What is MFA?

Multi-Factor Authentication (MFA) is a security feature that requires a user to validate their identity using something you know (user name and password) and something you have (your phone) to access a computer system/resource. Effective October 26, 2017, the CPUC will be implementing MFA to access the Virtual Private Network (VPN) and Virtual Desktop Infrastructure (VDI) systems.

Why do we need MFA?

MFA is a State Information Security Office requirement for remote access. The CPUC is implementing MFA as an added layer of security to prevent unauthorized access to our computing environment. This guide will help you complete the MFA registration process. Once your registration is complete, your selected MFA authentication method will be applied after you enter your user name and password each time you access VPN or VDI.

What if I have additional questions about MFA?

Questions about MFA can be directed to the IT Service Desk by filing a Service Desk Request from the CPUC intranet at: http://itservicedesk/. If you are unable to access the intranet, you can call (415) 703-1767 or email: itservicedesk@cpuc.ca.gov.

How to access MFA:

1. Open a web browser (Internet Explorer, Mozilla Firefox, etc.) and type the following address in the Address Bar of your browser.

   https://mfa.cpuc.ca.gov

2. On the **Multi-Factor Authentication User Log In** page, enter your 3-character ID and network password in the respective boxes and click on the **Log In** button.

- *Note – For the Username, you must use your 3-character ID. Using your firstname.lastname ID will display an error.*

3. On the **Multi-Factor Authentication User Setup** page, under **Method,** you can click on the drop-down box and choose 1 of the 3 ways in which to register your second authentication method. **Please note that standard call, text message or data charges may apply depending on your service plan.**

   a. **Text Message** – You will receive a text message to the supplied phone number with a one-time passcode that you will need to enter when prompted by VPN or VDI. **This is the preferred method recommended by your CPUC IT Service Desk.**

   b. **Phone Call** – You will receive a phone call to the supplied phone number asking you to press the pound (#) key to confirm your sign on.

   c. **Mobile App** – You must download and install an application to your device (Microsoft Authenticator). Once complete, after entering your user name and password, you will receive a notification from the Microsoft Authenticator application and then press the "approve" button to confirm your sign on. An Apple ID or Gmail account will be required to download this app.

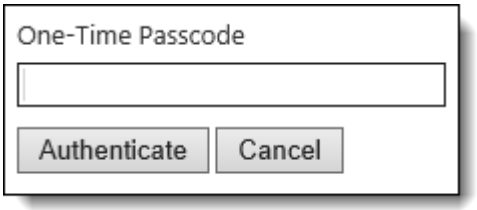
Method 1: Text Message

1. If you choose to authenticate using Text Message, you will need to enter a phone number that can receive text messages in the box next to the country code under **Phone Number. Please note that standard text message charges may apply depending on your service plan.**

2. Click on **Text Me Now to Authenticate.**

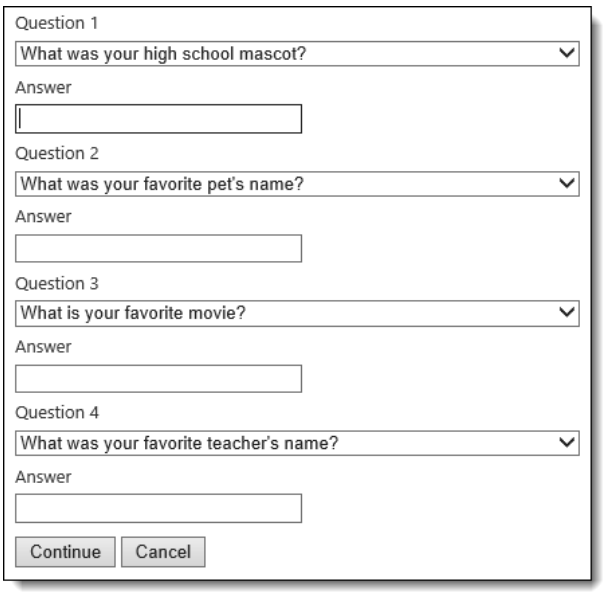
3. You will receive a text message that says **"XXXXXX Use this code for User Portal verification"** (XXXXX will be a random six-digit code).

4. Going back to your computer, your browser will take you to the **One-Time passcode** page where you will enter the random six-digit code you received from the text message in the box under **One-Time Passcode.**



5. Click on the **Authenticate** button.

6. You will then be redirected to the Security Questions page in which you will need to select 4 different security questions and specify answers to each question.

