Configuration of Multi-Factor Authentication

Instructions

简体中文
Česky
Le Français
Deutsch
日本語
한국의
Português
Español

Summary

In an effort to improve cyber security at Johnson Controls, Multi-Factor authentication will be enabled for VPN clients, Outlook Webmail (OWA), and SharePoint users across the Johnson Controls enterprise. With this new, established service, we will be able to support additional applications with MFA in the future. Multi-Factor Authentication (MFA) is an authentication method that employs more than one factor to verify a user's account. On JCI managed devices, second factor authentication happens behind the scenes for OWA and SharePoint. In order to be JCI managed, a device needs to be Intune managed or joined to JCI's Active Directory GO domain (go.johnsoncontrols.com); the device itself will provide the verification automatically. However, users will be required to provide second factor authentication when logging into VPN, even if the device is JCI managed. For non-managed devices (personal devices not managed by Intune or Tyco/JCI legacy PCs not on the GO domain); second factor authentication occurs via your mobile device and/or a landline. For more information visit the MFA site at https://on.jci.com/MFA.

This document provides the necessary instructions for configuration of the authenticator mobile application and phone verification.

Registration Information:

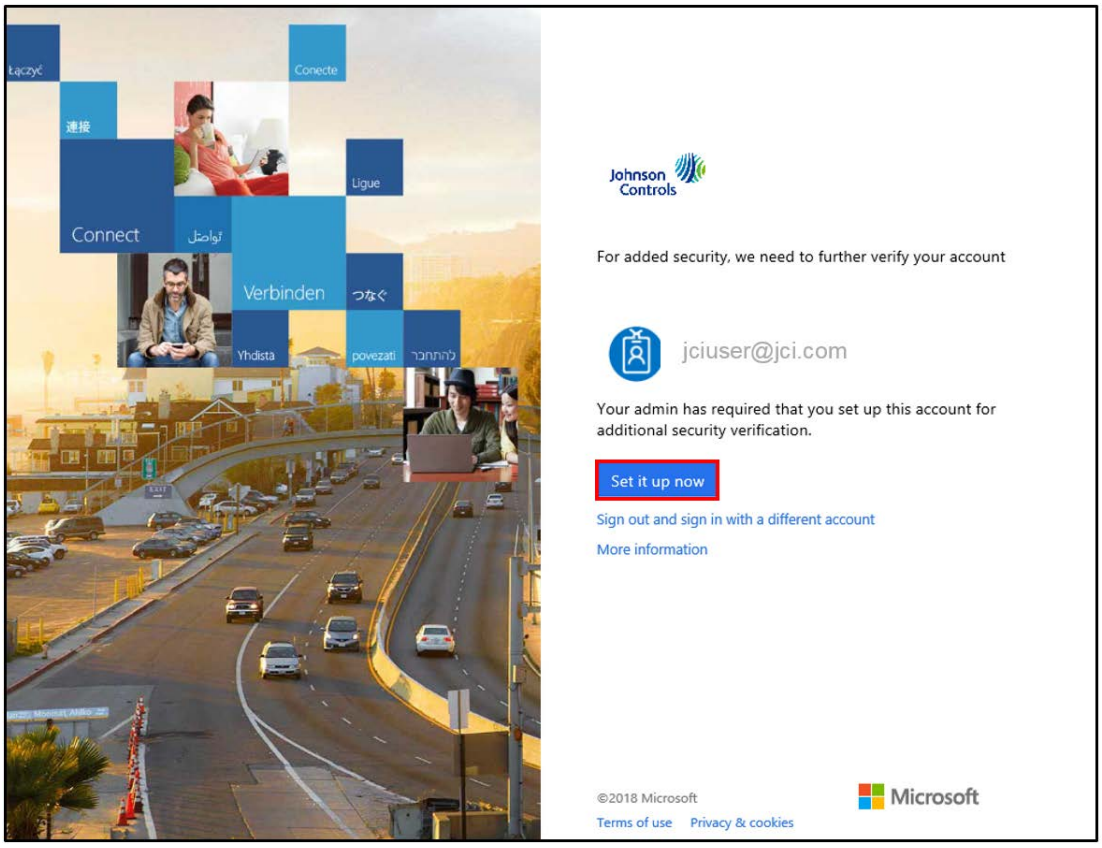
Once your MFA account has been turned on, you will have to configure your authentication preferences before you can use the VPN clients, Outlook Webmail and SharePoint.

Please contact the service desk for any questions regarding set up.

Set Up:

To trigger the registration process, you will need open **Internet Explorer** and go to https://aka.ms/mfasetup

This will prompt you with the following screen:



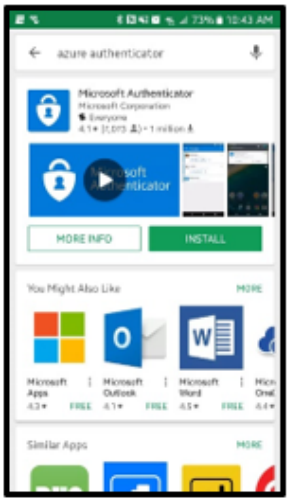
To get started, select **Set it up now.**

You have **two options** to setup verification preferences:

1. Mobile App (pages 3-9) - *preferred*
2. Calling Option Only (pages 10-12)

Obtaining the Mobile App:

The authenticator app should have been pushed to your Intune managed device already. If you are using a personal device, or if your managed device did not get the app pushed to it you can go to your app store and download it by searching for "Microsoft Authenticator App". If you do not have a way to access the mobile app, you may use the call option (see the next section for instructions).



