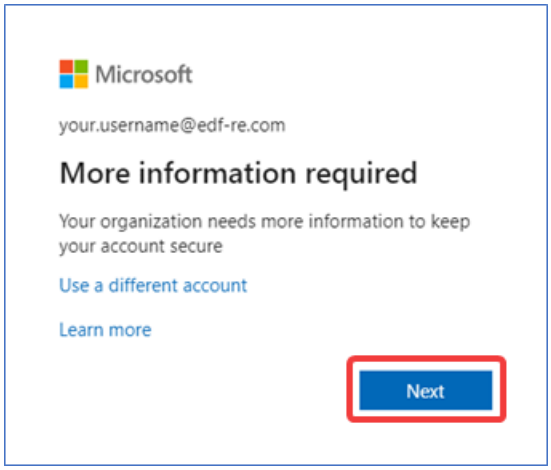
EDFR Remote Desktop Web Portal with MFA Guide

Microsoft MFA Setup

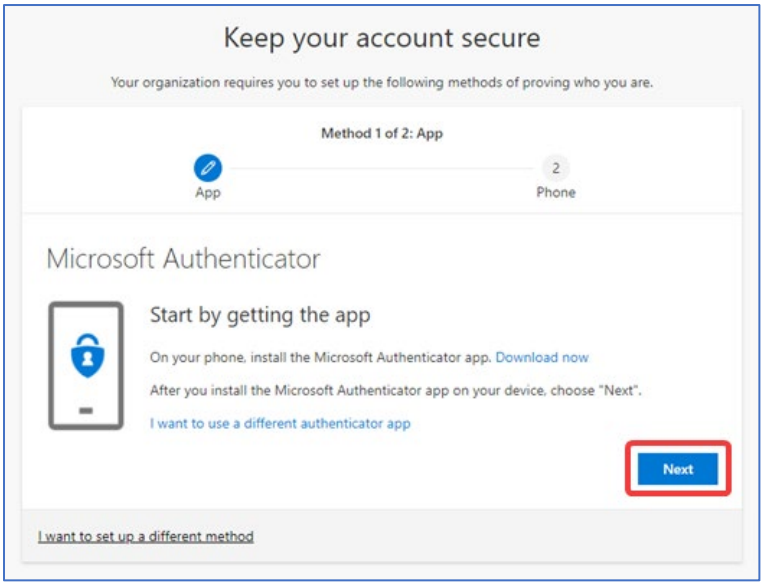
EDFR leverages MFA (Multi-Factor Authentication) to provide secure access to its Remote Desktop Web Portal. Follow the below steps to configure your MFA settings. To use the Remote Desktop Web Portal, you need to use either the Microsoft Authenticator mobile app or phone call verification options. The mobile app is recommended as it provides faster, more convenient notification approvals and is less intrusive than the phone call method.

1. Go to the Microsoft Security setup web page from your desktop or mobile device: https://aka.ms/MFASetup

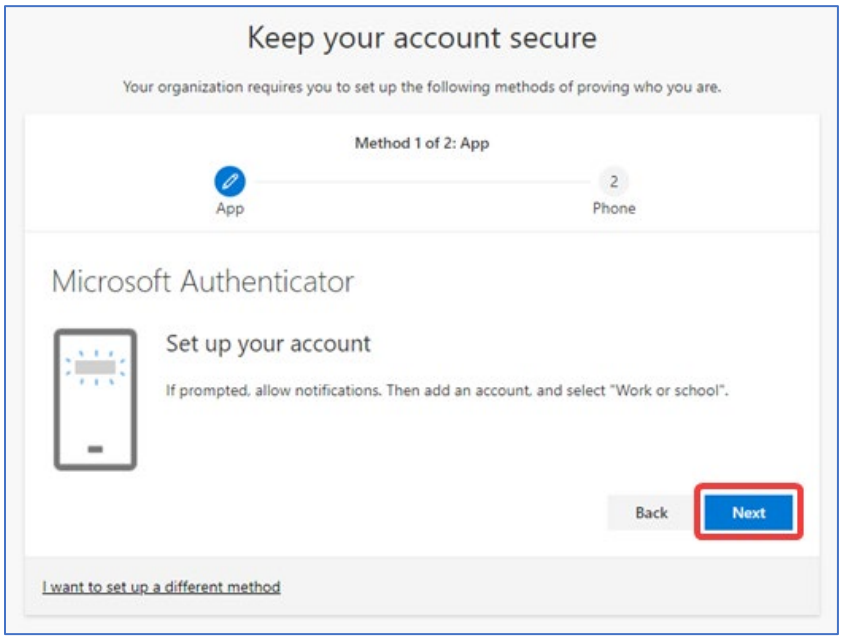
2. Sign in using your company email and password. After signing in, you should see a '**More Information Required'** message. Click **Next**.



