Enabling Multi Factor Authentication in TE Client

Introduction 2

Initial Setup (First Login) 2

- Logging In 2
- Setting up Google Authenticator 3
- Completing the Association 4

Logging In with MFA 5

- Standard Login Flow 5
- Handling Invalid Codes 5
- Re-associating a Device 6
- Cancelling Authentication 7

Administration & Configuration 8

- Enforcing MFA per User 8
- Batch Enforcement 9
- Monitoring MFA Status 9
- Container-Level Enforcement & Inheritance 9

Introduction

This document provides a step-by-step guide on how to set up and use Multi-Factor Authentication (MFA) with the TOPSpro Enterprise (TE) Client. It also covers administrative steps for enforcing MFA policies across different user or container levels.

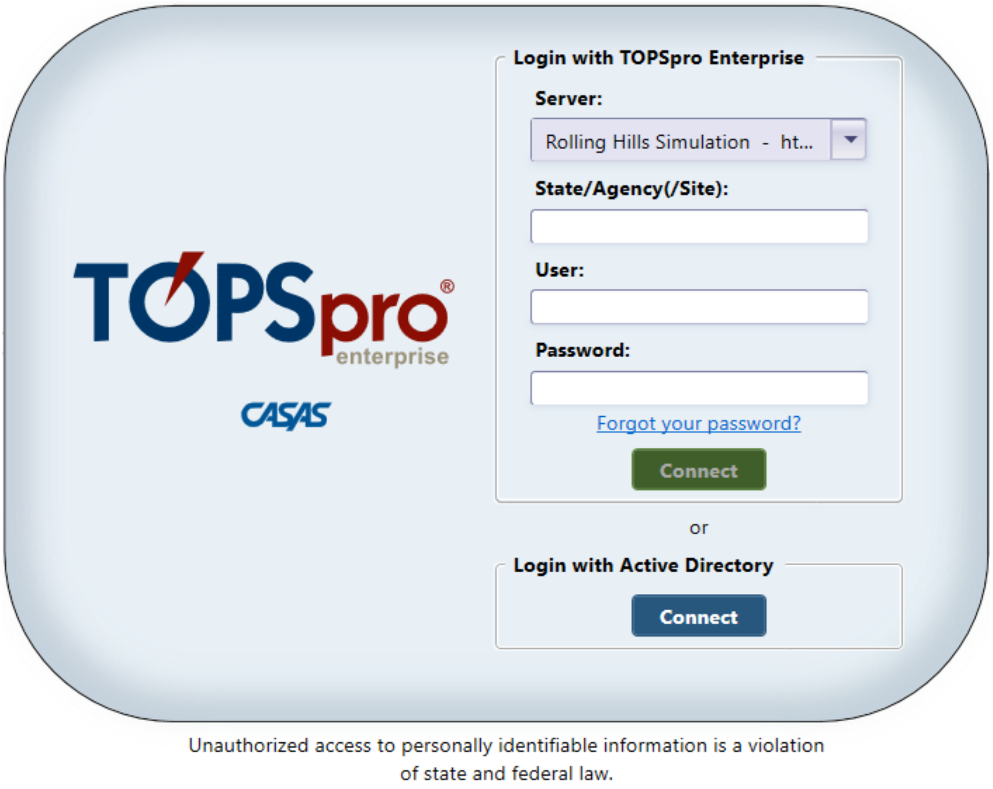
Please note that in order to use MFA, the Google Authenticator application must be installed on your device. You can find the app at this url: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2

or by searching for it in the Google Play Store.

Initial Setup (First Login)

Logging In

Start the TE Client application. The standard login screen will appear. Enter your **Server**, **State/Agency**, **User**, and **Password** credentials as usual.