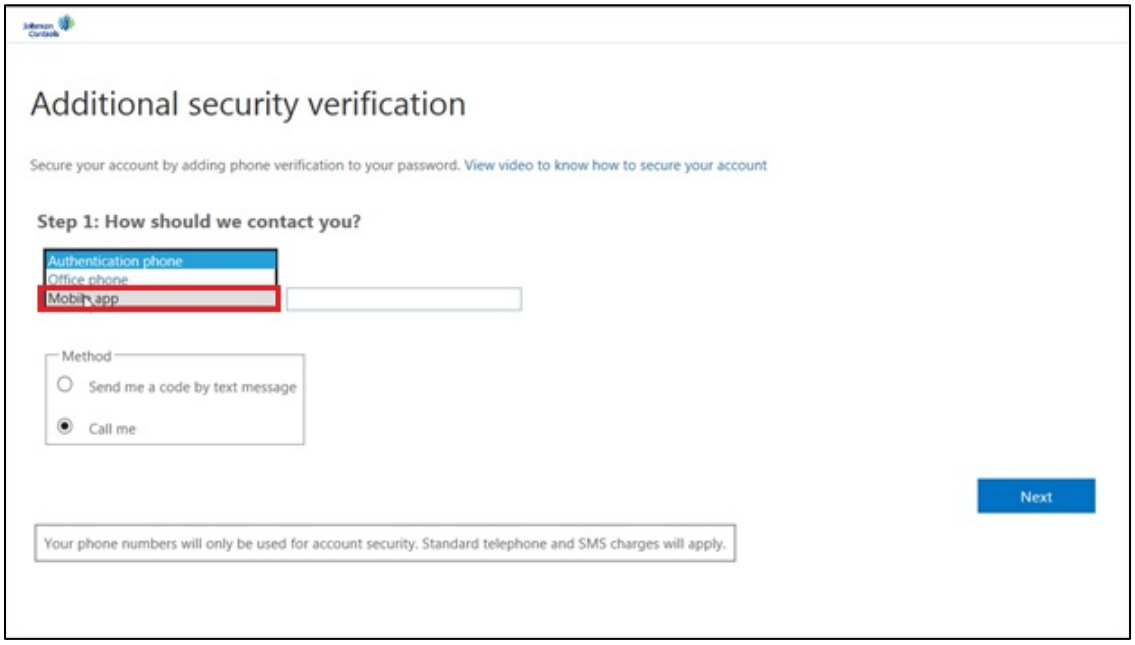
(Android)

(Apple)

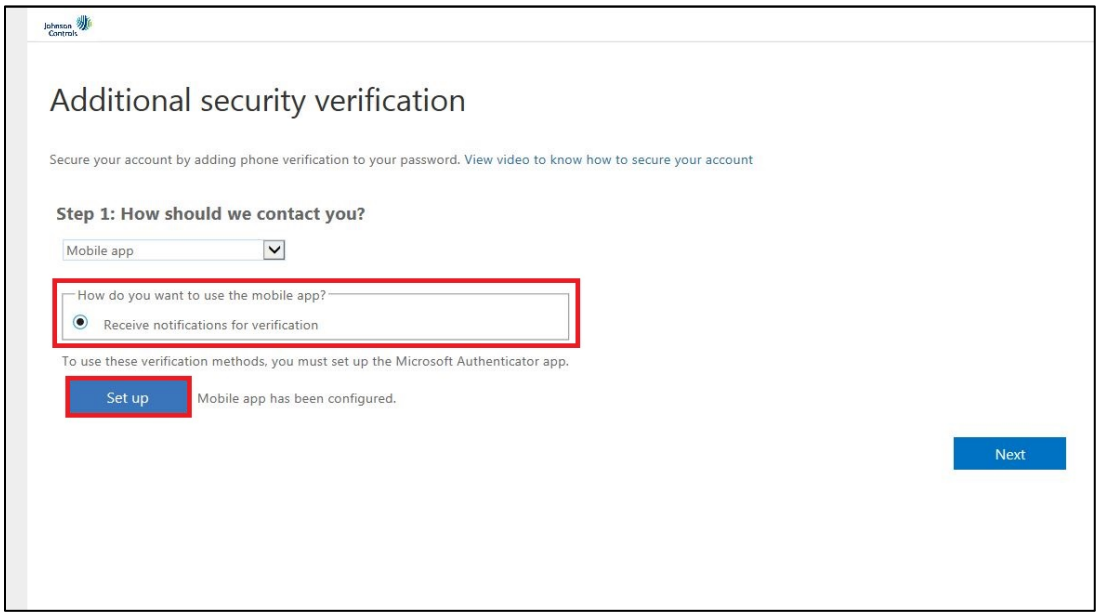
Set Up Verification Preferences (Mobile App)

The first question in the enrollment process is how you want to be contacted. We will be asking you to use the mobile app as the preferred method of verification.

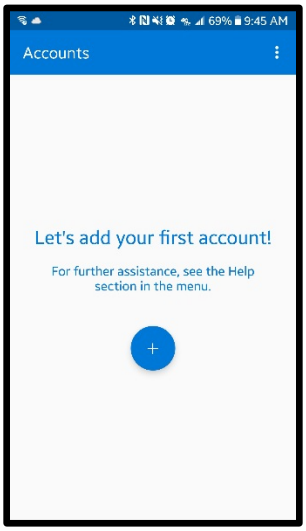
1. Select **Mobile App** from the drop-down list.



