MAXIMUS

Sign in to Office 365 Using Azure Multi-Factor Authentication (MFA)

MAXIMUS IT – Active Directory

Updated (02.12.2021)

Contents

MFA Conditions and Scope

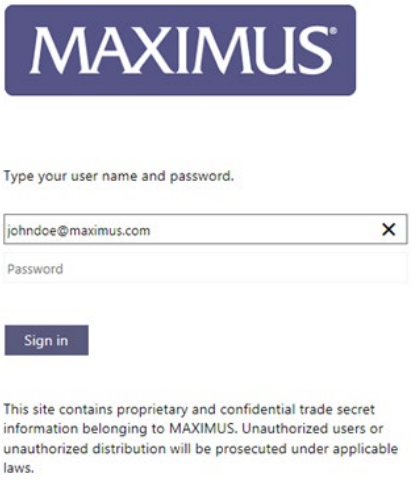
Maximus users will be required to sign in using Azure Multi-Factor Authentication (MFA) when using Microsoft Office 365 (O365) websites and applications (Teams, Outlook, Word, Excel, OneDrive, SharePoint, etc.) from non-Maximus networks and from workstations and mobile devices that are not registered as managed by Maximus.

Things to Know

- The use of MFA for sign-in to O365 products is not required in the following scenarios:
  - When connected to a Maximus network within physical Maximus office sites
  - While using Maximus AWS Workspaces
  - While using a device while connected to the Maximus VPN from any remote location
  - While using Mobile devices managed by Maximus Intune
  - While using Maximus-managed and registered workstations in any scenario - even outside of Maximus networks
- The use of a personal non-Maximus managed device **WILL** require Azure MFA to O365 resources
- The token used for MFA for O365 products is the Azure MFA service. The best user experience is to install the Microsoft Authenticator app on your mobile device (sign-in and installation instructions below).
- Other methods of acquiring an Azure token are outlined below in the Changing MFA Verification section.
  - Available Azure MFA verification methods include:
    - Acceptance of a push notification sent to the Microsoft Authenticator app.
    - Manual entry of a numeric code visible within the Microsoft Authenticator app.
    - Manual entry of a numeric code sent to a mobile device via SMS text message.
    - Manual entry of a numeric code communicated via an automated voice call.
    - Manual entry of a numeric code sent to an alternate email address.

How to Sign into Microsoft O365 Resources with MFA

1. Launch any Office 365 website or application from a non-Maximus network. Enter your Maximus email address and password and click **Sign in**.

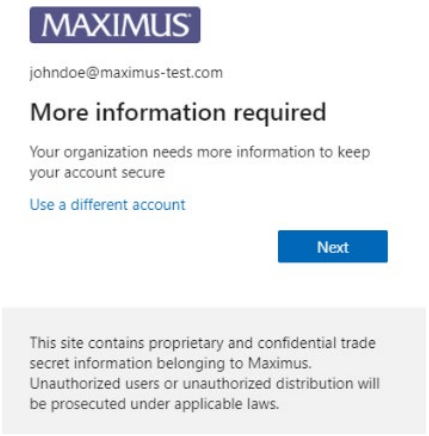


Azure MFA Enrollment Process

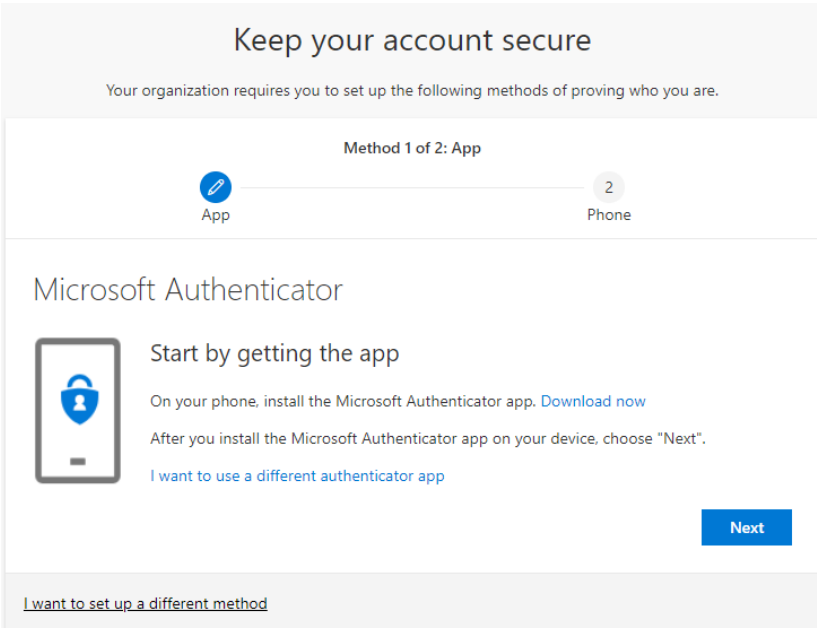
When signing into O365 applications from a non-Maximus network for the first time, you will be required to enroll in Azure MFA.

