctive users excluding EventTracker admins.

4. You can also disable the option **Apply for all interactive users** if you decide not to apply 2FA for any users. This option is helpful if you want to control the 2FA for individual users.

3.1 Enabling 2FA for individual user

This feature is applicable to EventTracker Admins, MSP Admins, MMSP Admins and those who manage the Users.

1. Click **Admin**-> **Users.** The users page opens.

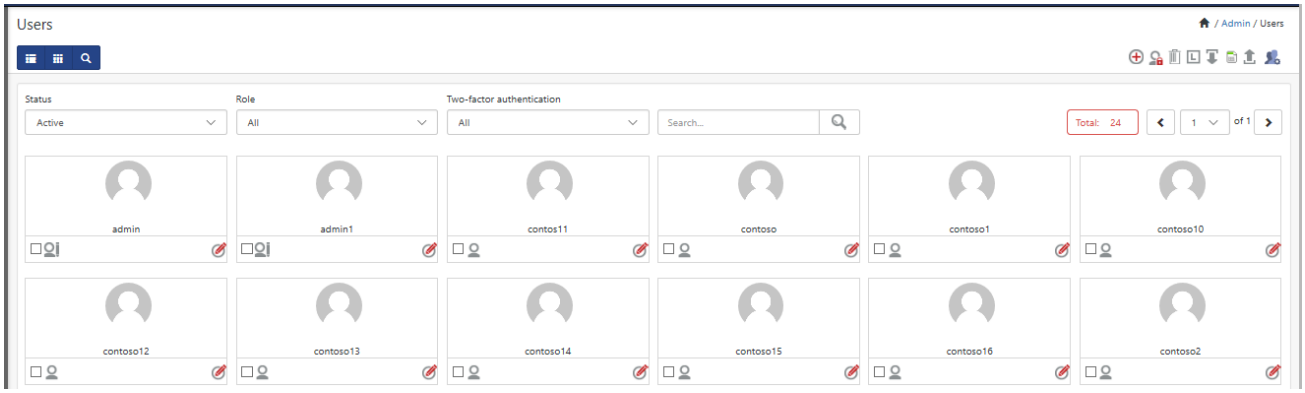

Figure 13

2. To Enable/Disable the 2FA authentication option for induvidual user level, Click Edit icon. Edit page opens and you can enable or disable 2FA for the users.