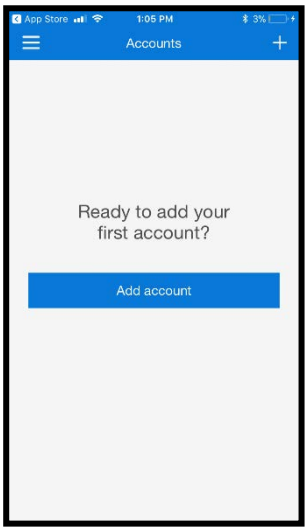
2. Select **Receive Notifications for Verification**, then select **Set up.**



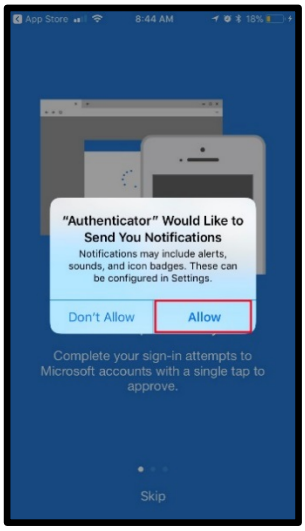
3. **On your phone or tablet**, open the Azure Authenticator Application and select **+ or Add account** to add an account. *Note*: If it looks like there is an account already set up, please ignore and add another account.



(Android)

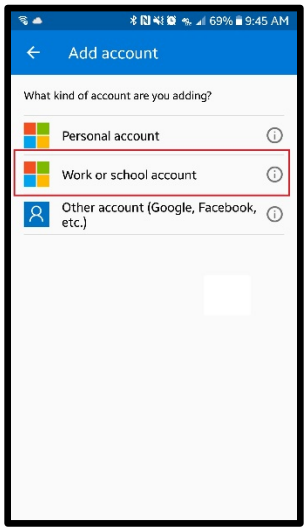


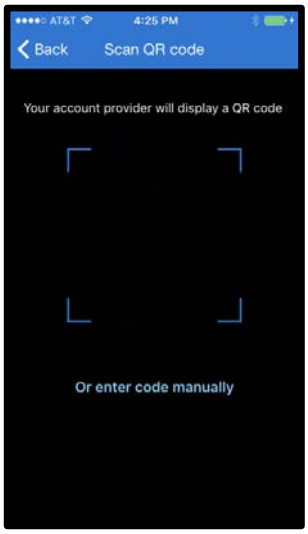
(Apple)

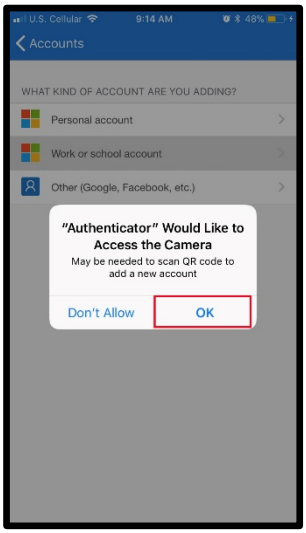


(If asked select Allow)

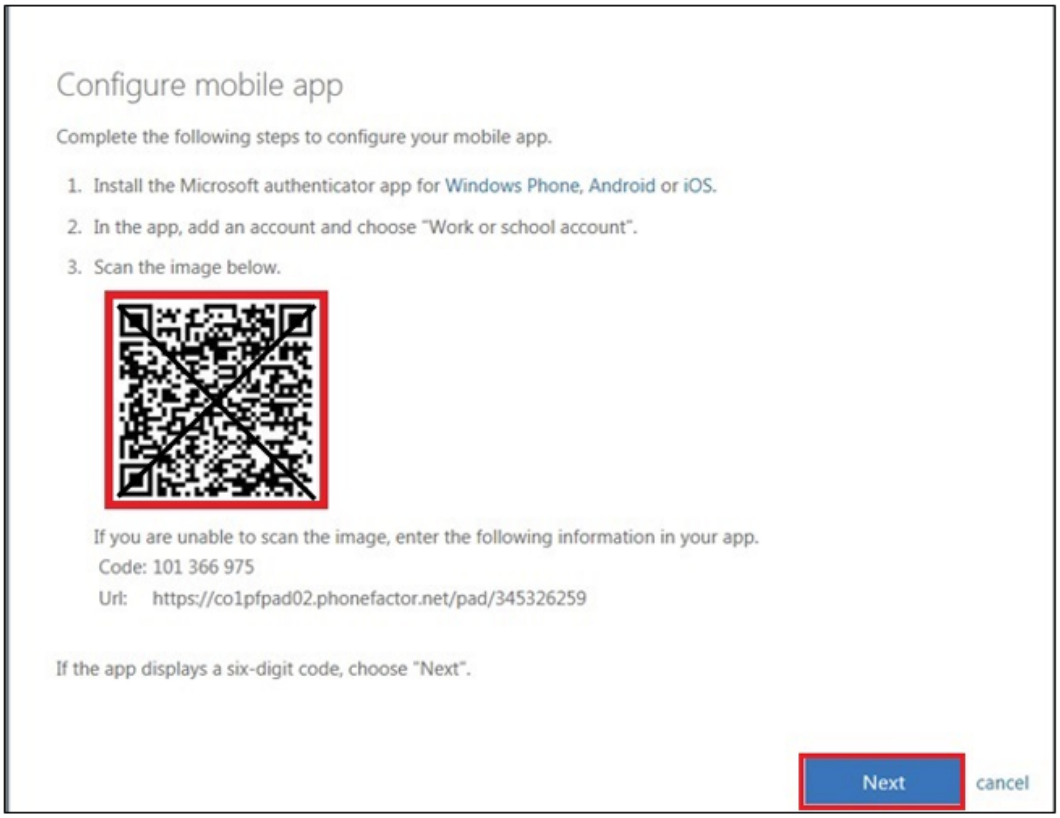
4. Specify that you want to add a work account. The QR code scanner on your phone will open (if prompted to allow access to the camera say **Ok**).