Follow the steps below to complete the enrollment process:

1. After sign-in you see a screen asking if you want to stay signed in, you may click either Yes or No. A “More Information Required” screen will appear. Click Next.



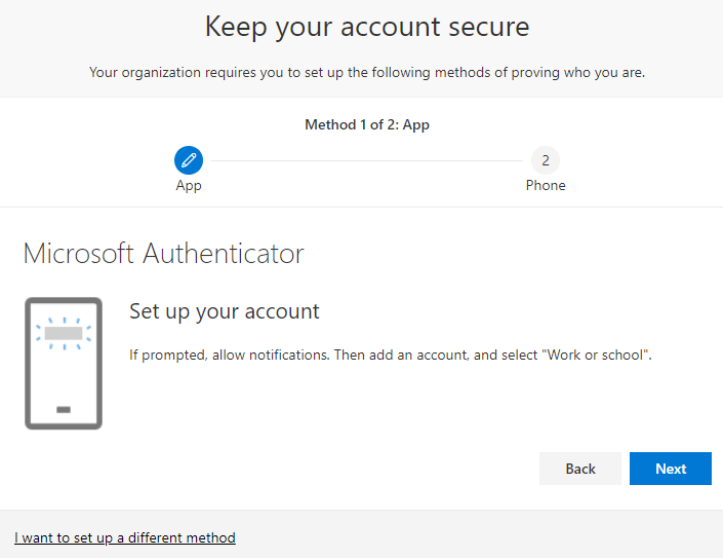
2. If you do not already have the Microsoft Authenticator app installed on your mobile device, install it from the device’s app store. The app is supported on the following devices:
   - iPhone/iPad
   - Android
   - Windows Phone



NOTE: *The first authentication method selected by default is the Microsoft Authenticator app.*

*Other options can be selected by clicking **I want to set up a different method**, but we strongly recommend using Microsoft Authenticator. It supports push notifications, just like the OneLogin Protect app, and thus is the easiest to use. It can also be configured to require manual code entry, rather than push notifications, but this is not recommended unless the mobile device does not have a reliable internet connection for the push notifications.*

3. After you have installed the Microsoft Authenticator app on your device, click **Next** to continue the setup.



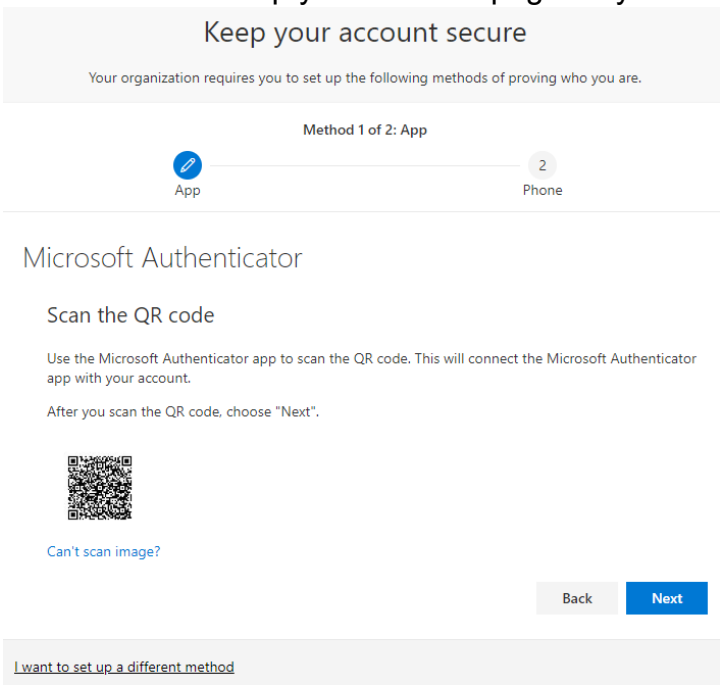
4. Open the Microsoft Authenticator app on your mobile device. If prompted, tap the option to allow notifications.

