

What?

A security process requiring two or more different ways to prove your identity (e.g., password + fingerprint, password + text code) before granting access to an app or website.

Why?

it creates a layered defense, dramatically increasing the difficulty for unauthorized users to gain access.

How?

Entering a One-Time Password (OTP) generated by an authenticator app such as **Google Authenticator**.



How?



1



password



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

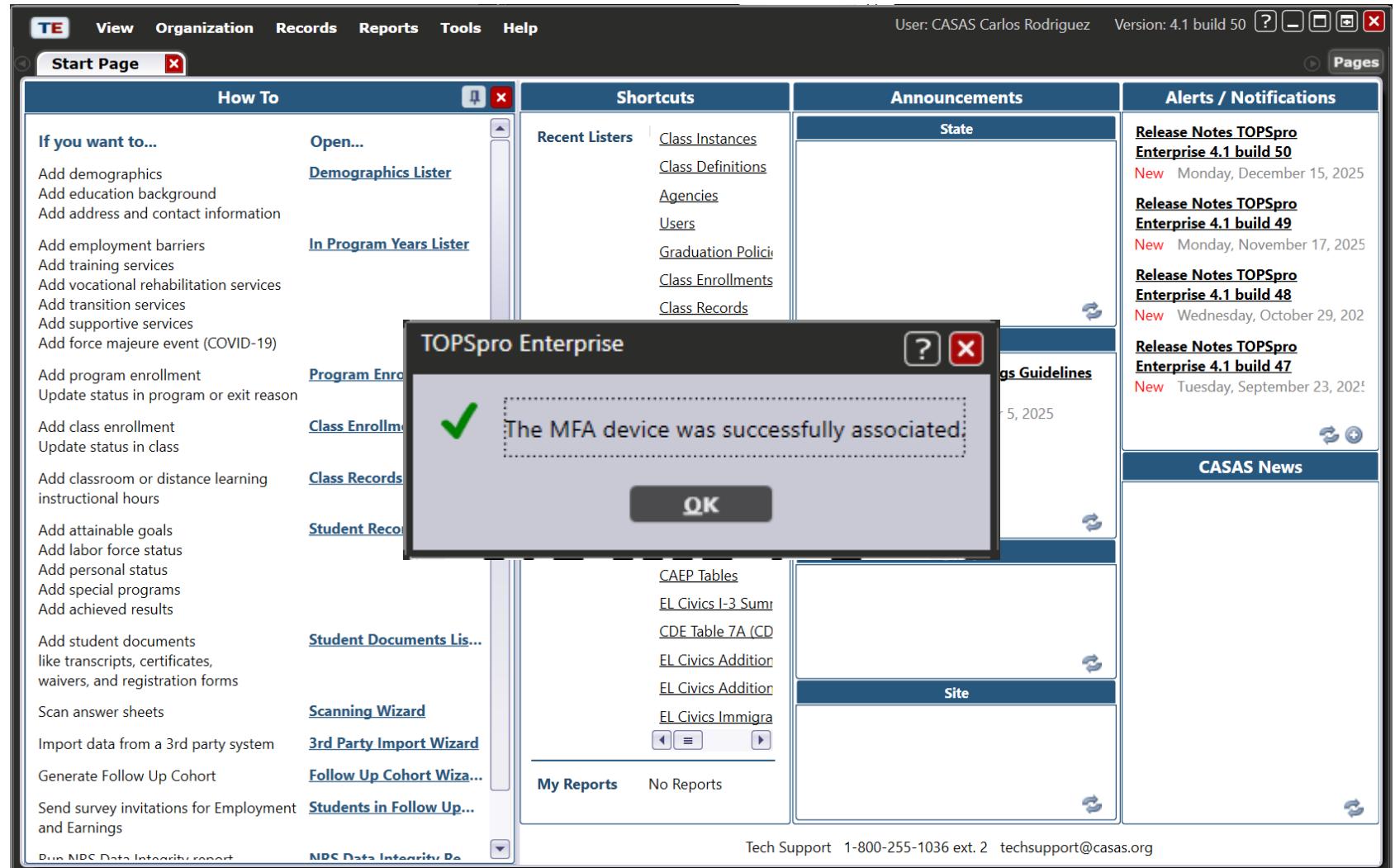
2



3



access granted



The screenshot shows the TOPSpro Enterprise software interface. At the top, there is a menu bar with 'TE', 'View', 'Organization', 'Records', 'Reports', 'Tools', and 'Help'. The top right corner displays 'User: CASAS Carlos Rodriguez' and 'Version: 4.1 build 50'. A 'Pages' button is also present. The main window is titled 'Start Page'. It features several sections: 'How To' (with a list of tasks like 'Add demographics', 'Add education background', etc.), 'Shortcuts' (listing 'Recent Listers', 'Class Instances', 'Class Definitions', etc.), 'Announcements' (listing 'State', 'Program Enrollment Guidelines', etc.), and 'Alerts / Notifications' (listing 'Release Notes TOPSpro Enterprise 4.1 build 50', 'Release Notes TOPSpro Enterprise 4.1 build 49', etc.). A central modal window titled 'TOPSpro Enterprise' displays a green checkmark and the message 'The MFA device was successfully associated.' with an 'OK' button. At the bottom, there are links for 'CAEP Tables', 'EL Civics I-3 Summative', 'CDE Table 7A (CD)', 'EL Civics Addition', 'EL Civics Addition', 'EL Civics Immigration', 'Site', and 'My Reports' (No Reports). The bottom right corner includes 'Tech Support' information: '1-800-255-1036 ext. 2' and 'techsupport@casas.org'. A small note at the bottom left says 'Run NDC Data Integrity report'.

2



Multi-Factor Authentication

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.

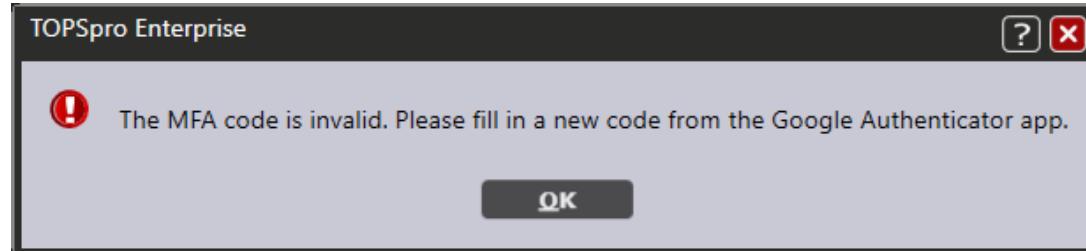
Fill in the MFA code:

Validate

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

Reasssociate MFA Device

2



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.

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

Reassociate MFA Device

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

1



User Identification

User Account:

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

Password:

Retype Password:

[Change Password...](#)

Roles:

Role	Level	
Teacher	Enhanced	<input type="button" value="X"/>
		<input type="button" value="Add"/>

Groups:

Group Name	
* TE Enhanced (Data Manager with Graduation) [--- System ---]	<input type="button" value="X"/>
No selection	<input type="button" value="Add"/>

Is Disabled

Password Recycling Is Enforced

MFA Is Enforced

Is Suspended

Password Should Be Changed

TE Authentication Settings

1



Authentication Settings

Container: B1000 - B1000

Settings

Effective Inherited Edit

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

Save Cancel