CapLEARN Security Policies

CapLEARN is implementing new security rules to comply with Department of Health and Human Services policies that protect user data. CapLEARN will require all users to utilize Two Factor Authentication (TFA) to access CapLEARN. Additionally, there are new password requirements and limitations on sessions (e.g., how long you leave your computer unattended/inactive while logged into CapLEARN). This document describes TFA, provides direction on setting up TFA for CapLEARN, provides the rules for CapLEARN passwords and session limitations.

TFA on CapLEARN

To comply with Department of Health and Human Services policies, starting 15 September 2022, CapLEARN will require all users to login using Two Factor Authentication (TFA) to log into user accounts. This is part of CapLEARN's increased security protocols to protect user data. You may be familiar with TFA as most online financial and banking systems apply TFA security to protect sensitive user data.

What is Two Factor Authentication?

Two factor authentication is a security process that requires users to verify their identity through two factors:

1. Entering a login name and password
2. Entering a credential only they can have possession, such as a time-sensitive code provided to users' mobile device.

There are several authentication tools available for CapLEARN users' mobile devices. Using any of these tools will ensure you can provide the necessary two methods of authentication.

You will also have access to a series of Recovery Codes, generated during your TFA setup that you can save and use to verify your identity if other methods are unavailable.

CapLEARN Security Policies

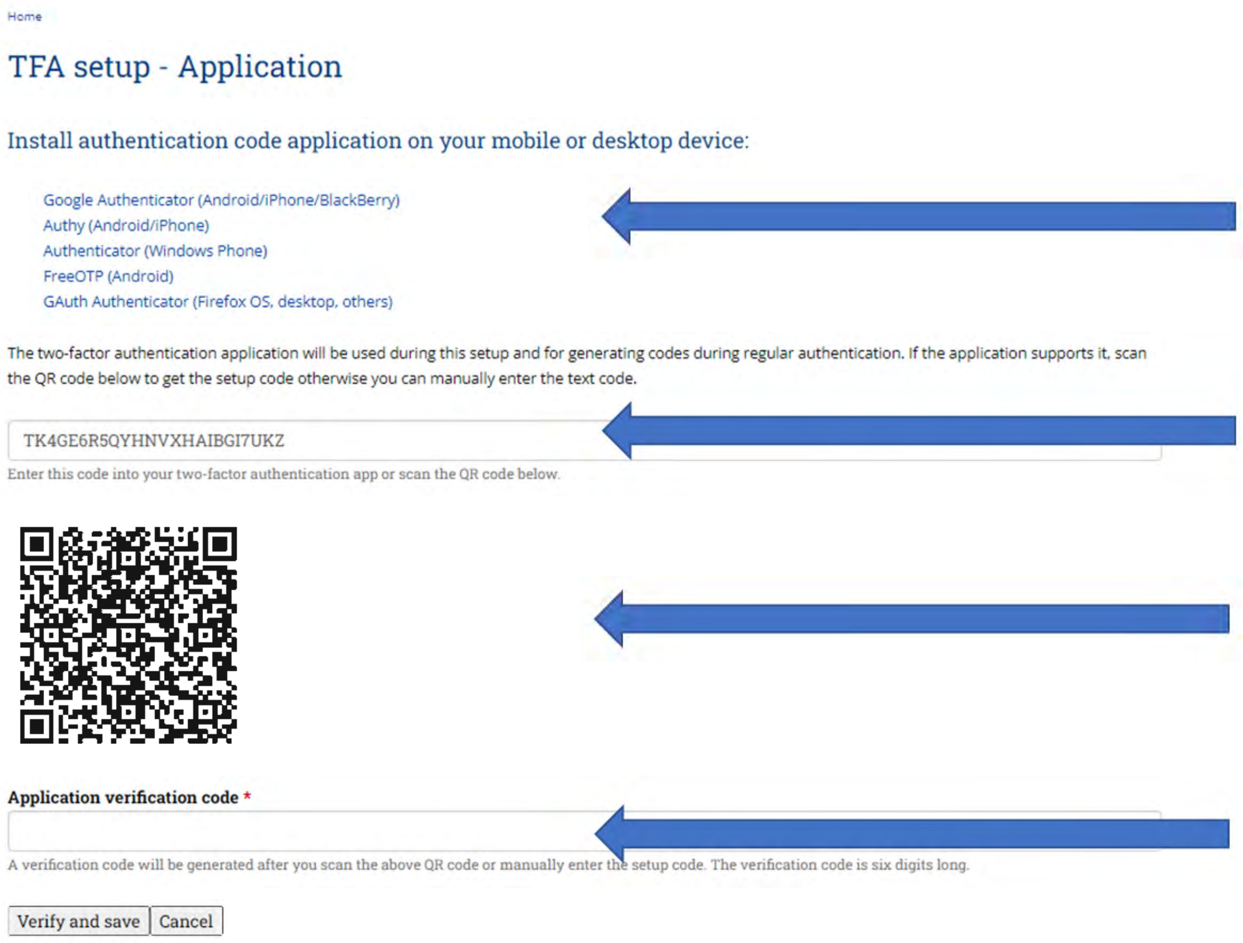
How to Set Up TFA for CapLEARN?