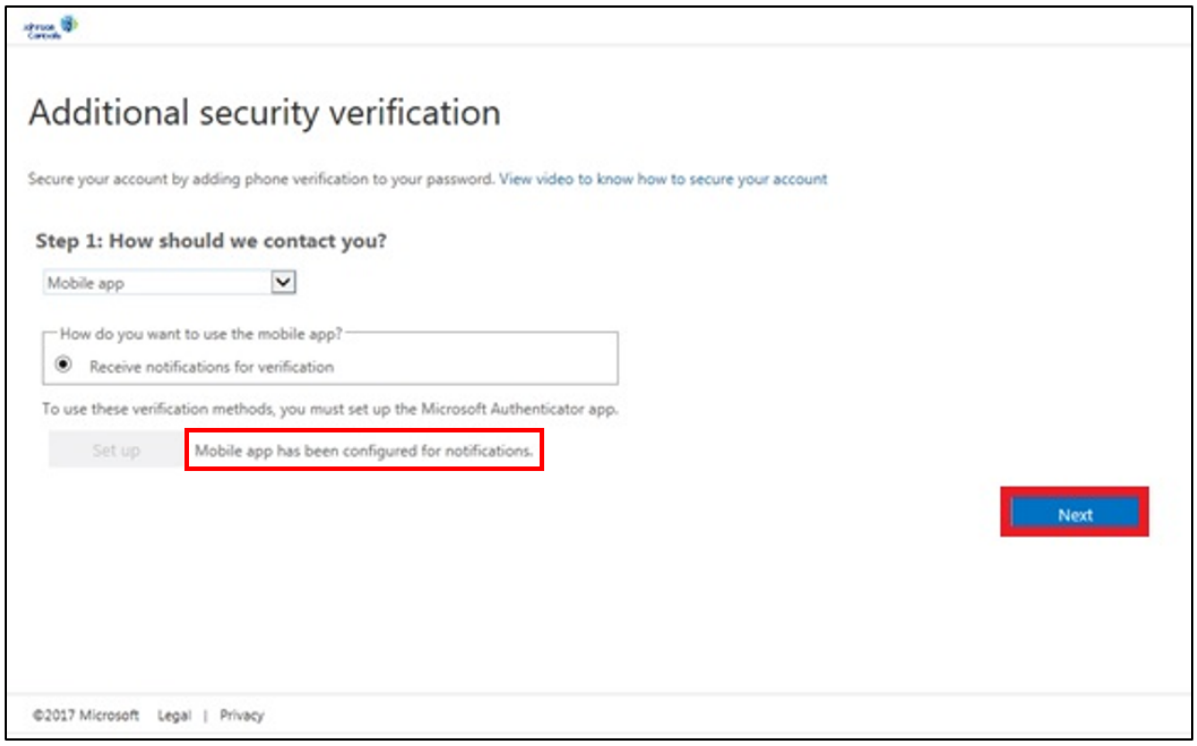




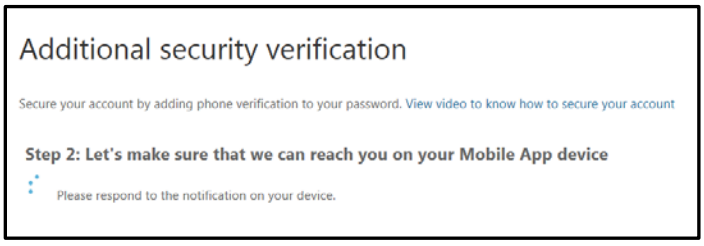
5. Scan the QR code picture with your mobile device that appears on the screen for configuring the mobile app. When that is complete, you will be able to select **Next.**

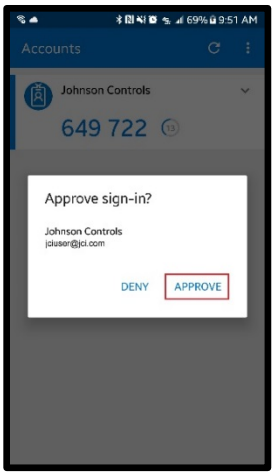


6. You will see a message indicating the Mobile App has been configured. When you see that message, select **Next**.

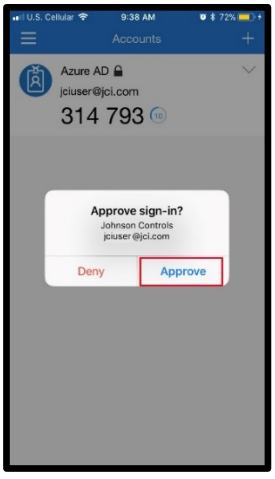


7. The **Azure Authenticator Application** will verify it can contact your phone. You will receive a test notification right away to verify your account. Select **Approve**.



