MEDHOST Business Intelligence Multifactor Authentication

User Guide 7.0

Released November 2026

MEDHOST | 6550 Carothers Parkway, Suite 250 | Franklin, TN 37067
PHONE 615.761.1000 | medhost.com
© 2026 MEDHOST All rights reserved.

Table of Contents

Document Information **3**

Overview **4**

MFA Setup for BI Administrators **5**

MFA Setup for BI Users **8**

Sign in with 2FA **11**

Document Information

Audience

BI users

Purpose

This guide provides a description of multifactor authentication (MFA) setup and workflows for Business Intelligence (BI) 7.0.

Content

This guide contains the following sections:

- **Overview**: describes MFA for BI
- **MFA Setup for BI Administrators**: describes the process by which BI administrators reset MFA enrollment for individual users
- **MFA Setup for BI Users**: describes the process by which users link their BI account with their mobile device
- **Sign in with 2FA**: describes the sign-in process after users' BI accounts are linked to their mobile devices

Overview

MFA improves security by requiring the following two authenticating factors from each user for BI access:

- Authenticating factor one: the user's username and password
- Authenticating factor two: a unique MFA code provided by an authenticator app on the user's mobile device

To use MFA, users must install an authenticator app such as Google Authenticator or Microsoft Authenticator on their mobile device. When the authenticator app is installed, users must link their mobile device to their BI account as part of the first-time sign-in workflow. Once a user's mobile device and BI account are linked, the authenticator app provides an MFA code to be used as the second authenticating factor for each successive sign-in.