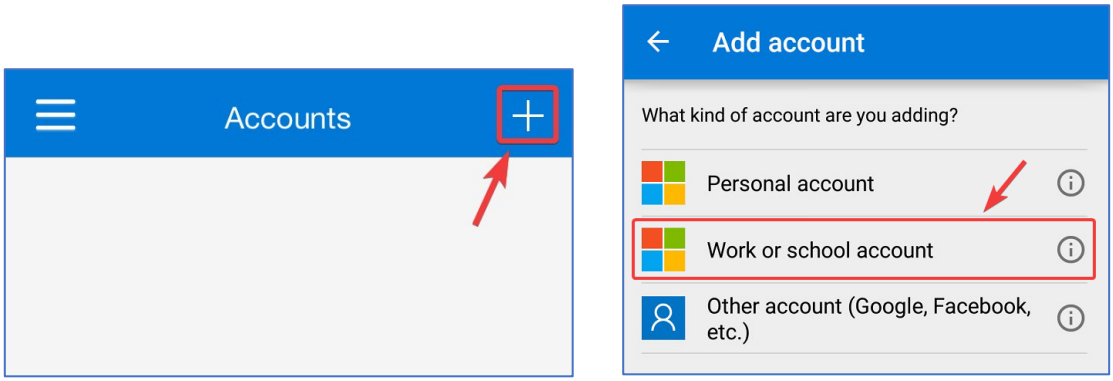
3. A '**Keep your account secure'** wizard appears, showing the first verification method to set up. On your mobile phone, use the iOS AppStore / Google Play Store to search for and install the **Microsoft Authenticator** app. To send a link for the app directly to your mobile phone, click here. After you have intalled the Microsoft Authenticator app, select **Next**.