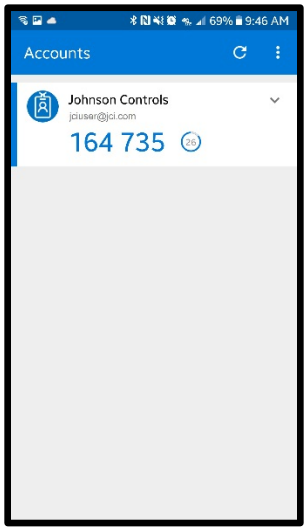


(Android)

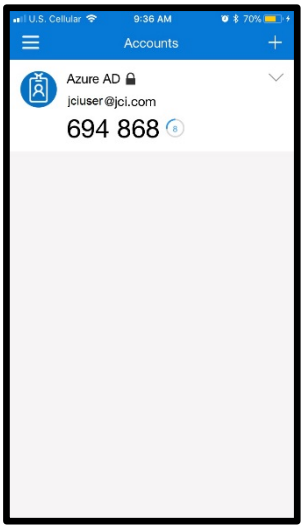


(Apple)

On your mobile device you will now see your account in the Azure Authenticator Application.

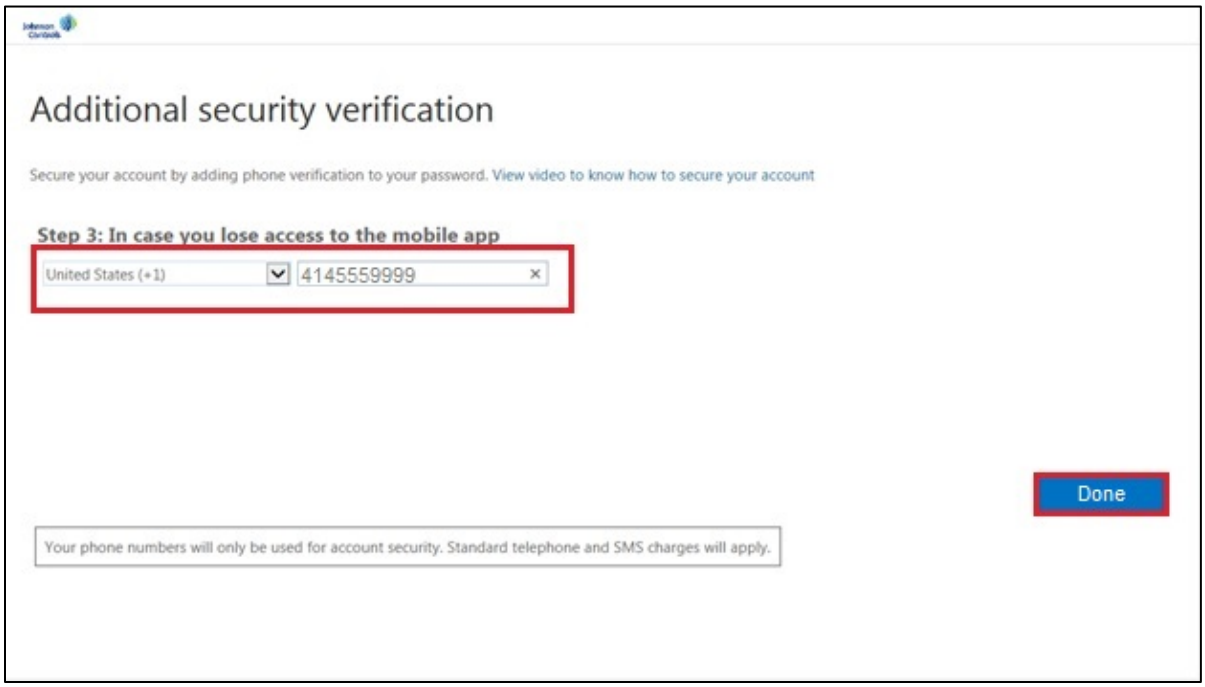


(Android)