5. Add a work account by **one** of the following methods, depending on your device:
   - iOS
     - Tap the plus (+) icon in the upper right corner, then tap **Work or school account**.
     - Tap the option to allow the app to access your camera.

   - Android
     - Tap the three vertical dots in the upper right corner, then tap **Add account**, and then **Work or school account**.
     - Tap the option to allow the app to take pictures and record video.

   ***NOTE:** The step for allowing camera access is necessary for the app to scan the QR code on the next screen in the MFA enrollment wizard, which adds the account information into the app.*

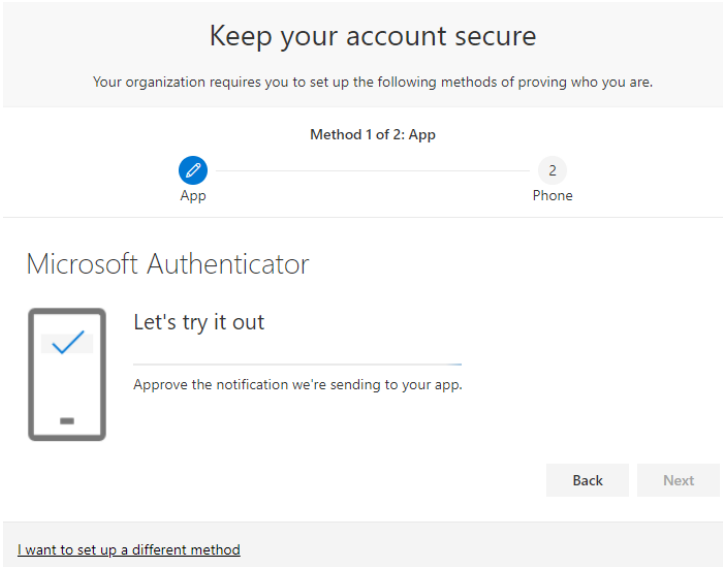
6. Return to the Set up your account page on your computer, then click **Next**.



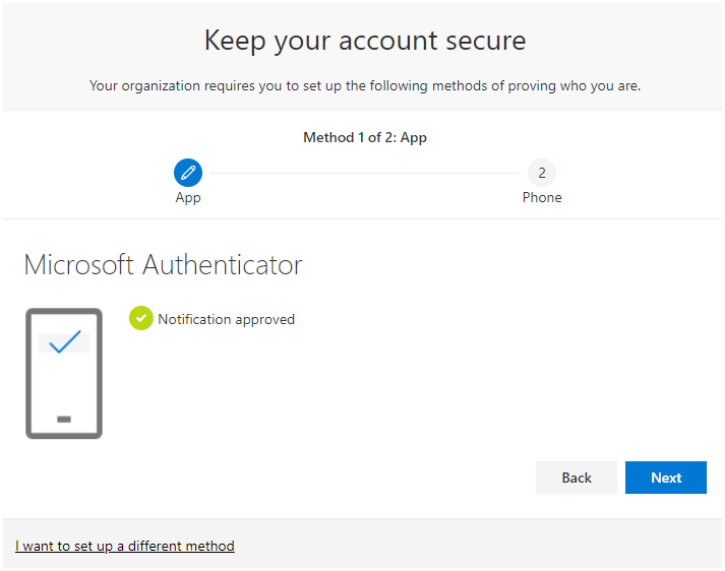
7. Hold your phone over the square QR code image on the screen so that it's visible within the camera view in the app. Once the code has been successfully scanned, the account will be automatically added to the app. Click **Next**.