4. The '**Set up your account'** page will appear. Click Next and go to your mobile device to continue the setup.

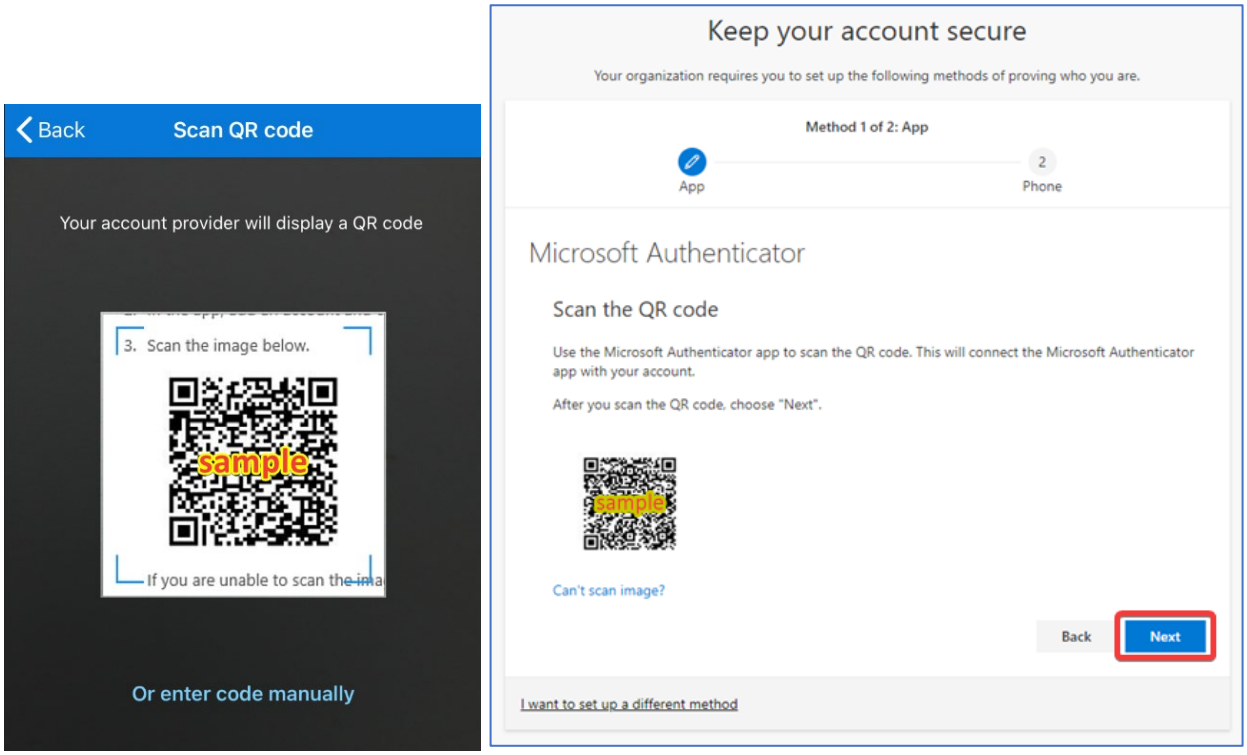


5. Open the Microsoft Authenticator app on your mobile device. If prompted, **Allow** notifications. Select **Add account** from the icon in the upper-right corner, and then select **Work or school account**.

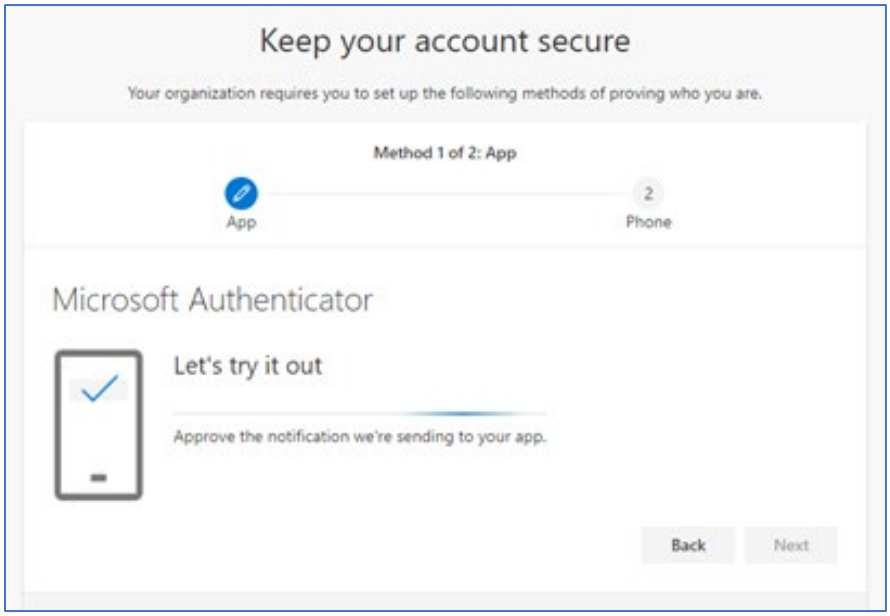


Note: If prompted, select **Allow** for the app to access your camera. This is needed so the app can take a picture of the QR code in the next step. If you do not allow camera access, you can still set up the authenticator app, but you'll need to add the code manually.

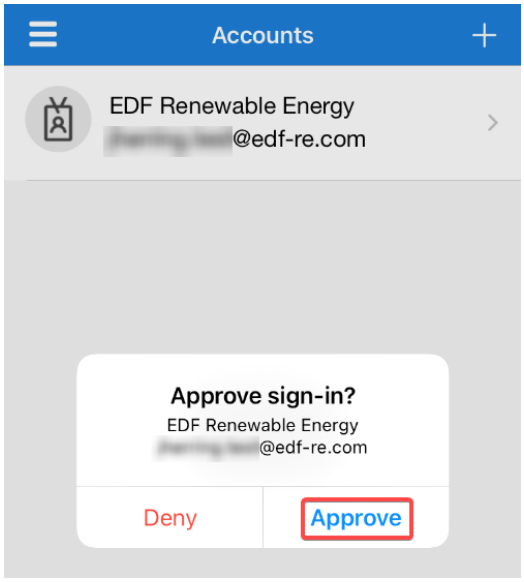
6. Use your mobile device to scan the QR code displayed on your browser. The authenticator app should automatically add your account. If the app cannot read the QR code, you can select the **Can't scan image?** link and manually enter the displayed code and URL into the Microsoft Authenticator app.