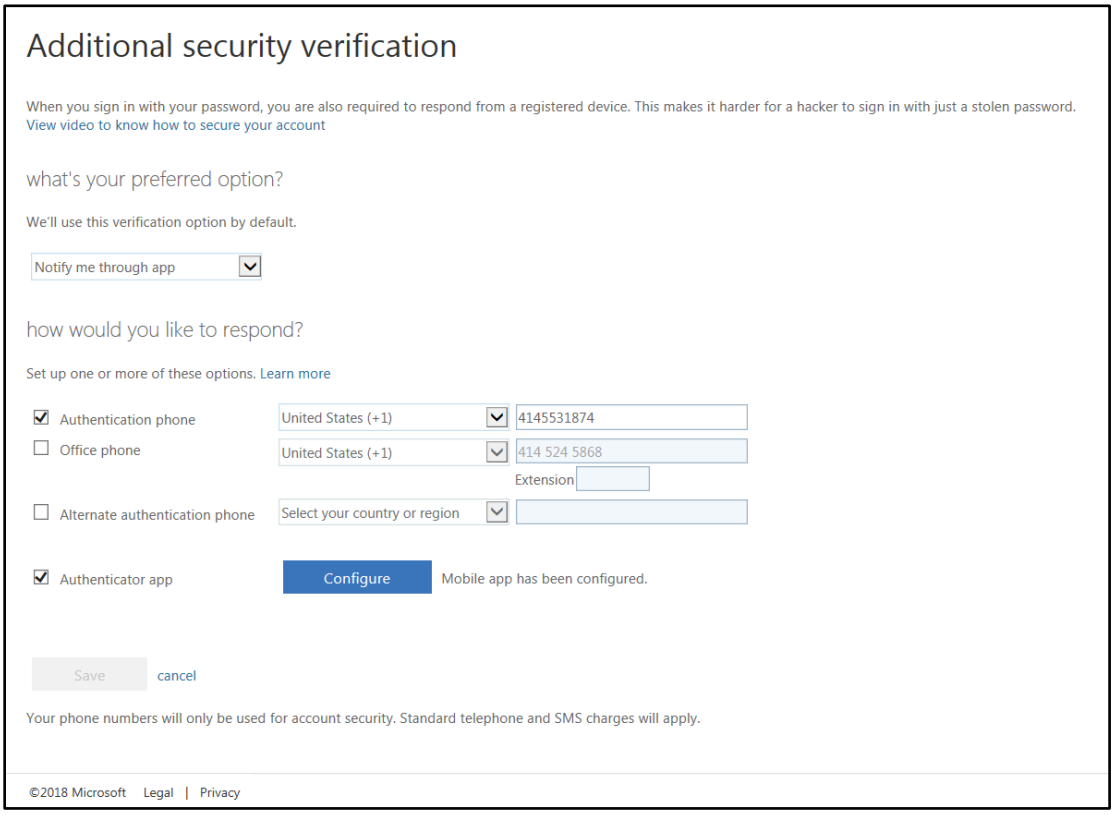


(Apple)

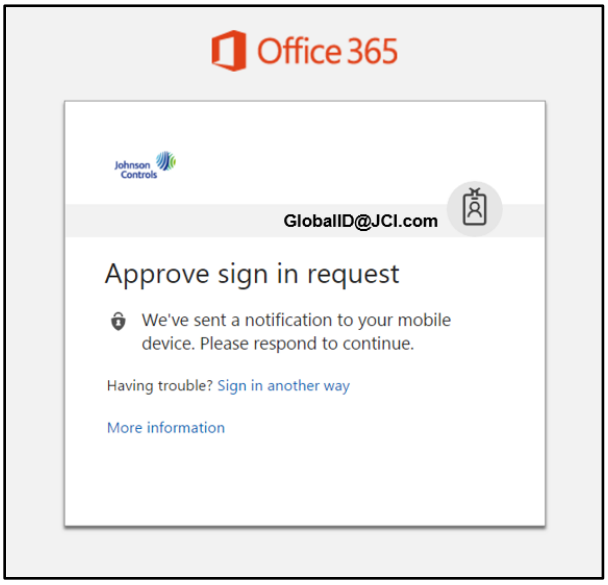
8. To finish setting up your account, Azure will ask you for your phone number. This is a secondary form of authentication in case you could not be reached through the application. Enter your phone number, then select **Done.**

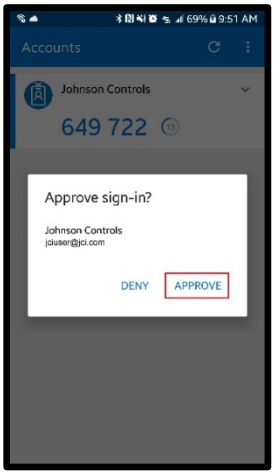


9. After you have completed the initial setup, you may be brought to a screen similar to below based on your preferences. You will have to have at least **two methods** configured (e.g. authentication phone and authentication app or authentication phone and office phone, etc.)

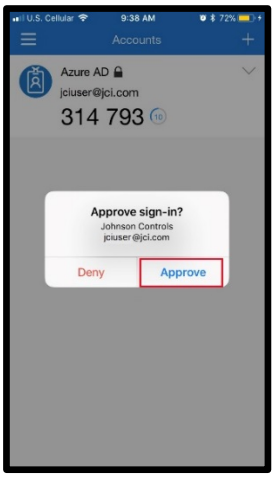


10. Once your account configuration is complete, you will be prompted for mobile verification when accessing the select applications. Once you see the following screen, use the **Azure Authenticator Application** on your mobile device to respond/verify.





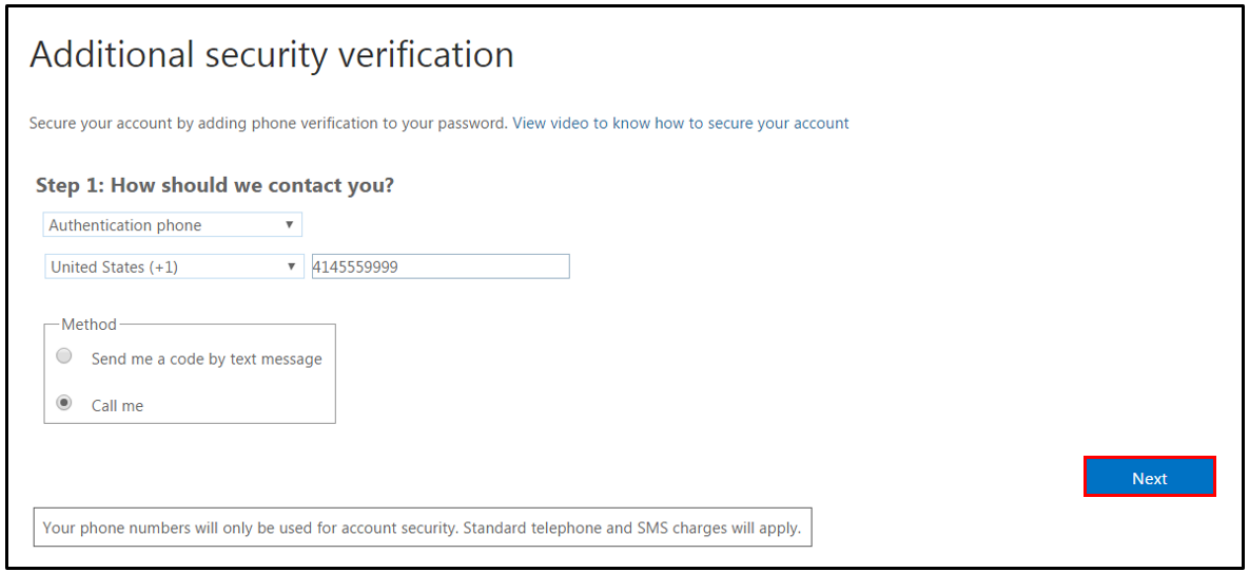
(Android)