   NOTE: *The authenticator app will add your work or school account without requiring any additional information from you. However, if the QR code reader can't read the code, you can click the* ***Can't scan image*** *link and manually enter the code and URL into the Microsoft Authenticator app. For more information about manually adding a code, see Manually add an account to the app.*

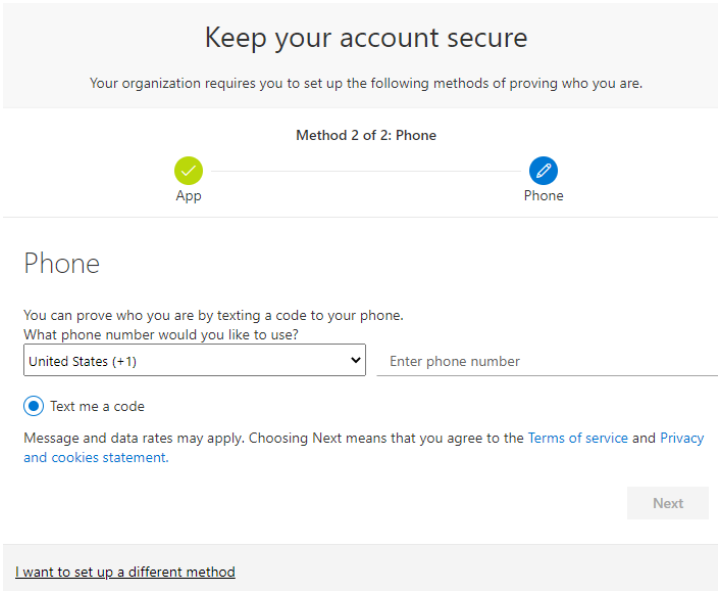
8. Azure will now send a push notification to the Microsoft Authenticator app on your mobile device to confirm that the setup is complete. On your device, tap the **Approve** option on the notification.



9. On your computer, click **Next**.

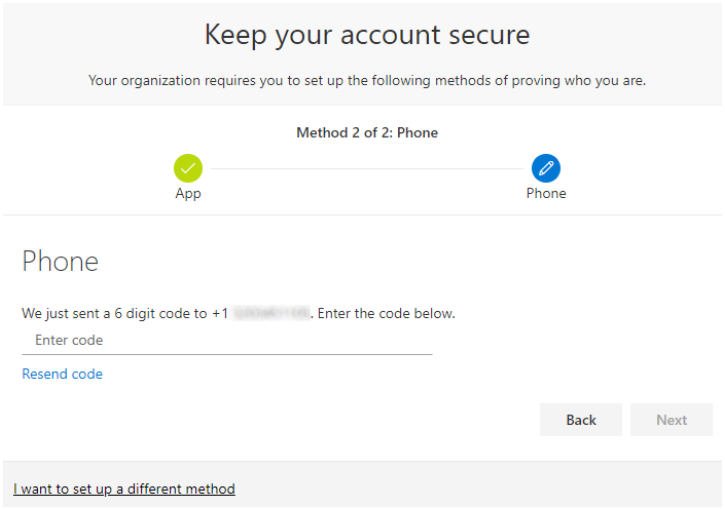


10. On the "Keep your account secure" screen on your computer, begin the setup of the second verification method. Maximus requires you to set up two verification methods to ensure continuous access to your resources. This is used as a backup method if the first (default) method that was just setup is at any point unavailable during sign-in. Choose your next method and click **Next**.