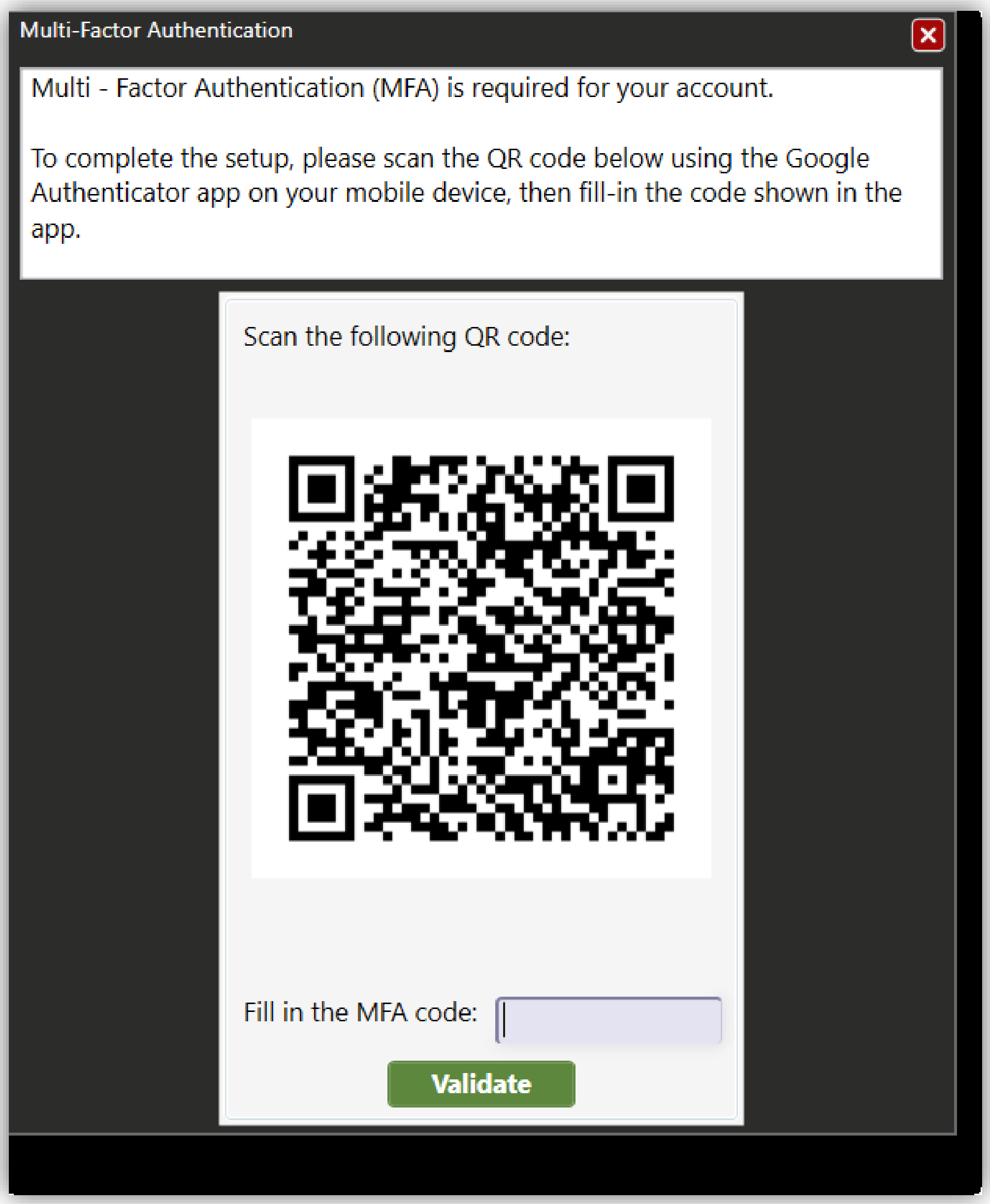


Server: Rolling Hills Simulation - ht...

Unauthorized access to personally identifiable information is a violation of state and federal law.

Setting up Google Authenticator

If MFA is enforced for your account but you have not yet set it up, the system will automatically prompt you with the MFA Setup screen after you click "Connect". You will see a QR code displayed on the screen.