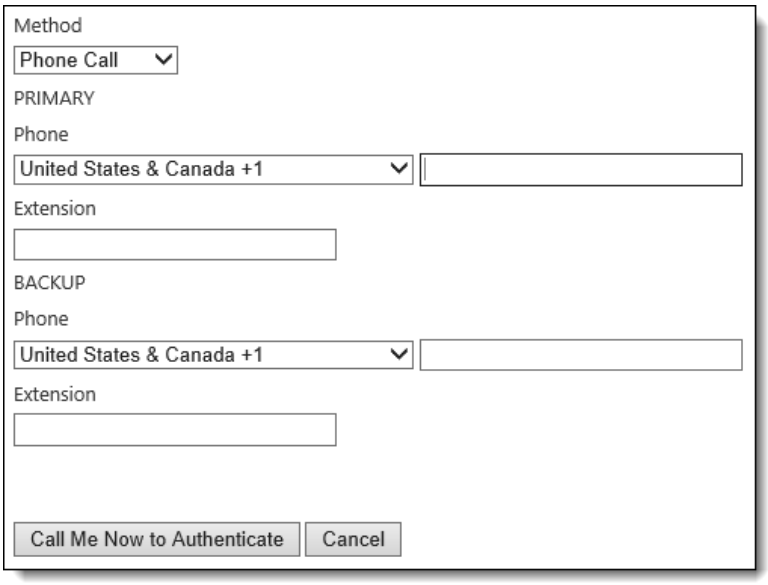


- *Note: You must select 4 different security questions. If you select a duplicate security questions, you will get an error message that says, "Duplicate question not allowed".*

7. After successfully selecting your security questions, click on **Continue** to complete the MFA process.

Method 2: Phone Call

1. If you choose to authenticate using a phone call, you will need to enter a phone number where you can be reached in the box under **PRIMARY Phone**, next to the country code. If you have an extension, you can enter that in the box under **Extension**. You may also enter a different phone number under **BACKUP Phone** to register an alternative phone number should the primary phone number become unreachable. **Please note that standard call charges may apply depending on your service plan.**



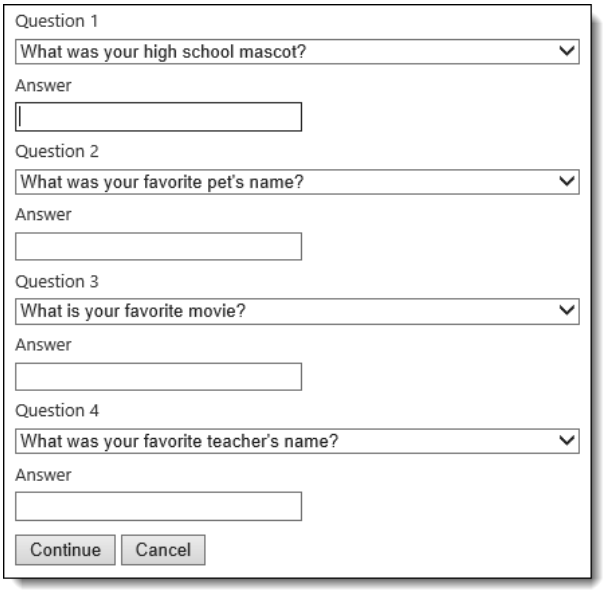
2. Click on the **Call Me Now to Authenticate** button.

3. You will receive a phone call on your PRIMARY Phone number.

4. An automated system will say: **"Thank you for using the Microsoft sign in verification system. Please press the # key to finish your verification."** After pressing the # key, you will hear the system say: **"Your sign in was successfully verified".** You can now end the call.

    - *Note - If you **do not** answer the call, the automated system will leave a voicemail message stating "Cannot finish your verification, I'm sorry. Please try again later."*

5. Going back to your computer, your browser will redirect you to the Security Questions page in which you will need to select 4 different security questions and specify answers to each question.



- *Note: You must select 4 different security questions. If you select a duplicate security questions, you will get an error message that says, "Duplicate question not allowed".*

6. After successfully selecting your security questions, click on **Continue** to complete the MFA process.

Method 3: Mobile App

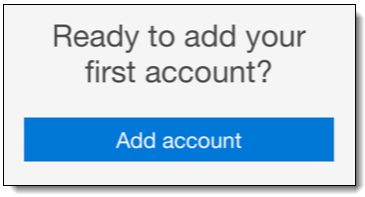
1. If you choose to authenticate using Mobile App, you will be instructed to install the free **Microsoft Authenticator** app. If you are using an iOS device such as an Apple iPhone or Apple iPad, you will need to download the app from the Apple App Store. If you are using an Android-based device such as a Samsung Galaxy, Samsung Note, or similar device, you can download the app from the Google Play Store. **Please note that standard data charges may apply depending on your service plan.**

   Note: To gain access to the Apple App Store or the Google Play Store, it will be required that you have an active Apple ID or Gmail account.