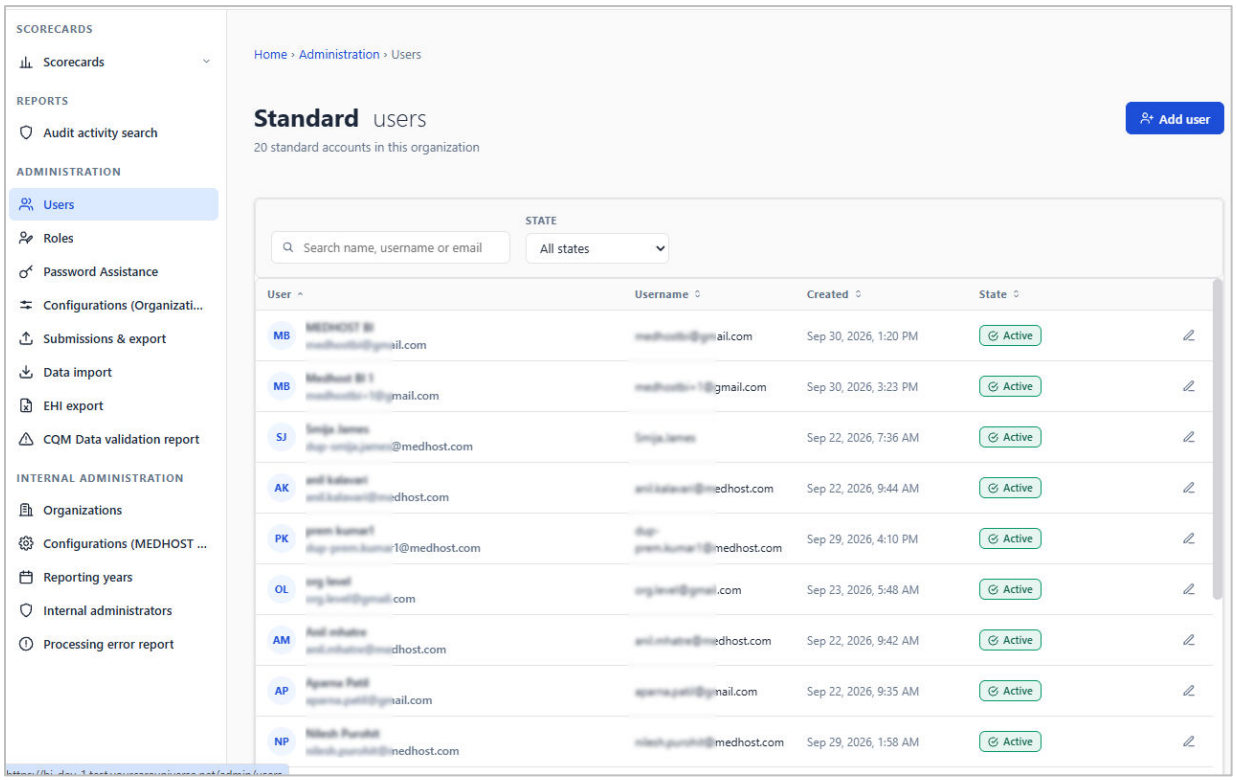
MFA Setup for BI Administrators

BI administrators can reset a user's MFA enrollment. When a user's MFA enrollment is reset, the user must link their mobile device to their BI account using a new authenticator app the next time they sign in. Their existing authenticator app recovery codes stop working immediately and they are signed out of the current session if signed in.

To reset a user's MFA enrollment

1. Click **Users** in the navigation menu

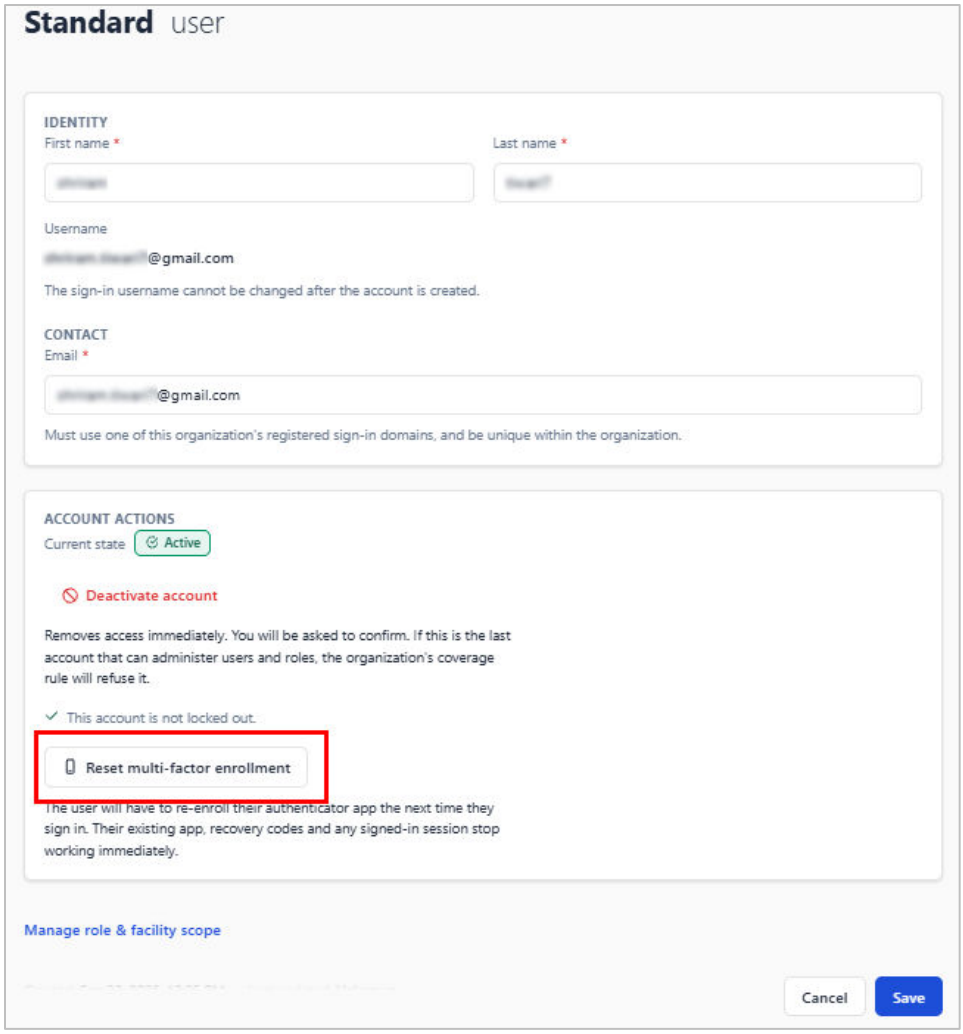
   Standard users displays.