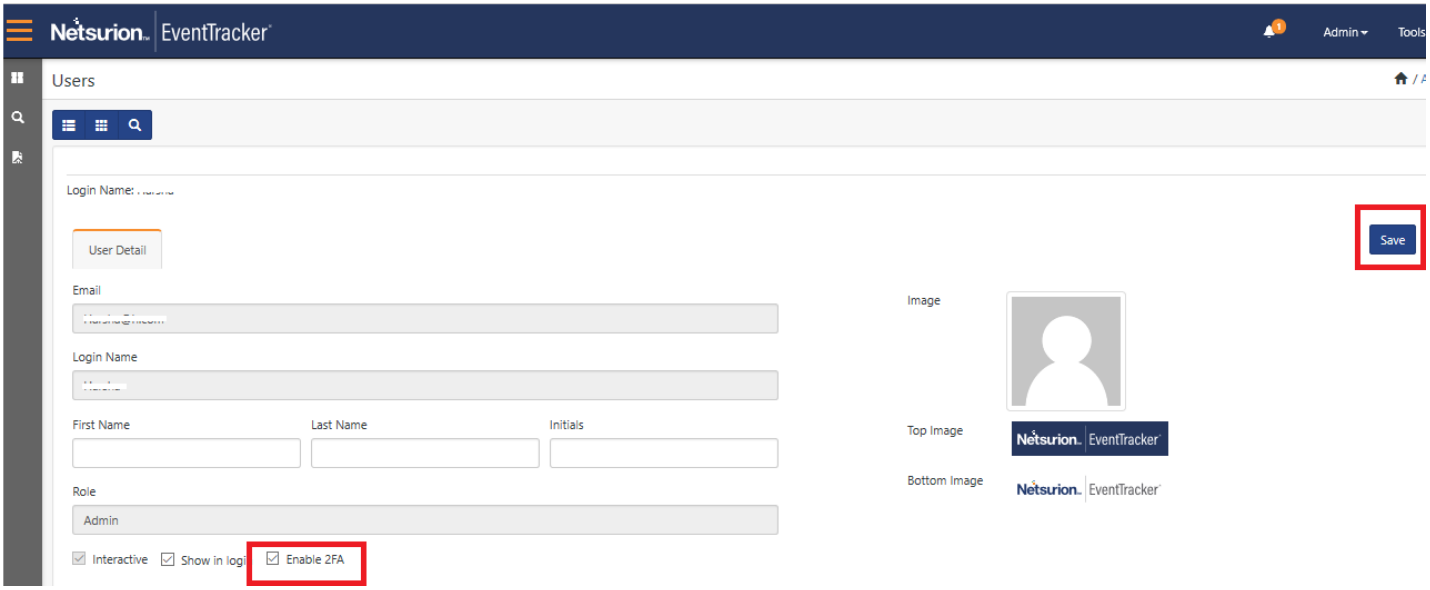

Figure 14

- Disabling 2FA will allow the user to log into EventTracker with just user name and password.

3.2 Enabling 2FA for all users using Bulk option

This feature is applicable to EventTracker Admins, MSP Admins, MMSP Admins and those who manage the Users.