Multi-Factor Authentication

Multi - Factor Authentication (MFA) is required for your account.

To complete the setup, please scan the QR code below using the Google Authenticator app on your mobile device, then fill-in the code shown in the app.

Scan the following QR code:

Fill in the MFA code:

Action Required on Mobile Device:

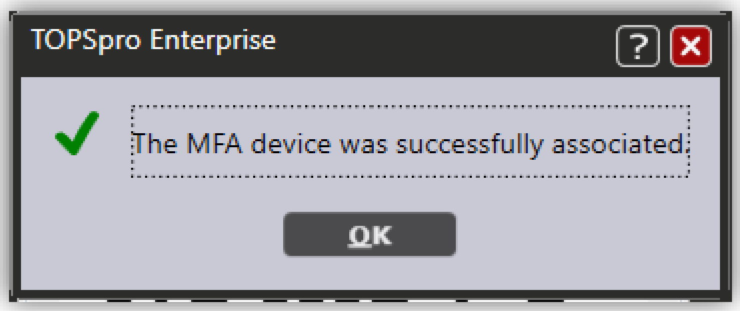
1. Open the **Google Authenticator** app on your mobile device.
2. Select the option to **Scan a QR code**.
3. Point your camera at the QR code displayed on your computer screen.
4. Once scanned, a new entry will appear in your app labeled **TE Client (Instance Name)** (e.g., *TE Client (California)*).

Note: Due to security policies, screenshots of the Google Authenticator app interface cannot be included here. Please follow the on-screen instructions within the app.

Completing the Association

Locate the 6-digit code generated by the app for the new TE Client entry. Enter this code into the **"Fill in the MFA code"** field on your computer screen and click **Validate**.

If the code is correct, you will receive a confirmation message stating that the device has been successfully associated.

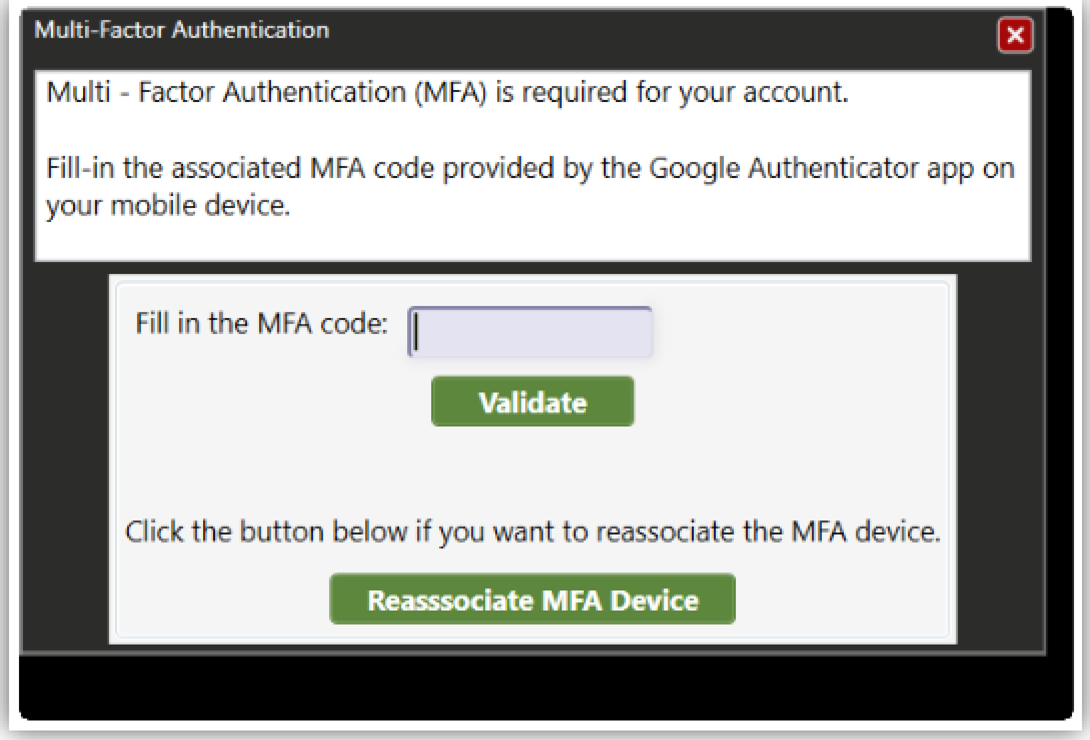


The MFA device was successfully associated.