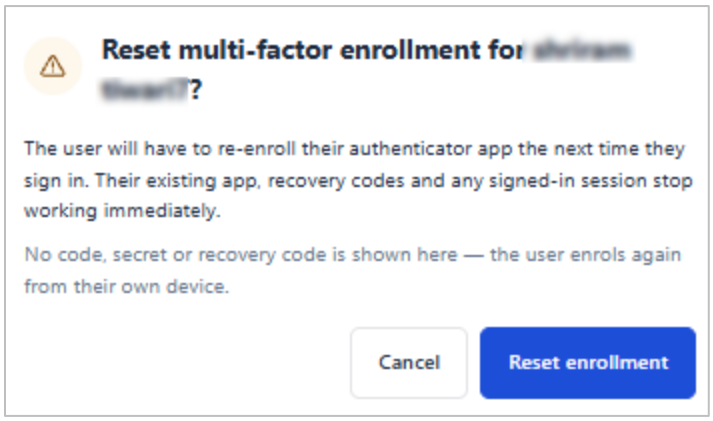
2. Click the relevant user

   The user's details display.

3. Under **Account Actions**, click **Reset multi-factor enrollment**

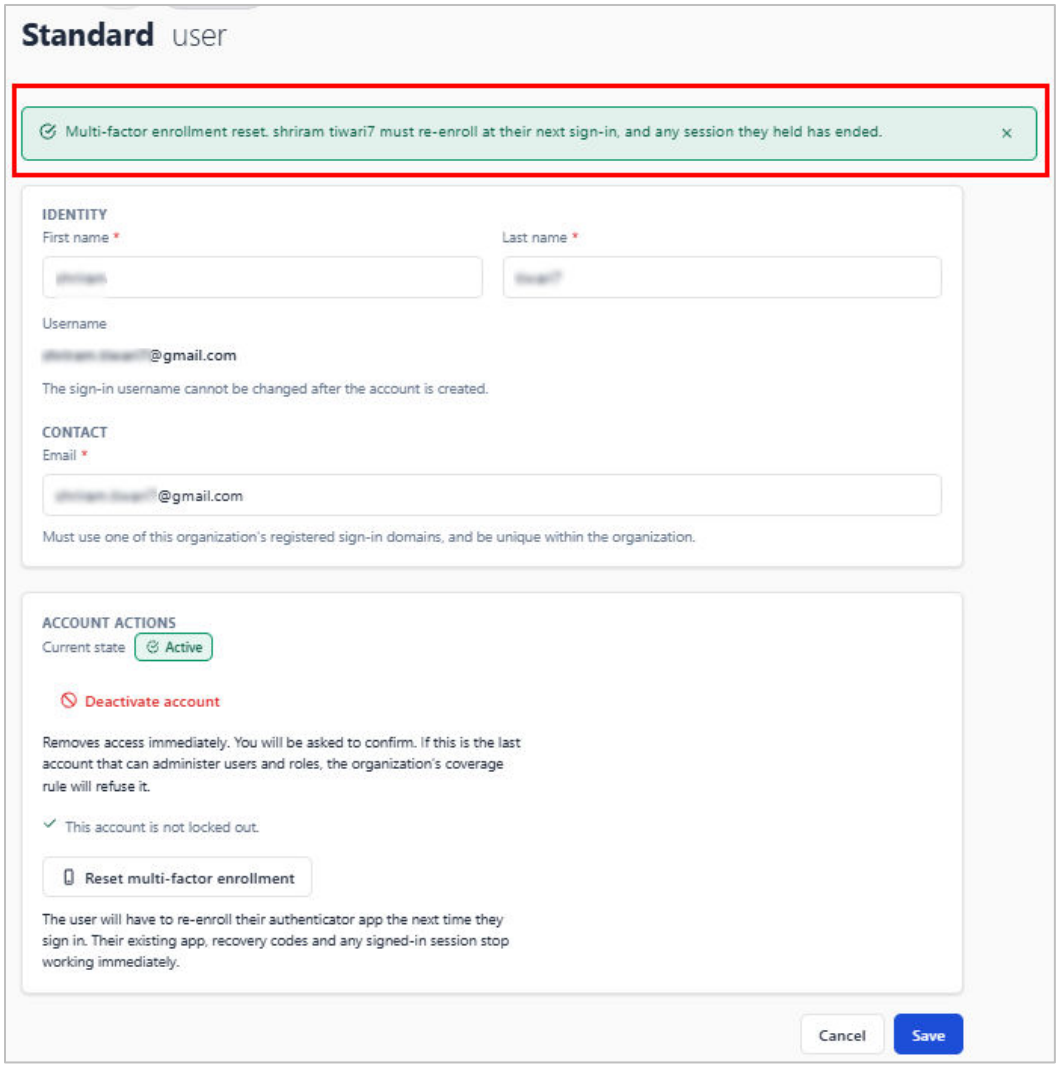


A confirmation window displays.