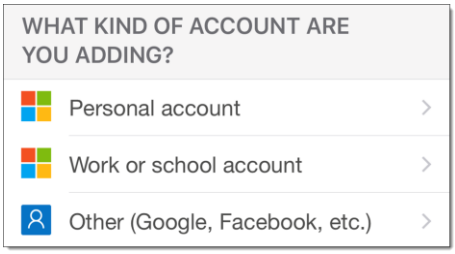
2. After installing the **Microsoft Authenticator** app, open the app.

3. You will be presented with instructions which you can view or click on **Skip** to move forward.

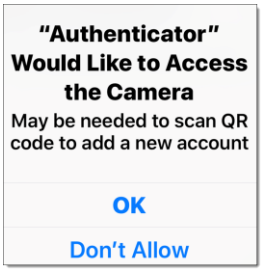
4. In the **Accounts** page on the app, tap on **Add Account** under **Ready to add your first account?**



5. You will then be asked **What kind of account will you be adding?** Tap **Work or school account**.

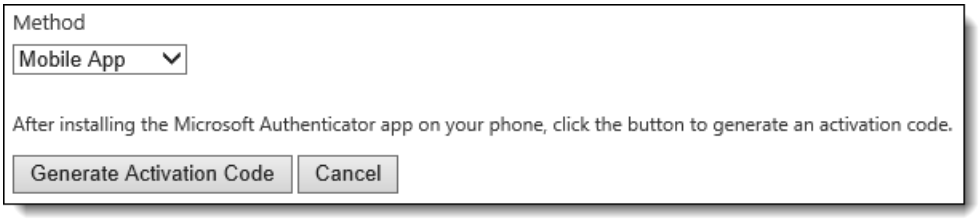


6. A prompt will appear: "Authenticator" Would like to Access the Camera. May be needed to scan QR code to add a new account. Tap **OK**.



7. You will then be directed to the Scan QR code page on the app and a message stating **Your account provider will display a QR code**.

8. Going back to your computer, select **Mobile App** from the drop-down list box and click **Generate Activation Code**.



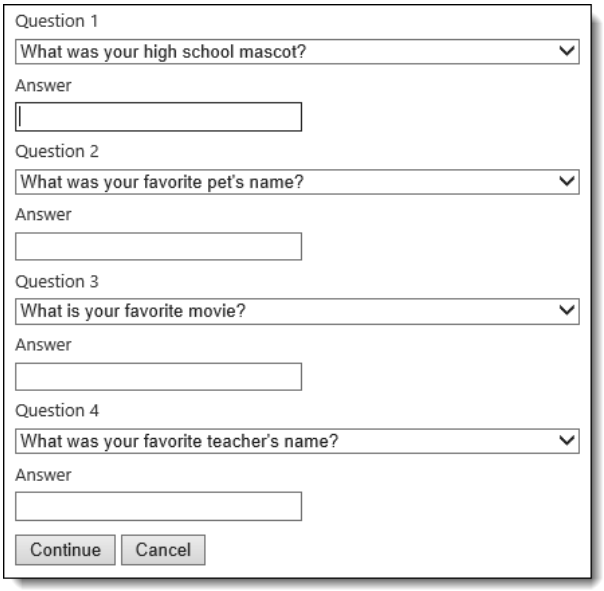
9. You can then use your phone to scan the **QR code** displayed on the **User Setup** page.

- *Note - Alternatively, you can tap **Or enter code manually** on your phone to enter the **Activation Code** displayed on the **User Setup** page.*

10. Click on **Authenticate Me Now.**

11. On your phone, you will receive a message to approve your authentication. Tap **Approve**.

12. You will then be redirected to the **Security Questions** on your computer in which you will need to select 4 different security questions and specify answers to each question.



- *Note: You must select 4 different security questions. If you select a duplicate security questions, you will get an error message that says, "Duplicate question not allowed"*

13. After successfully selecting your security questions, click on **Continue** to complete the MFA process.