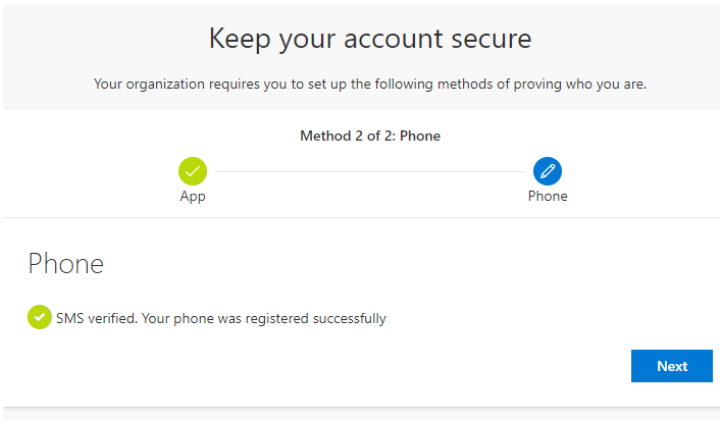


NOTE: *If a voice call or alternate email address is preferred over SMS text message, click the* ***I want to set up a different method*** *link to choose an alternate authentication method. Please also note that one of the alternate method options is to create security questions, but that method can* ***ONLY*** *be used for the self-service password reset feature, not for MFA verification.*

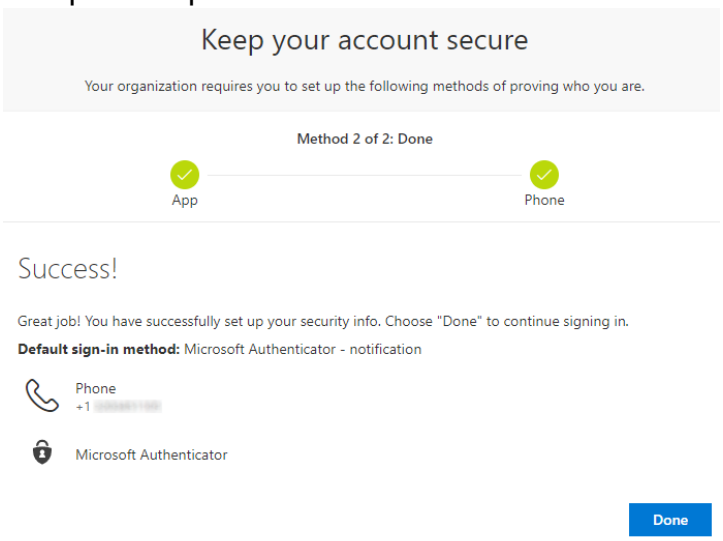
11. Enter your mobile device's phone number and click **Next**.



12. Azure will now send an SMS text message to your mobile device with a temporary 6-digit verification code. Enter the code and click **Next**.



13. Setup is complete. Click **Done**.

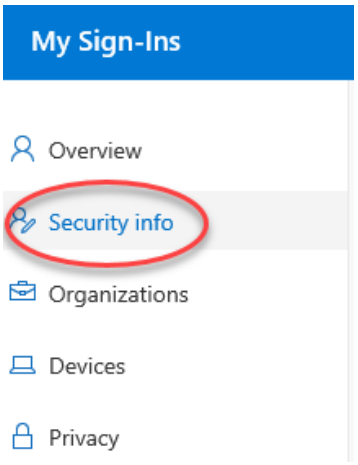


MAXIMUS

Changing MFA Verification Methods

If you later wish to change your registered MFA verification methods after completing the initial enrollment process, you may do so by completing the following steps.

1. Open your web browser and navigate to https://myaccount.microsoft.com.
2. Click on **Security info** on the left side of the screen.



3. From this page, you can add and delete registered methods as needed, as well as change which method is set as default.

   NOTE: *The default method is what Azure will first attempt to use as the second authenticator factor when you are signing in outside of a Maximus network and you receive an MFA prompt. If you have multiple methods registered, and want to use one other than your default, there is a link to click on in the MFA prompt that will allow you to choose one of the other methods available.*

User Experience

MFA Requirement Scenarios

You will be prompted to use Azure MFA when signing in to O365 in the following scenarios:

Method of access to O365 Resources	**Policy**
While physically at a Maximus location	MFA not required
Connected to Maximus VPN from any location	MFA not required
Using Maximus-managed mobile device with Intune	MFA not required
Using Maximus AWS WorkSpaces	MFA not required
From Maximus-managed computer	MFA not required *NOTE: If you are getting prompted for MFA, see FAQ for next steps.