Logging In with MFA

Standard Login Flow

For all subsequent logins, you will be prompted to enter your MFA code immediately after entering your username and password. Open your Google Authenticator app and enter the current code displayed for your TE Client instance.



Multi - Factor Authentication (MFA) is required for your account.

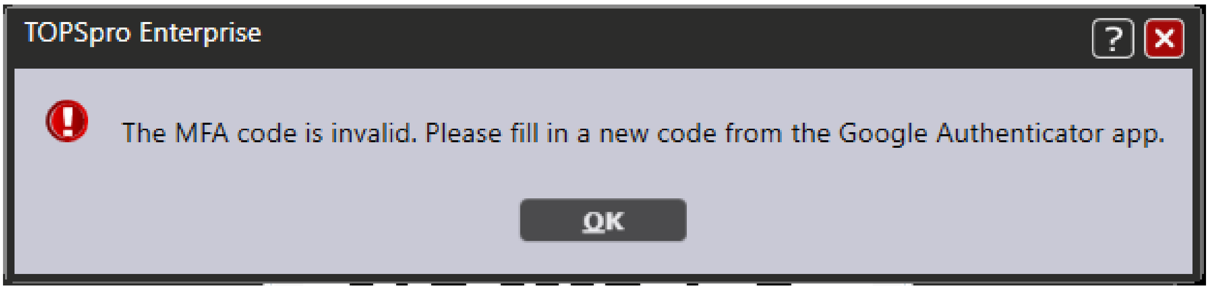
Fill-in the associated MFA code provided by the Google Authenticator app on your mobile device.

Fill in the MFA code:

Click the button below if you want to reassociate the MFA device.

Handling Invalid Codes

If you enter an incorrect or expired code, the system will display an error message. Please wait for the Google Authenticator app to generate a fresh code and try again.