4. Click **Reset enrollment**

   The user details screen displays a message stating that the user must enroll again at their next sign-in and that any current session has ended.


Standard user
Multi-factor enrollment reset. shriram tiwari7 must re-enroll at their next sign-in, and any session they held has ended.
IDENTITY
First name *
Last name *
Username
@gmail.com
The sign-in username cannot be changed after the account is created.
CONTACT
Email *
@gmail.com
Must use one of this organization's registered sign-in domains, and be unique within the organization.
ACCOUNT ACTIONS
Current state
Active
Deactivate account
Removes access immediately. You will be asked to confirm. If this is the last account that can administer users and roles, the organization's coverage rule will refuse it.
This account is not locked out.
Reset multi-factor enrollment
The user will have to re-enroll their authenticator app the next time they sign in. Their existing app, recovery codes and any signed-in session stop working immediately.
Cancel
Save

MFA Setup for BI Users

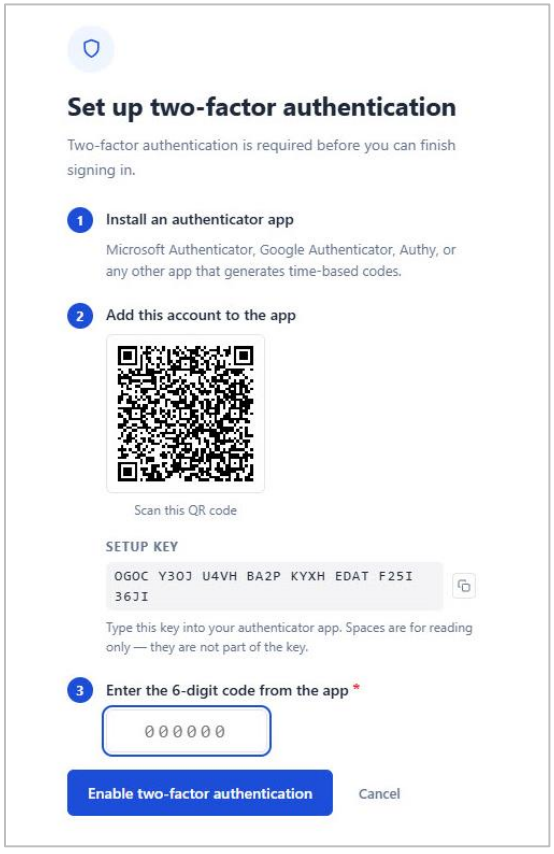
Users must install an authenticator app such as Google Authenticator or Microsoft Authenticator on their mobile device. When the authenticator app is installed, users must link their mobile device to their BI account as part of the first-time sign-in workflow after MFA enrollment.

To link your mobile device with your BI account

1. Install an authenticator app on your mobile device from Apple's App Store or Google's Android Play store
2. From the BI **Sign in** page, enter your credentials
3. Click **Sign in**

   The system sends a one-time passcode to the email address associated with your BI credentials and the **Set up two-factor authentication** page displays.
4. For **passcode**, enter the passcode from the email you received
5. Click **Validate**

   The **Set up two-factor authentication** page displays instructions for using an authenticator app to link your mobile device with your BI account.



6. Using your authenticator app, do one of the following:

   - Use a QR code:

     1) Tap **Scan a barcode**

        Your device's barcode scanner opens.

        > **NOTE**
        >
        > If the authenticator app cannot locate a barcode scanner on your mobile device, you might be prompted to download and install one. Follow your device's prompts to complete the barcode scanner installation process, then reopen your authenticator app.