Using personal device, not Maximus-managed, not on VPN	Use of MFA to O365 resources IS required.

Sign-In Experience

After you sign in to O365 resources using Azure MFA, your token will last for 12 hours. After that 12 hour period, you will be required to sign in again and get another token through the sign-in process. Each O365 app may prompt you to sign in separately. For example, a separate sign-in for Outlook, Teams, OneDrive, and each Office application may be required.

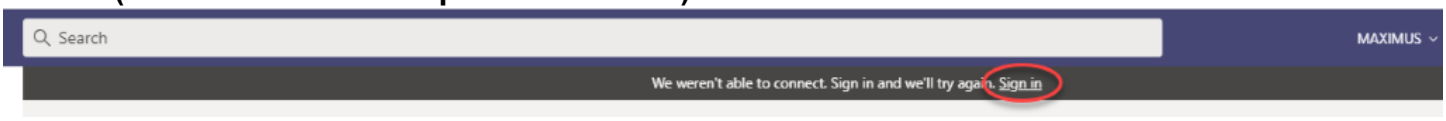
When your token expires, some apps may automatically prompt you to sign in again, but others may simply silently disconnect from the cloud service and wait for the user to manually click a button of to present the sign-in screen. When this happens, you need to either click the sign-in button for each application, or simply close and re-open the app, which also triggers a fresh sign-in.

When you sign into a browser (when you open a SharePoint site, for example), you session will persist for the full 12 hours even if you close the browser.

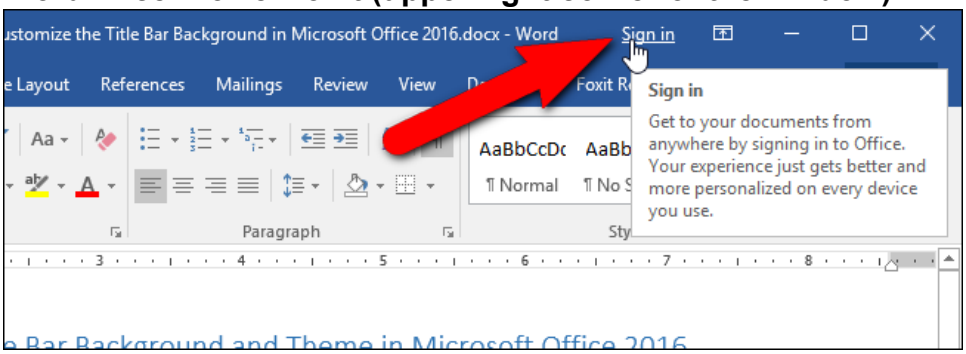
Below are some examples of app-specific buttons that a user can click on to manually launch a sign-in process to reconnect them to the cloud services:

Outlook (status bar on the lower right side of the window):

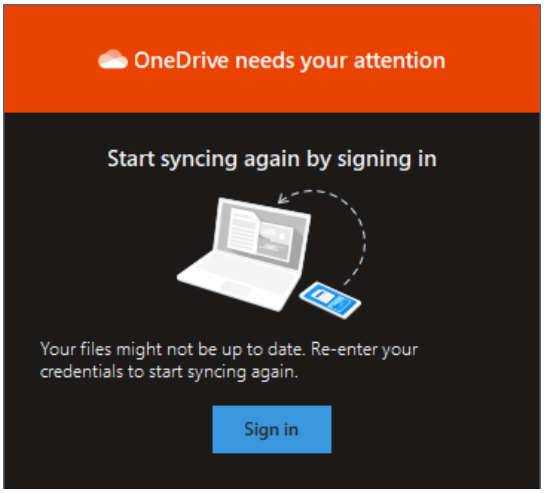
Teams (banner across the top of the window):



Word/Excel/PowerPoint (upper right corner of the window):



OneDrive (upon clicking the OneDrive icon in the taskbar, which looks like a small blue cloud):



Additional Resources

(CTRL + Click to follow the link below)

- Microsoft Documentation on Authenticator Setup
- Microsoft Documentation to Change Verification Methods
- Instructions for installing apps on different mobile devices:
    - iPhone/iPad
    - Android
    - Windows Phone