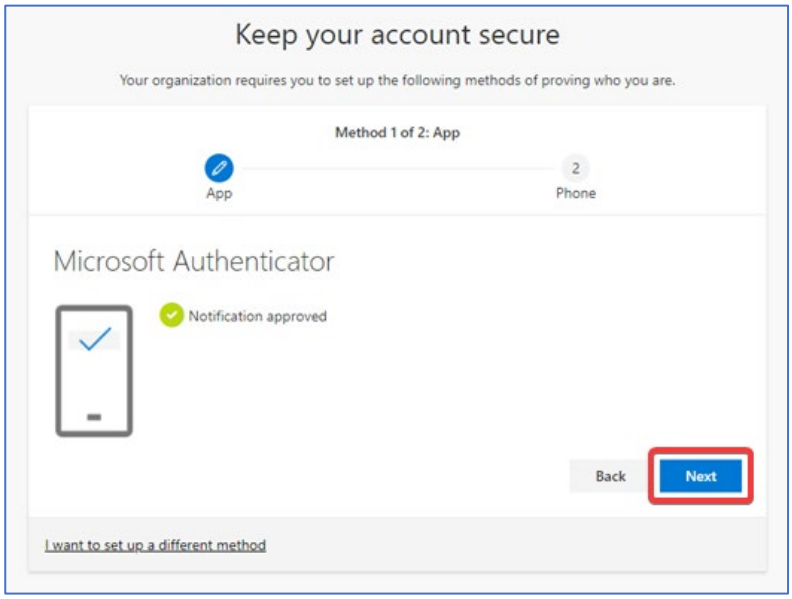


7. Select **Next** on the '**Scan the QR code'** page on your computer. A notification will be sent to the Microsoft Authenticator app on your mobile device to test your account.

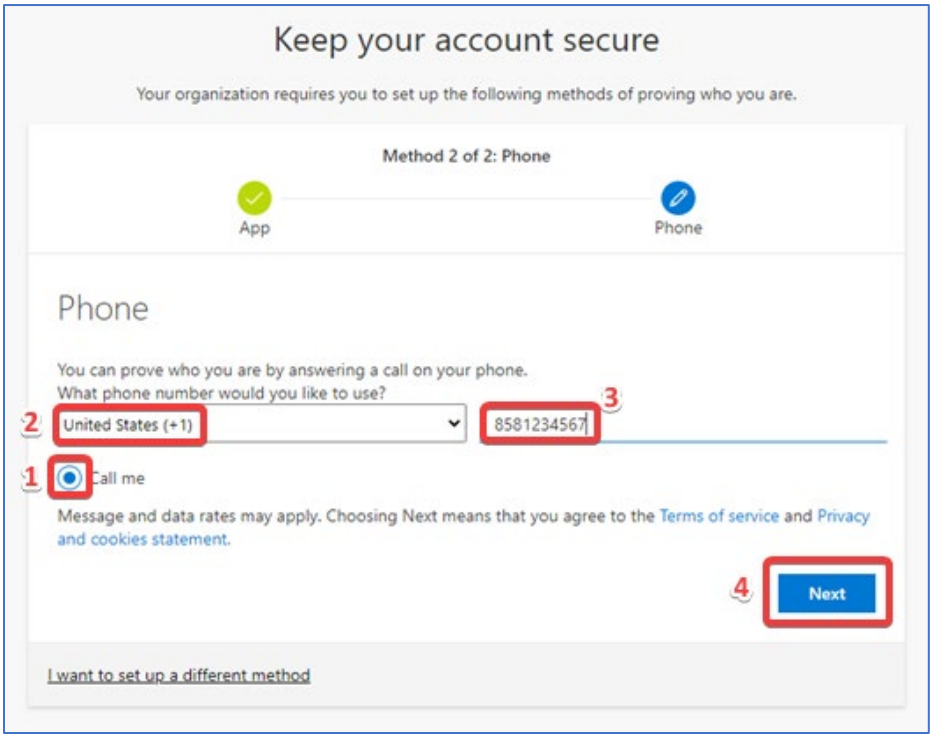


8. Approve the notification that appears in the Microsoft Authenticator app. Back on your computer, the status on the web page should show the notification was approved. Click **Next** to continue.

