Multi-Factor Authentication (MFA) Job Aid

PURPOSE

All California Department of Fish and Wildlife (CDFW) staff (employees, contractors, volunteers, etc.) are now required to have Multi-Factor Authentication (MFA) configured on their CDFW account. MFA requires you to provide a second form of identification in order to validate you are who you say you are when attempting to access department resources off the CDFW network, this includes email on any Department issued iPhone.

As you complete the steps below, if you have difficulty configuring the Authenticator Application or have issues accessing services after performing the MFA setup, please contact your local field staff or the DTD helpdesk at Helpdesk@wildlife.ca.gov (916) 445-5158.

MFA SETUP INSTRUCTIONS

STEP 1 – (From your CDFW Workstation or Laptop) VERIFY MFA SETTINGS

Navigate to the MFA security verification page from the browser on a department network connected computer: https://account.activedirectory.windowsazure.com/proofup.aspx

1. During login, you will receive a phone call to your office phone number.
    a. When prompted, hit the "#" sign on your phone - the Office 365 "Additional security verification" setup page will finish loading.
2. Under "What's your preferred option?", **select the option** that you want to use for MFA.
    a. *Call my authentication Phone* – this option will result in a phone call at a number you designate.
    b. *Text code to my authentication phone* – this allows for you to get a 6-digit code texted to your mobile device.
    c. *Call my office phone* – this will be the default setting, but it can be changed
    d. *Notify me through the app* – this is the recommended option, that requires the use of a mobile device. This will send you an alert on your mobile device through the Authenticator App (configuration instructions available in step 2).
    e. *Use verification code from app or token* – the Authenticator app generates a random 6-digit code to use for MFA. This requires the use of a mobile device and download of the Authenticator App (configuration instructions available in step 2).
3. Under "How would you like to respond?", **review** these settings:
    a. Depending on what option you've chosen, you need to either enter or validate the information that is listed. Make sure the checkbox is selected for the option you want to use
        i. If you choose an option other than the Authenticator app, **click** the save button on the page, *SKIP step 2 and PROCEED to step 3***.**
        ii. If you choose to use the authenticator app, **click** the "setup Authenticator App" box, and popup window will appear titled "*configure mobile app"*
        iii. Leave this window up and proceed to step 2 below.

STEP 2 – (From your Personal Mobile Phone - Optional) CONFIGURE MFA APP ON YOUR MOBILE DEVICE

Phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

1. **Open** the Authenticator Application on the iPhone
2. **Select** "Add account" button
3. When asked "Do you have a backup?" **click** "Continue". A backup is not required, but this step needs to be completed to proceed.
4. **Select** *"Work or school account"*
5. This opens your device's camera app
6. Use the camera to **scan** the **QR code** from the end of **Step 1** (Verify MFA settings using your PC)
7. After the app loads a name and 6-digit code, proceed to **Step 3**

STEP 3 – (From your CDFW Workstation or Laptop) FINISH WITH MFA SETTINGS ON YOUR PC

1. Return to your PC and **Click** the "save" button
2. **Type** a contact number for backup (in case the app has issues)
3. **Click** *"Done"* button

A FEW HELPFUL TIPS:

1. If you select "Call my authentication phone" or "Text code to my authentication phone" as your preferred option, you must select "Authentication phone" and the phone number you provide in this field must be a mobile phone number, do not use your office/desk phone number.

2. Do Not set your Authentication Phone number to your office/desk phone number. If you do, you will not receive the security verification notification when you attempt to connect to resources from a non CDFW network.

3. Do Not select "Call my office phone" as your preferred option. The Office Phone number is automatically set and is defaulted to the telephone number that you have set in your Human Resources Management System (HRMS) "Who am I" contact information page, which should be your office/desk phone. To review and or change your telephone number in HRMS visit https://internalapps.ad.dfg.ca.gov/hrms/ then click on the "Manage my contact information (Who am I?) link. If you update your HRMS information it may take up to 24 hours to replicate to all CDFW Identity Systems, including the MFA setup page.

4. If you have a Department issued iPhone, you are required to configure and use the Authenticator App on your Department issued iPhone. If you do not configure the Authenticator App your email, contacts, and calendar items will not synchronize to your iPhone/iPad. The Authenticator App was deployed to all Department iPhones and iPads. (Detailed setup instructions have been provided in previous email messages; however, if you need additional assistance please contact the helpdesk or your local field support staff.)

5. If you do not have a Department issued iPhone, you may elect to download, install and configure the Authenticator App for use on your personal phone. Please note: *Phone numbers will only be used for account security. Standard telephone and SMS charges will apply.*

MFA PROJECT DETAILS

Why is MFA Happening?
Per SIMM 5360-A and the California Natural Resource Agency (CNRA) mandate, CDFW is required to turn on multi-factor authentication (MFA) for all department personnel. MFA is a critical pillar of the CNRA and CDFW's cybersecurity programs – namely stopping phishing attacks and unauthorized access by users who have obtained the login details of CDFW personnel.

Why is it Important?
As we use more cloud services, your professional identity is more at risk, with MFA configured on your account, the department can better protect you and the department's assets from external risks.

How will MFA work?
With MFA, you will be prompted to verify your identity when you try to login to Office 365 apps, including Outlook, from outside the CDFW's network, either from a personal or CDFW issued device. However, you will not be prompted to verify your identity when login is from within the CDFW's network or from an active VPN session.