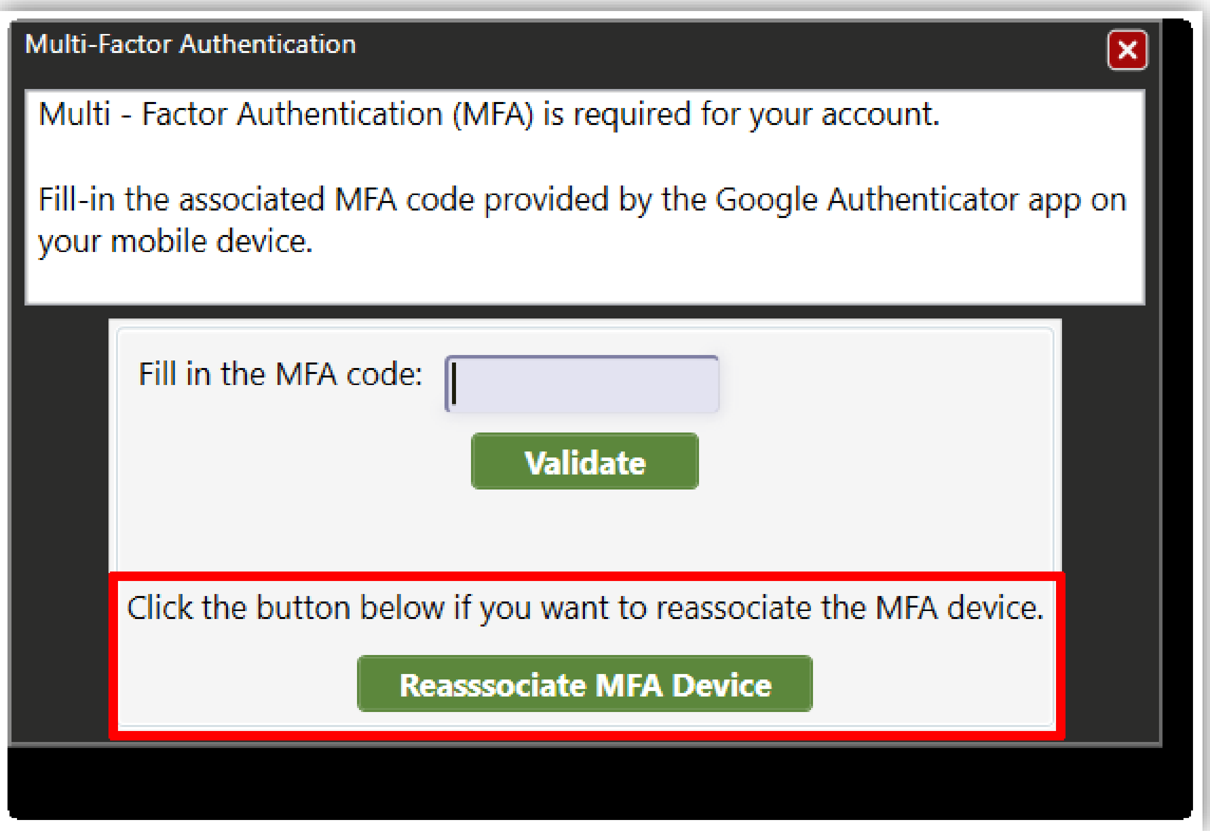


The MFA code is invalid. Please fill in a new code from the Google Authenticator app.

Re-associating a Device

If you have a new mobile device or need to reset your MFA configuration, click the **"Reassociate MFA Device"** button on the login screen.

Warning: This action will invalidate the previous association. You will be taken back to the Setup Screen (QR Code) to scan the new secret key.



Multi - Factor Authentication (MFA) is required for your account.

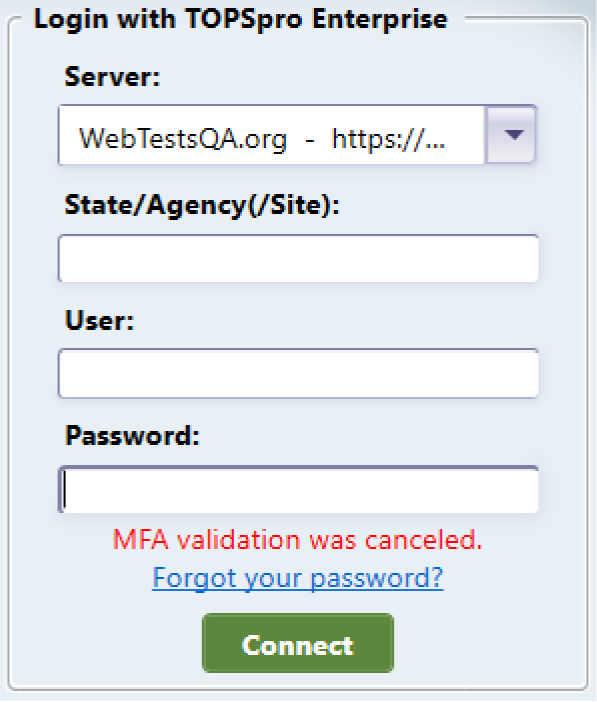
Fill-in the associated MFA code provided by the Google Authenticator app on your mobile device.

Fill in the MFA code:

Click the button below if you want to reassociate the MFA device.

Cancelling Authentication

If you choose to close the MFA window (by clicking the **X** button) without entering a code, the login process will be aborted. You will be logged off immediately and returned to the main login screen with a cancellation message.