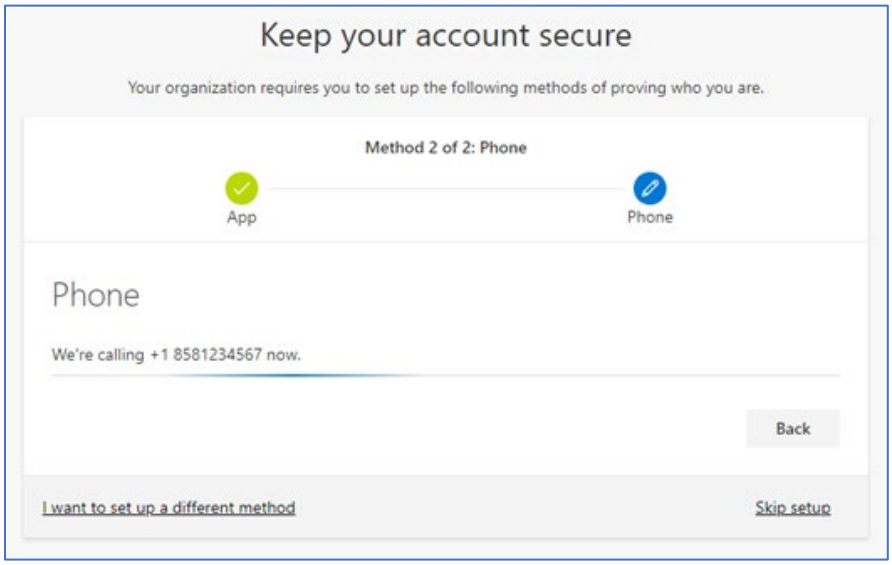




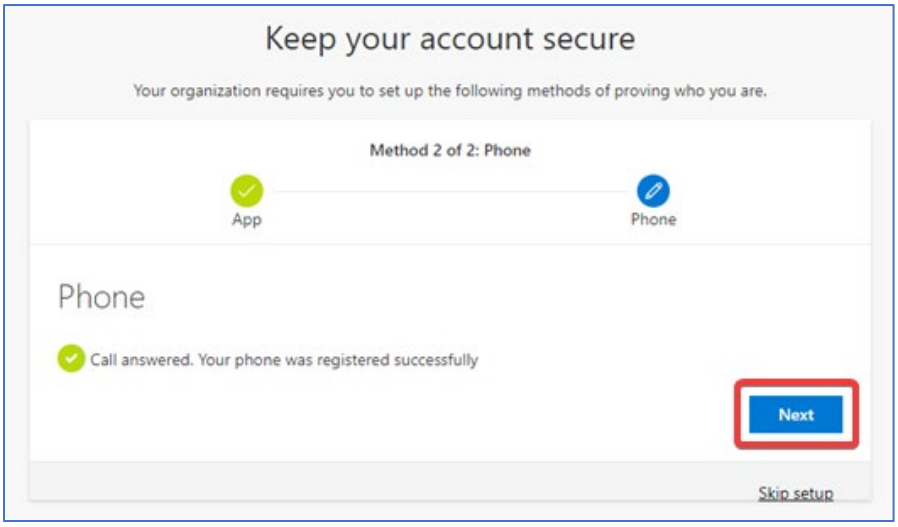
9. On the **Phone** set up page, choose **Call me.** Select your country code and enter your preferred phone number that can be used for future verification purposes. This would typically be your mobile phone number. Click **Next** to continue.