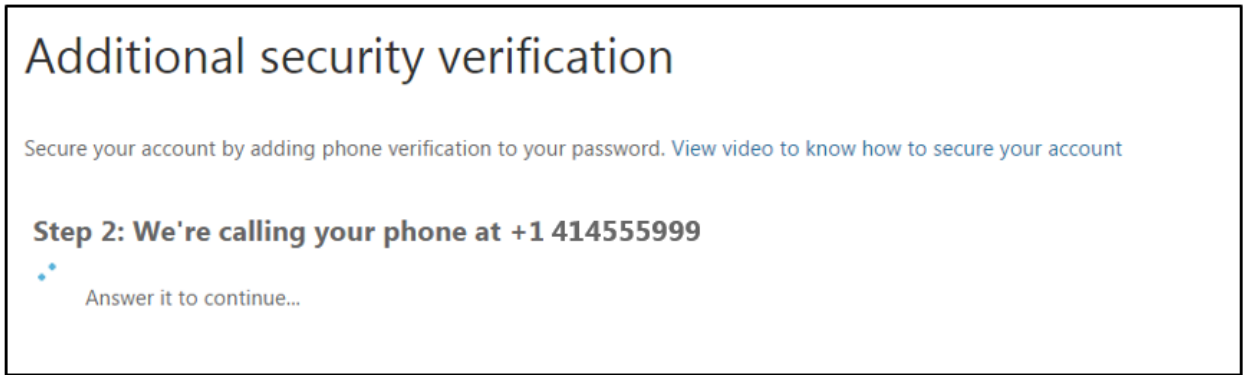
(Apple)

Set Up Verification Preferences (Calling Option Only)

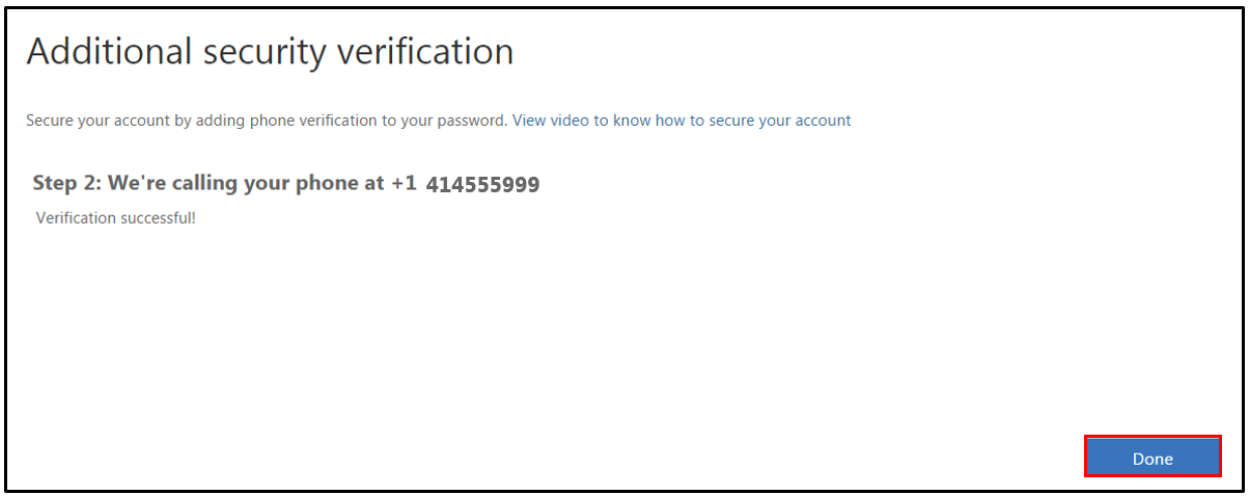
1. Select **Authentication phone** from the drop-down list, input your phone number, and select **Next.**