The first time you log into CapLEARN after 15 September 2022, you will be prompted and guided to set up the TFA verification application (see below). You can choose from the following authenticator applications to generate the TFA codes needed to successfully log into CapLEARN:

- Google Authenticator (Android/iPhone/BlackBerry)
- Authy (Android/iPhone)
- Authenticator (Windows Phone)
- FreeOTP (Android)
- GAuth Authenticator (Firefox OS, desktop, others)

Install the authenticator app of your choice and then scan the provided QR code or manually enter the text code into the TFA app. The verification app will generate a 6-digit TFA verification code.

The images below represent an example of screen shots, instructions, and QR codes users may experience in setting up TFA for CapLEARN.



Home

TFA setup - Application

Install authentication code application on your mobile or desktop device:

- Google Authenticator (Android/iPhone/BlackBerry)
- Authy (Android/iPhone)
- Authenticator (Windows Phone)
- FreeOTP (Android)
- GAuth Authenticator (Firefox OS, desktop, others)

The two-factor authentication application will be used during this setup and for generating codes during regular authentication. If the application supports it, scan the QR code below to get the setup code otherwise you can manually enter the text code.

TK4GE6R5QYHNVXHAIBGI7UKZ

Enter this code into your two-factor authentication app or scan the QR code below.

Application verification code *

A verification code will be generated after you scan the above QR code or manually enter the setup code. The verification code is six digits long.

Step 1 – Install one of these TFA authenticator apps.

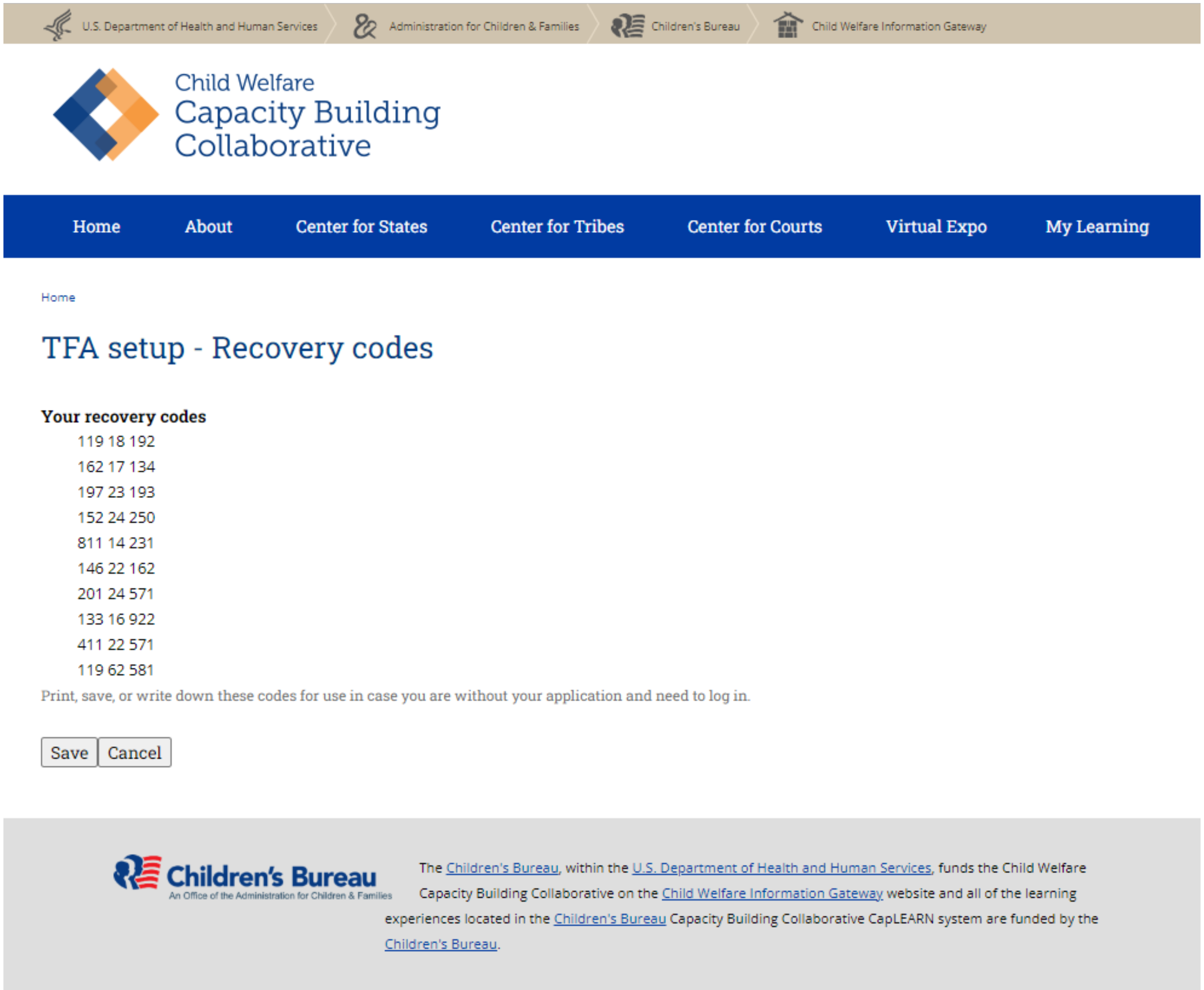
Step 2a – Type this code in the TFA app downloaded as part of Step 1

