Table of Contents

Document Information............................................................................................................. 3
Overview .................................................................................................................................. 4
MFA Setup for BI Administrators ............................................................................................... 5
MFA Setup for BI Users ............................................................................................................. 8
MFA Login................................................................................................................................. 11
Document Information

Audience

BI users

Purpose

This guide provides a description of multifactor authentication (MFA) setup and workflows for Business Intelligence (BI) 6.0.

Content

This guide contains the following sections:

- **Overview**: describes MFA for BI
- **MFA Setup for BI Administrators**: describes the process by which BI administrators enable MFA for individual users or entire facilities
- **MFA Setup for BI Users**: describes the process by which users link their BI account with their mobile device
- **MFA Login**: describes the login process after users’ BI accounts are linked to their mobile devices
Overview

When enabled, 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

MFA can be enabled for individual BI users and globally for entire facilities. If MFA is enabled globally for a facility, all of the facility’s BI users are automatically enrolled for MFA.

**NOTE**

Only BI Internal Administrators or ORG Super Administrators can globally enable MFA for a facility’s BI users.

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 login workflow after MFA enrollment. 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 login.
MFA Setup for BI Administrators

BI administrators can set a user’s MFA enrollment status as follows:

- **Enrolled** – the user is enrolled for MFA; BI login requires two authenticating factors
- **Disenrolled** – the user is disenrolled from MFA; BI login only requires username and password
- **Reset** – the user’s MFA setup process is restarted in the event that the user’s one-time passcode is not received or that a new QR code is needed for linking the user’s BI account and authenticator app

**NOTE**
BI automatically sets a user’s MFA status to **Enrolled** after the user is reset.

To enroll a user for MFA

1. Navigate to **Scorecards > Administration > users**
2. Click the user you want to enroll for MFA
   The user’s details page displays.
3. For **mfa**, select **Enrolled**
4. Click **Save**
   The user is enrolled for MFA.
To disenroll or reset a user for MFA

1. Navigate to the user’s details page as described in steps 1-3 of To enroll a user for MFA
2. For mfa, select one of the following:
   - Disenrolled
   - Reset
3. Click Save
   The user is disenrolled or reset according to your selection.

To globally enable MFA for a facility

NOTE
This workflow can only be performed by users with the BI Internal Administrators or ORG Super Administrator role. Contact MEDHOST support for help globally enabling MFA if your facility does not have a user with the necessary permissions.

1. Navigate to Internal Administration > Organizations
2. Click the relevant organization
   The organization’s details page displays.
3. Select Edit facilities

![Configuration options for the organization’s facilities display.](image)
4. Select MFA for the relevant facility

![Facilities table]

5. Click **Save**

MFA is globally enabled for the facility’s BI users.
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 first-time login 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 Login page, enter your credentials
3. Click Login

The following occur:

- The system sends a one-time passcode code to the email address associated with your BI credentials

- The Multi-factor Authentication page displays
4. For passcode, enter the passcode from the email you received

5. Click Validate

The Multi-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 Multi-factor Authentication page
   - Use a secret key:
     1) Tap Enter provided key
     2) Enter the account name and secret key displayed on the Multi-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 the following occur:

- Your authenticator app displays an MFA code
- The **Multi-factor Authentication** page displays an **mfa code** field

7. For **mfa code**, enter the MFA code displayed by the authenticator app

8. Click **Validate**

You are logged in to BI.
MFA Login

This section describes the login process for users who are enrolled for MFA and who have linked their BI account with their mobile device using an authenticator app.

To log in using MFA

1. From the BI login page, enter your credentials
2. Click Login

   The following occur:

   • Your authenticator app displays an MFA code
   • The Multi-factor Authentication page displays an mfa code field

3. For mfa code, enter the MFA code displayed by the authenticator app
4. Click Validate

   You are logged in to BI.