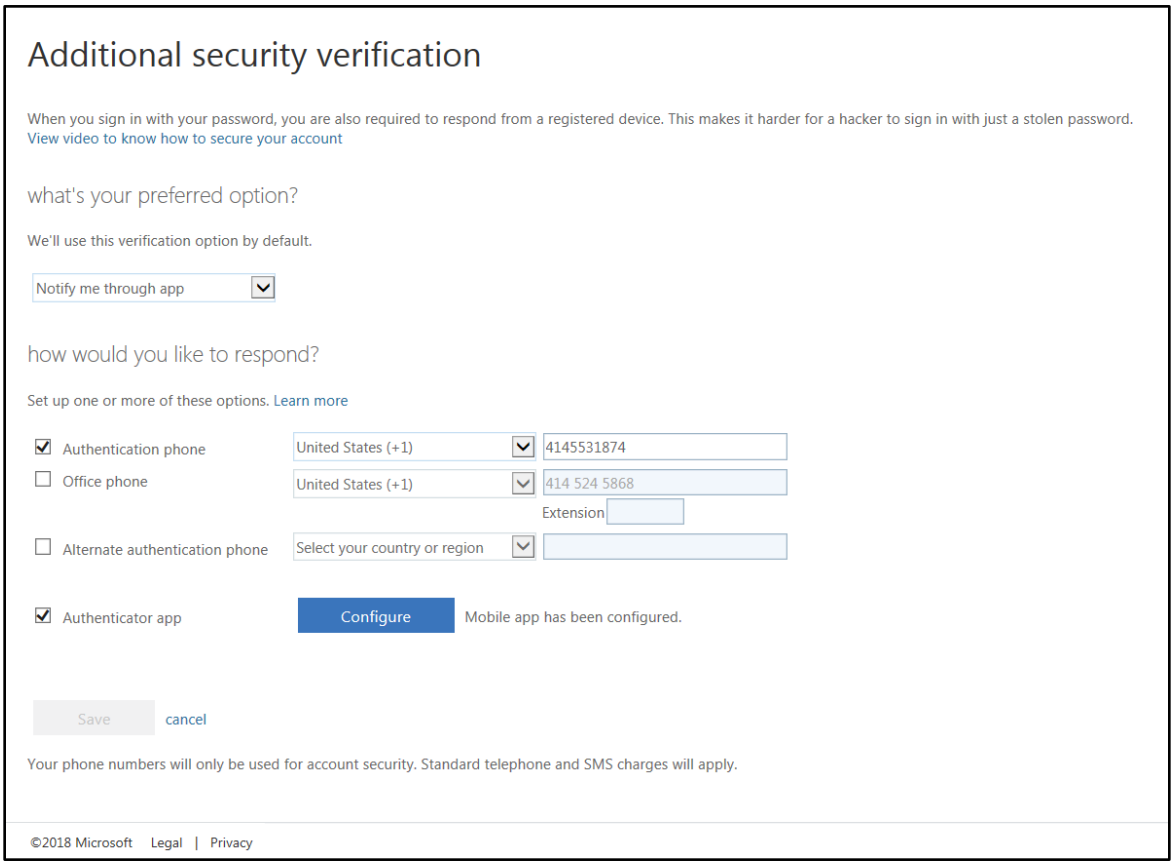
2. You will receive a phone call. **Answer the call** and follow the instructions provided.



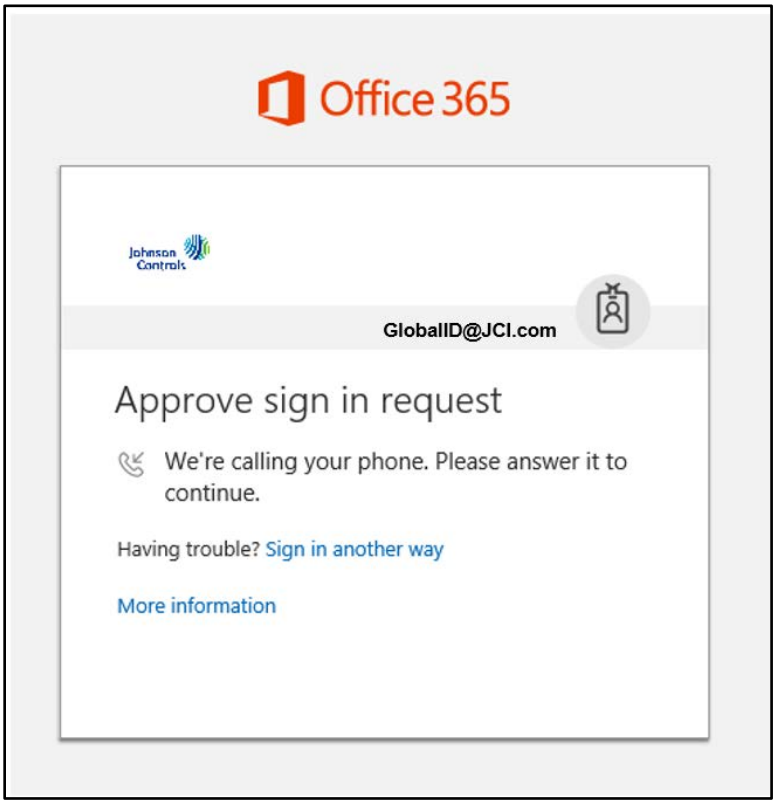
3. Once the phone call is complete, you will see "Verification successful!" and select **Done.**



4. After you have completed the initial setup, you will be brought to a screen similar to below based on your preferences. You will have to have at least **two methods** configured (e.g. authentication phone and authentication app or authentication phone and office phone, etc.).



11. Once your account configuration is complete, you will be prompted for phone verification when accessing the select applications. Once you see the following screen, you will receive a call from **+1 (855) 330-8653**. You will need to answer the call and press **#** to authenticate.



Replacement Device

In order to update your account with a new device, visit https://aka.ms/mfasetup and **follow the configuration process on the new device.**