Step 2b – Alternatively, scan this QR code into the app downloaded as part of Step 1.

Step 3 – Enter the six-digit verification code generated by the app into this field and then click "Verify and Save"

The final step in the TFA setup is the generation of recovery codes to be used if other methods of verification are not available. Follow the system prompts to generate, print or save (recommended) these codes.

CapLEARN Security Policies


U.S. Department of Health and Human Services
Administration for Children & Families
Children's Bureau
Child Welfare Information Gateway
Child Welfare Capacity Building Collaborative
Home
About
Center for States
Center for Tribes
Center for Courts
Virtual Expo
My Learning
Home

TFA setup - Recovery codes

Your recovery codes

119 18 192
162 17 134
197 23 193
152 24 250
811 14 231
146 22 162
201 24 571
133 16 922
411 22 571
119 62 581

Print, save, or write down these codes for use in case you are without your application and need to log in.

Save
Cancel
Children's Bureau
An Office of the Administration for Children & Families

The Children's Bureau, within the U.S. Department of Health and Human Services, funds the Child Welfare Capacity Building Collaborative on the Child Welfare Information Gateway website and all of the learning experiences located in the Children's Bureau Capacity Building Collaborative CapLEARN system are funded by the Children's Bureau.

CapLEARN Security Policies

How to Log into CapLEARN with TFA?

The login process has not changed significantly.

1. You will be presented with the same login screen requesting email address and password.
2. You will be prompted to enter the six-digit time-sensitive verification code generated by the application on your mobile device.

What if I need Technical Support?

If you require support for this new change, there are two ways you can connect with CapLEARN technical support:

- Go to CapLEARN Help | Capacity Building Collaborative Learning Management System (childwelfare.gov)
- Email caplearn@gjhildwelfare.gov and providing as much technical information that is available, such as OS version, browser in use, etc.

Thank you so much for your patience as we increase the protection and security of your and all CapLEARN users' data.

CapLEARN Security Policies

Password Rules

User passwords are governed by rules regarding lifespan, reuse, and complexity as follows.

- Password Lifespan and Reuse
    a. Passwords expire and must be changed at least every 60 days (IA-05(01))
    b. At least 50% of total password content must be changed when a new password is created
    c. Passwords may not be reused for 24 generations
- Password Length – at least 8 characters
- Password Complexity – Passwords must comply with the following complexity rules (IA-05(01))
    a. User passwords must contain characters from each of the following four categories:
        i. Uppercase letters (e.g., A, B, C, Y, Z, etc.)
        ii. Lowercase letters (e.g., a, b, c, y, z, etc.)
        iii. Special characters (e.g., ! @, #, $, %, ^, &, etc.)
        iv. Numbers (e.g., 1, 2, 3, 4, 5, etc.)
    b. Passwords may not contain any of the following:
        i. Dictionary words (e.g., computer, work) or common names (e.g., Betty, Fred, Rover).
        ii. Portions of associated account names (e.g., user ID, login name)
        iii. Consecutive character strings (e.g., abcdef, 12345)
        iv. Simple keyboard patterns (e.g., QWERTY, asdfgh)
        v. Generic passwords (i.e., password consisting of a variation of the word “password” [e.g., P@ssw0rd1])]

CapLEARN Security Policies

Session Rules

The time between when a user properly authenticates and logs into CapLEARN and the time they log out is a “session”. The following rules apply to user sessions in CapLEARN.

- Users are limited to one (1) session. Attempts to create another session (i.e., log in) on CapLEARN from another browser or browser tab will automatically be prevented by the system. This means users cannot be logged onto CapLEARN from multiple computers or browsers at the same time.
- User sessions will automatically be locked after 15 minutes of inactivity. Users may unlock their session by following the on-screen instructions to re-enter their username and password.
- Sessions will be automatically terminated after 30 minutes of inactivity. Current user activity will be lost when the session is terminated unless saved before the session terminates.