     2) Scan the barcode displayed on the **Set up two-factor authentication** page

   - Use a secret key:

     1) Tap **Enter provided key**

     2) Enter the account name and secret key displayed on the **Set up two-factor authentication** page in your authenticator app

     3) Set the key to be time-based

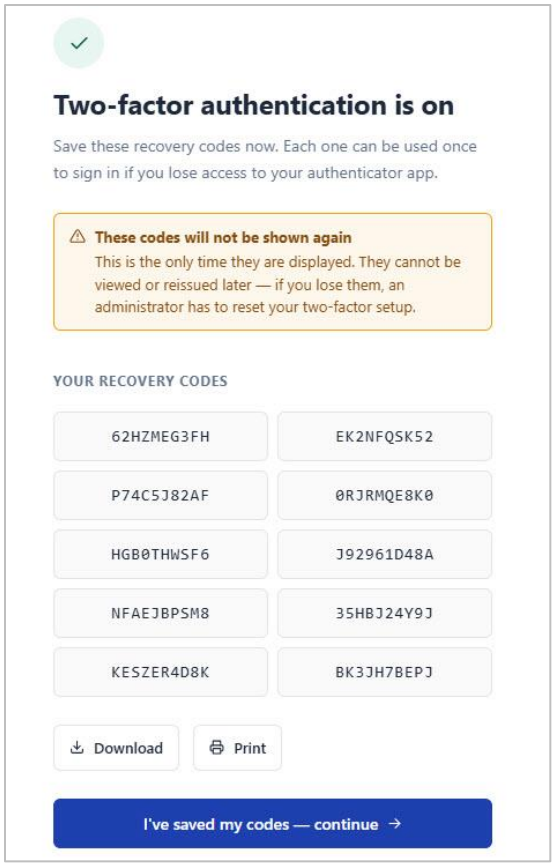
     4) Tap **Add**

   Your BI account is linked to your mobile device and displays an authentication code.

7. Enter the authentication code on the **Set up two-factor authentication** page

8. Click **Enable two-factor authentication**

   Two-factor authentication setup is complete and recovery codes display.



9. You can:
   - Click **Download** to download your recovery codes
   - Click **Print** to print your recovery codes

   Important

   Save your recovery codes somewhere secure. They will not be shown again.
10. Click **I've saved my codes - continue**

    You are signed in to BI.

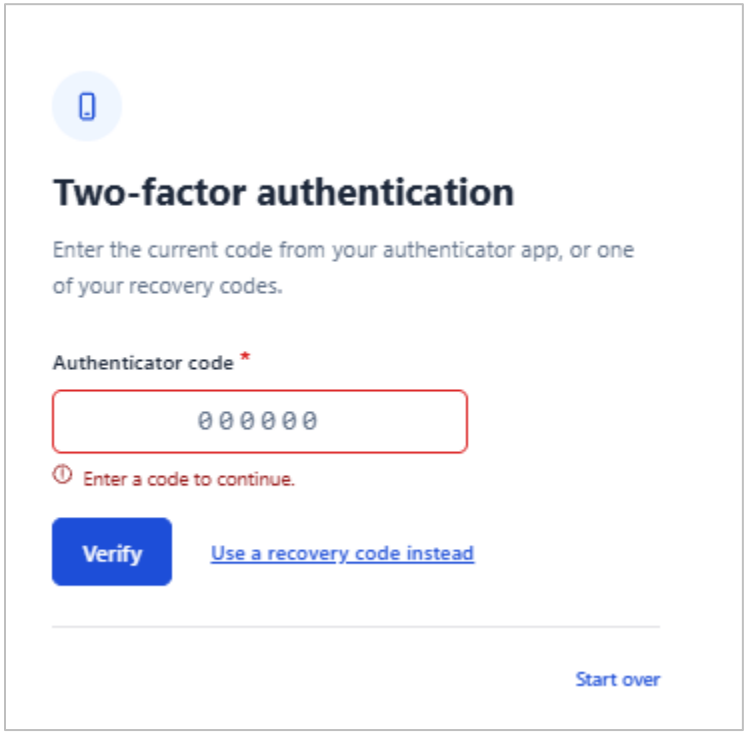
Sign in with 2FA

This section describes the two-factor authentication (2FA) sign-in process for users who have linked their BI account with their mobile device using an authenticator app.

To sign in using 2FA

1. From the BI **Sign in** screen, enter your credentials
2. Click **Sign in**

   The **Two-factor authentication** screen displays.



3. For **Authenticator code**, enter the code displayed in your authenticator app
4. Click **Verify**

   You are signed in to BI.