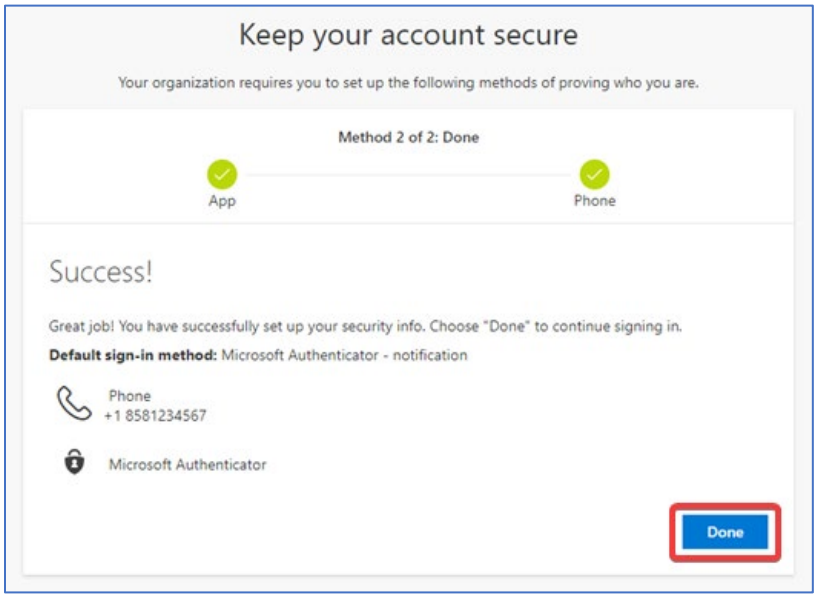
10. Microsoft will call to verify the phone number. When you receive the call, answer, and press the # key to approve the verification. You can then end the call.



11. The status on the web page should show your phone was successfully registered. Your security info is now updated to use a phone call as a backup method to verify your identity when using two-step verification or password reset. Click **Next** to continue.

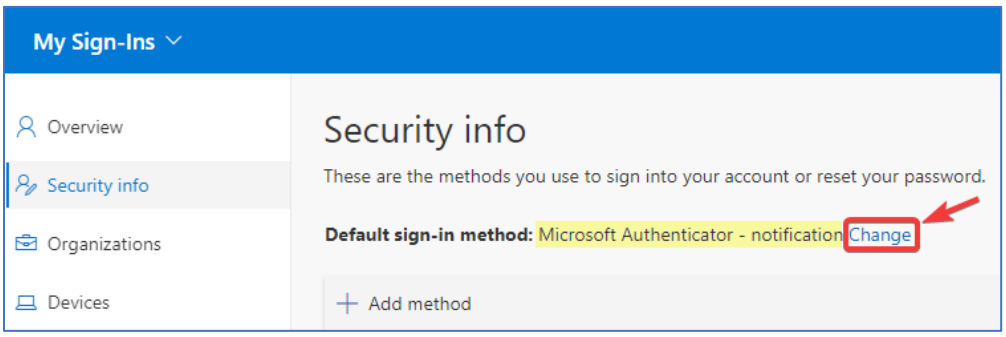


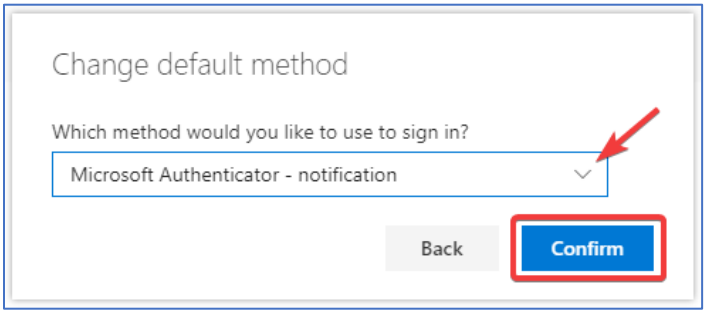
12. Review the **Success** page to verify that you've successfully set up your security info for both the Microsoft Authenticator app and phone call methods. Select **Done** to complete the registration process.



13. If you registered a phone number for your account in the past, it might be set as your default verification method. You can check and change this by clicking the **Security info** tab on your account page or using this link: https://mysignins.microsoft.com/security-info

14. Verify the listed phone number(s) are correct and the **Default sign-in method** is set to **Microsoft Authenticator - notification**, or **Phone - call** if you prefer. To make a modification, click **Change** and make your selection. Be aware, if you select **Phone - call**, you may receive phone verification calls at unexpected times when authentication sessions expire and attempt to automatically authenticate again. This is another reason the Microsoft Authenticator notification method is recommended as it is less intrusive.