Login with TOPSpro Enterprise

Server: WebTestsQA.org - https://...

State/Agency(/Site):

User:

Password:

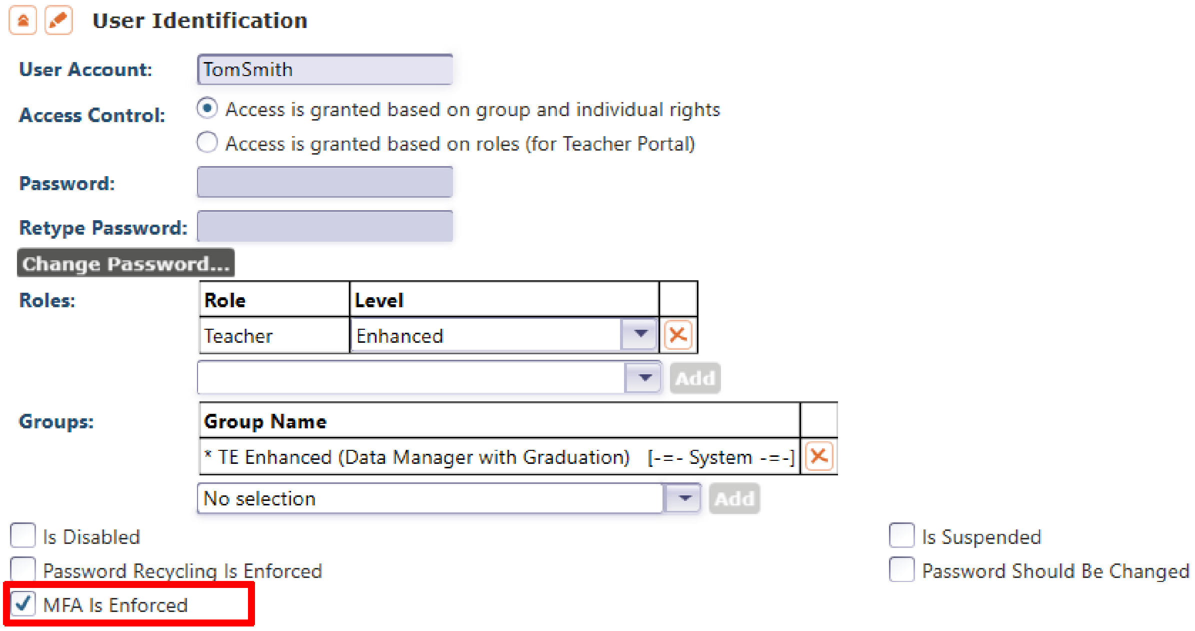
MFA validation was canceled.

Administration & Configuration

This section is intended for System Administrators

Enforcing MFA per User

MFA is automatically enforced for **System-level users**. For lower-level users (State, Consortium, Agency, or Site), it can be enabled on an individual basis. To do this, navigate to the **User Information** edit page and check the box labeled **MFA Is Enforced**.



User Identification

User Account: TomSmith

Access Control:
● Access is granted based on group and individual rights
○ Access is granted based on roles (for Teacher Portal)

Password:

Retype Password:

Roles:

Role	Level
Teacher	Enhanced

Groups:

Group Name
* TE Enhanced (Data Manager with Graduation) [-=- System -=-]