1. Click Two-factor authentication drop down, choose **All** to display all the users.

Figure 15

2. Chose **Enabled**, all the Two-factor authentication enabled users are displayed.

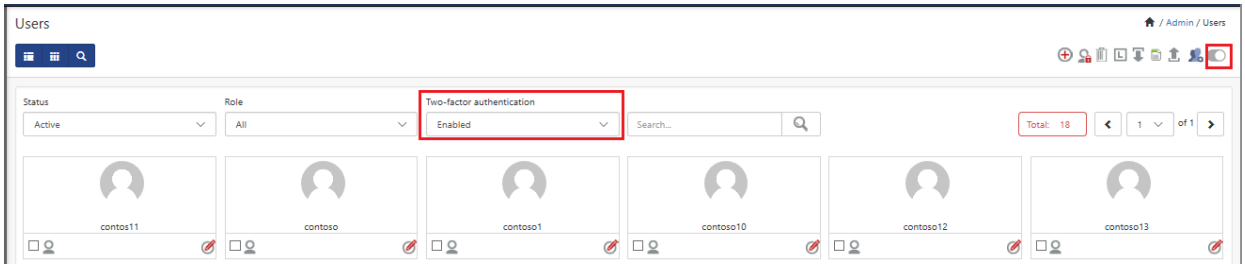

Figure 16

3. Select multiple users you want to disable 2FA, and click the icon on the right top corner.

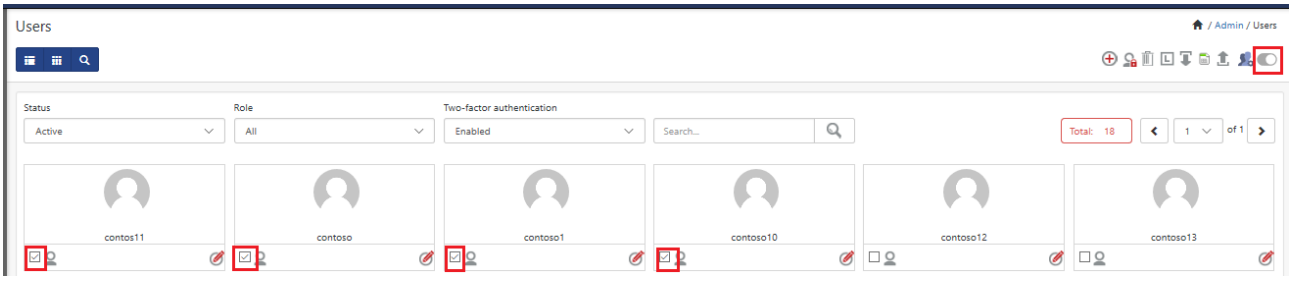

Figure 17

4. Choose **Disabled**, all the Two-factor authentication disabled users are displayed.

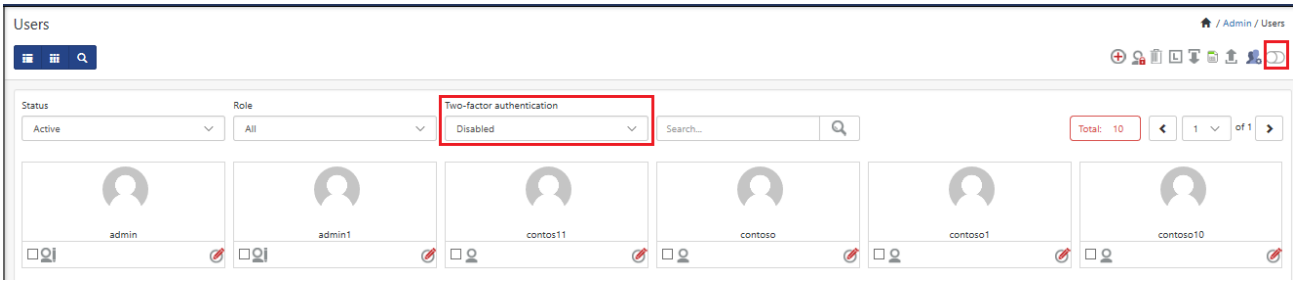

Figure 18

5. Select multiple users you want to enable 2FA on, and click the icon on the right top corner.

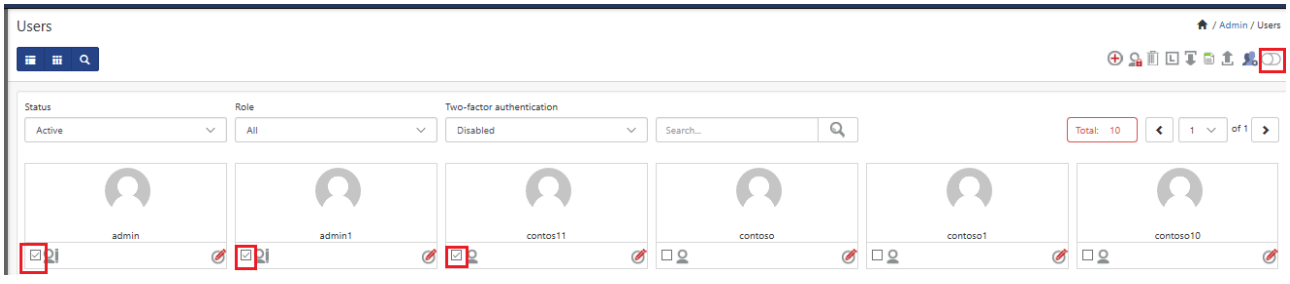

Figure 19

4. FAQ's

1. **What shall I do if I have more than one EventTracker application logins?**

   You need to configure different account in the Google Authenticator App. By default, Account Name is set to the login URL domain. However, you can choose to select your own Account Name as per your convenience.

2. **What shall I do if I accidentally delete the account configured on Google Authenticator App?**

   Please contact your EventTracker Administrator to reset the 2FA for your account. Once reset, you will be presented with 2FA configuration screen upon your login to EventTracker application.

3. **What shall I do if I lost my mobile or get a new mobile?**

   Please contact your EventTracker Administrator to reset the 2FA for your account. Once reset, you will be presented with 2FA configuration screen upon your login to EventTracker application.