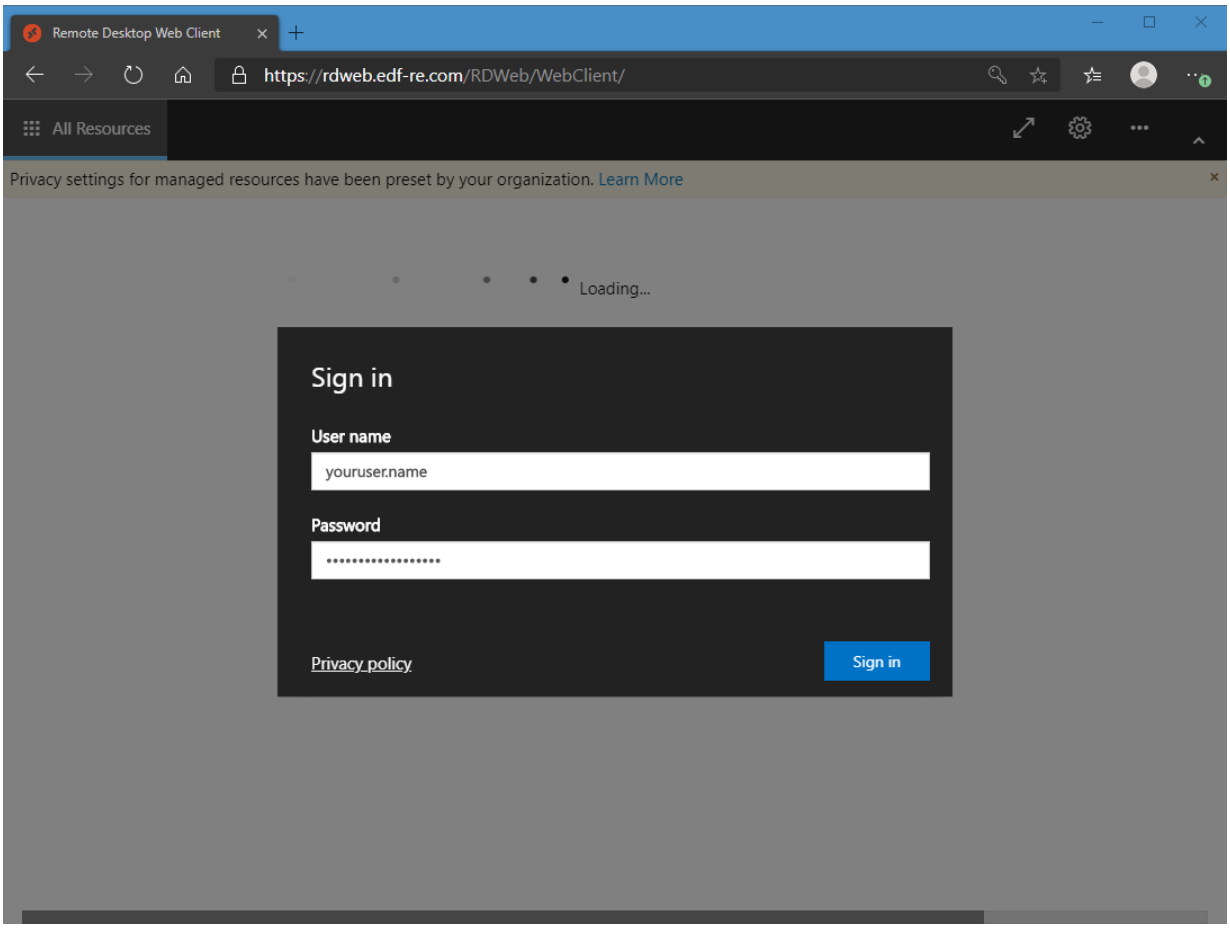


continued on next page…

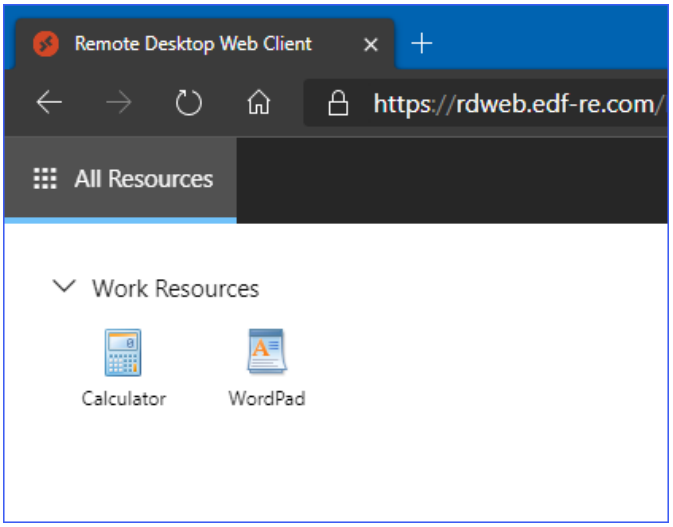
EDF Remote Desktop Web Portal

1. Got to the web portal address https://rdweb.edf-re.com
   (Have your phone ready as you will need it in the coming steps for MFA approval.)

2. Enter your Username and Password when prompted and click the “Sign in” button.

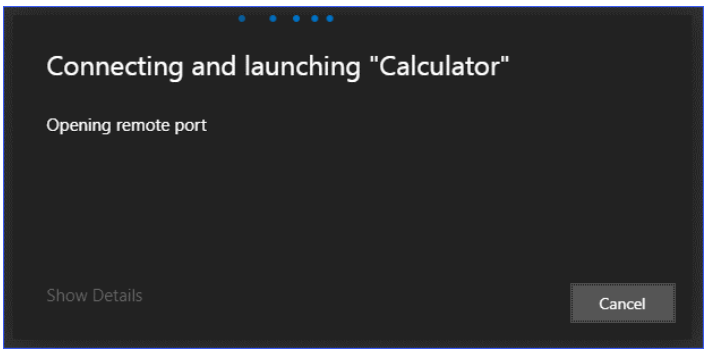


3. Upon successful login, you will be presented with the published apps you’ve been granted access to.



4. Click on the published app you would like to launch.

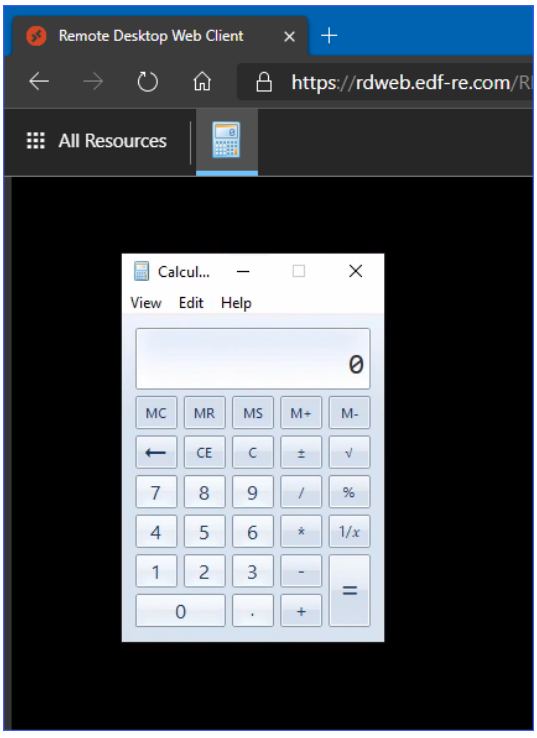
5. During this connection process, an approval request will be sent either via phone call or notification to the Microsoft Authenticator app on your mobile phone depending on the option you chose earlier for your default MFA method. This should occur during the "**Opening remote port**" status shown above.



For the phone call method, press "#" to approve after answering the call. For the mobile app, click "Approve" when the pop-up notification appears on your phone.

*If the published app fails to connect and you did not receive the notification, unlock your phone and launch the Microsoft Authenticator mobile app. Then repeat the above step to launch the published app on the web page.

6. The application should then launch in the portal.



7. If you need to launch another app, click on "**All Resources**" and then click on the next app.
8. When you are finished working, click "Sign Out" in the upper right corner and close the tab in your browser.