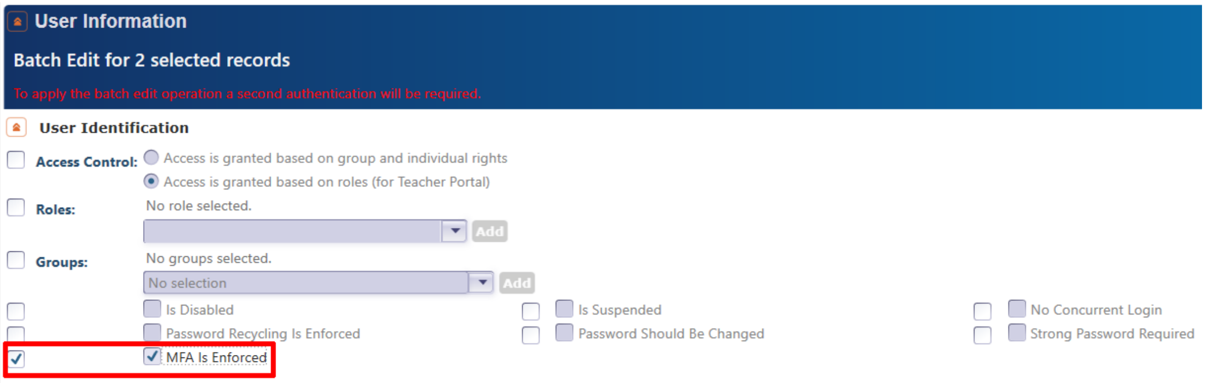
No selection

□ Is Disabled
□ Password Recycling Is Enforced
☑ MFA Is Enforced

□ Is Suspended
□ Password Should Be Changed

Batch Enforcement

To enable or disable MFA for multiple users simultaneously, use the **Batch Edit** feature. Select the desired user accounts in the User Lister, right-click to Batch Edit, and change the **MFA Is Enforced** setting.



User Information

Batch Edit for 2 selected records

To apply the batch edit operation a second authentication will be required.

User Identification

□ Access Control: ○ Access is granted based on group and individual rights
● Access is granted based on roles (for Teacher Portal)

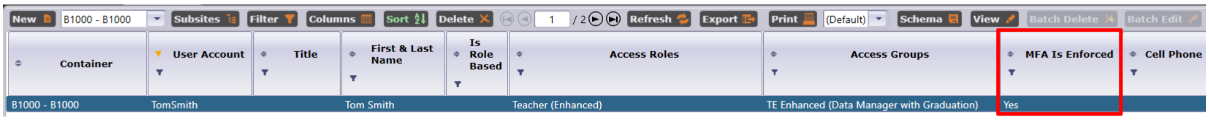
□ Roles: No role selected.

□ Groups: No groups selected.
No selection

□ □ Is Disabled
□ □ Password Recycling Is Enforced
☑ ☑ MFA Is Enforced
□ □ Is Suspended
□ □ Password Should Be Changed
□ □ No Concurrent Login
□ □ Strong Password Required

Monitoring MFA Status

Administrators can quickly verify which users have MFA enabled by checking the **MFA Is Enforced** column in the User Lister grid.



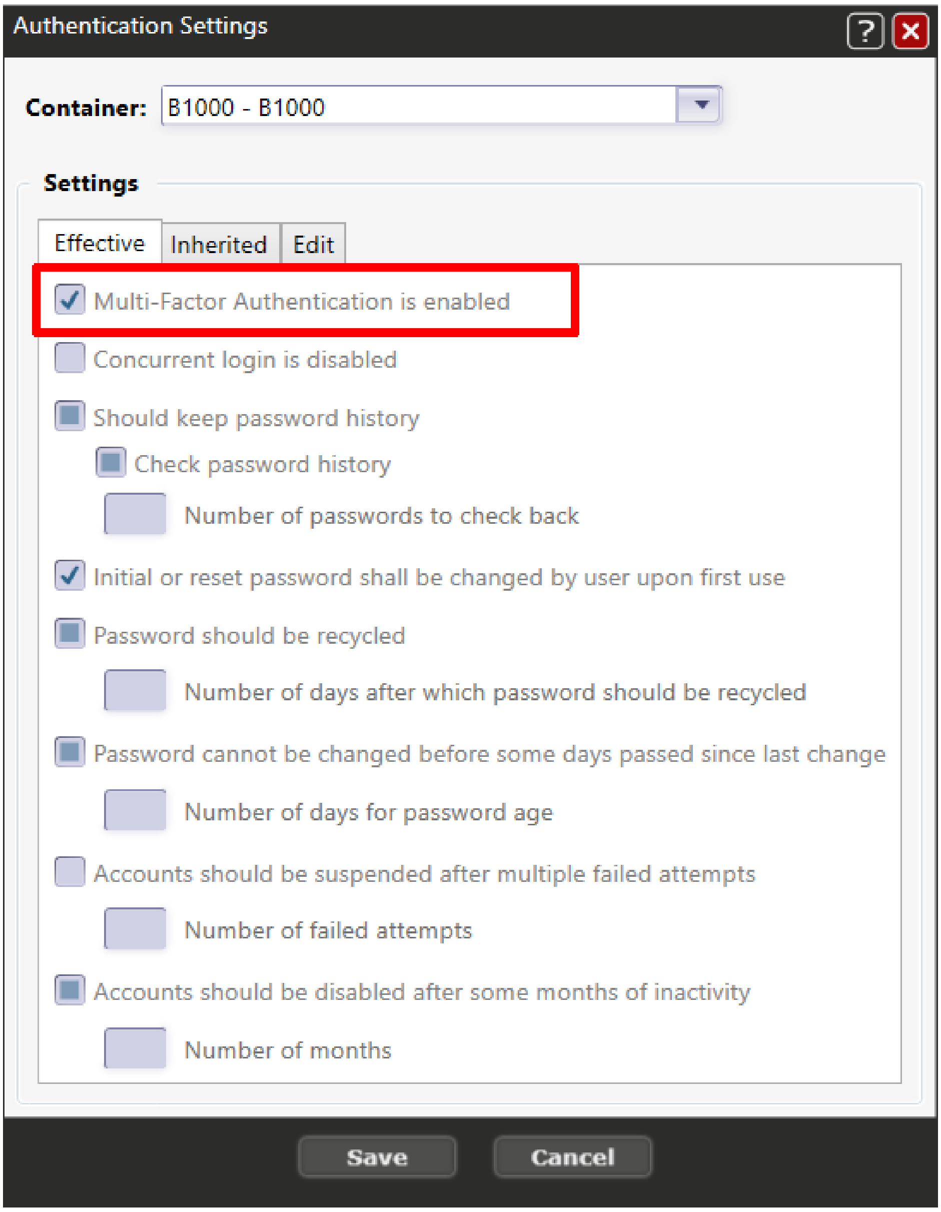
Container	User Account	Title	First & Last Name	Is Role Based	Access Roles	Access Groups	MFA Is Enforced	Cell Phone
B1000 - B1000	TomSmith		Tom Smith		Teacher (Enhanced)	TE Enhanced (Data Manager with Graduation)	Yes	

Container-Level Enforcement & Inheritance

MFA can be enforced globally for an entire data container (e.g., an entire Agency or Consortium) via the **Authentication Settings**.

Important Inheritance Rule: Selection at a higher container level **supersedes** selection at lower levels.

- *Example:* If a Consortium enforces MFA, all Agencies within that Consortium are forced to use it. They cannot "opt-out" individually.



Authentication Settings

Container: B1000 - B1000

Settings

☑ Multi-Factor Authentication is enabled

□ Concurrent login is disabled

■ Should keep password history

■ Check password history

□ Number of passwords to check back

☑ Initial or reset password shall be changed by user upon first use

■ Password should be recycled

□ Number of days after which password should be recycled

■ Password cannot be changed before some days passed since last change

□ Number of days for password age

□ Accounts should be suspended after multiple failed attempts

□ Number of failed attempts

■ Accounts should be disabled after some months of inactivity

□ Number of months

Note for **multiple accounts** on the **Same Instance:** If a user manages multiple accounts within the *same* TE instance (e.g., a Consortium Manager with individual accounts for different agencies), the entries in Google Authenticator may appear with identical labels. Users in this situation should be careful to identify which code corresponds to which account, or consider using different devices/apps if possible to avoid confusion.