

Mobile Mailbox Access, Syncing Contacts, Adding Shared Mailboxes, and Multifactor Authentication (MFA)

This document covers the following topics that will assist you upon migration to the M365 platform:

- 1. Downloading the Outlook mobile application
 - Mobile access to your NCHS Outlook account will require use of the Outlook application. The use of the application is required to enhance network security and protection of all NCHS accounts when accessed from mobile devices. The below steps will walk you through downloading the application and adding your Nicklaus email credentials to your mobile device.
 - Native applications formerly used to access your Nicklaus account will no longer work. Users can remove their Nicklaus email credentials from formerly used native applications.
- 2. Syncing Contacts on your mobile device
- 3. Downloading shared mailboxes
 - After downloading the Outlook mobile application and adding your Nicklaus email, you can also add any shared mailboxes that you may access frequently.
- 4. Downloading Multifactor Authentication (MFA)
 - If you do not currently have MFA access, you will be required to download MFA to access your M365 account off network on personal devices.

Outlook Access on your mobile device:

iPhone

- 1. <u>Download Outlook for iOS from the iOS App Store</u> and then open it
- Enter your full email address, then tap Add Account. (Firstname.lastname@nicklaushealth.org)
- 3. Enter your network password and hit next
- 4. Use Multi-Factor Authentication to verify your identity:



Microsoft
For security reasons, we require additional information to verify your account (yourname@yourdomain.com)
We're calling your phone. Please answer it to continue. xxx-xxx-7721
Sign in with other options

- 5. Accept any prompts for permission you may receive
- 6. Swipe through the features and you're now ready to use Outlook for iOS

Android

- 1. Install the **Outlook for Android** app from the <u>Google Play Store</u> and then open it
- 2. Tap Get Started if this is your first time
- 3. Enter your full email address, then tap Add Account Firstname.lastname@nicklaushealth.org
- 4. Enter your network password and hit next
- 5. Use Multi-Factor Authentication to verify your identity:



- 6. Accept any prompts for permission you may receive
- 7. Swipe through the features and you're now ready to use Outlook for Android

To Sync your contacts on your mobile device, use the following steps:

- 1. Tap your **profile picture (photo icon)** or the **More** \equiv button. This is located in the upper left corner of the screen
- 2. Tap Settings (gear icon). This is located in the lower left corner of the screen
- 3. Under mail accounts, click on your NCHS email account. Go to **account settings** and **save contacts**



4. Switch Sync my device contacts to on

Note: If you are advised to **Allow Access to Contacts**, please follow the prompts on your device.

5. Your contacts will be available to start new chats and calls with after they are synced

To add a shared mailbox on a mobile device, use the following steps:

- 1. Sign in to your primary account in Outlook for iOS or Android
- 2. Tap the Add Account button in the left navigation pane, then tap Add a Shared Mailbox
- 3. If you have multiple accounts in Outlook Mobile, select the account that has permissions to access the shared mailbox

10:28				.ul 🤋	
<	Add Sha carlos@luc	ared Mail	box com		
Enter	the share	ed or dele	gate	email	
katri@luc	ernepub	intl.com			
	Ado	l Mailbox			
QWE		ΓΥ	U	ı c	Ρ
AS	DF	GН	J	κ	L
▲ Z	x c	VB	Ν	м	$\langle \times \rangle$
123		space		0	òo
	_		_		Ŷ

After the account setup process completes, the shared mailbox will display in your account list in Outlook for iOS or Outlook for Android

To add MFA to your mobile device, use the following steps:

If you currently have MFA on your mobile device, you will use the same application and do not need to complete the steps outlined below.



Contoso	My Profile				
Coverview Security info Organizations Devices Privacy	J	Alain Charon alan@contois.com Why can't ledi?	Security info Security info Keep your verification methods and security info up to date UPDATE INFO	Devices Disable a lost device and review your connected devices. MANAGE DEVICES >	
			Password With the source password stonger, or change it if someone eibs knows it. CHANGE PASSWORD >	Organizations Description: See all the organizations that you're a part of. MANAGE ORGANIZATIONS >	
		Sign out everywhere	Privacy B See how your organization and services are handing your data. REVIEW PRIVACY >		

1. Sign into your work account and then go to your My Account portal

Select Security info in the left menu or by using the link in the Security info pane. If you have already registered, you'll be prompted for two-factor verification. Then, select Add method in the Security info pane

Contoso	My Profile Search
Q Overview Security info	Security info These are the methods you use to sign into your account or reset your password.
 Organizations Devices 	+ Add method No items to display.
A Privacy	

- 3. On the Add a method page, select Authenticator app from the list, and then select Add
- 4. On the Start by getting the app page, select Download now to download and install the Microsoft Authenticator app on your mobile device, and then select Next. For more information about how to download and install the app, see <u>Download and install the Microsoft Authenticator app</u>:



Microsoft	Authenticator		
	Start by getting the app		
Û	On your phone, install the Microsoft Authenticator app. Download now		
	After you install the Microsoft Authenticator app on your device, choose "Next".		
	I want to use a different authenticator app		
	Cancel Next		

5. Remain on the **Set up your account** page while you set up the Microsoft Authenticator app on your mobile device:

Microsoft	Authenticator		
	Set up your account When prompted, allow notifications. Then add an account, and select "Work or school".		
Ŀ		Back	Next

 Open the Microsoft Authenticator app, select to allow notifications (if prompted), select Add account from the Customize and control icon on the upper-right, and then select Work or school account.

Note: The first time you set up the Microsoft Authenticator app, you might receive a prompt asking whether to allow the app to access your camera (iOS) or to allow the app to take pictures and record video (Android). You must select **Allow** so the authenticator app can access your camera to take a picture of the QR code in the next step. If you don't allow the camera, you can still set up the authenticator app, but you'll need to add the code information manually. For information about how to add the code manually, see Manually add an account to the app.

7. Return to the **Set up your account** page on your computer, and then select **Next**. The Scan the QR code page appears:



Microsoft Authenticator				
	Scan the QR cod	е		
	Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.			
	Can't scan image?			
		Back	Next	

- Scan the provided code with the Microsoft Authenticator app QR code reader, which appeared on your mobile device after you created your work or school account in Step 6.
- 9. The authenticator app should successfully 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 select **Can't scan the QR code** and manually enter the code and URL into the Microsoft Authenticator app. For more information about manually adding a code, see <u>Manually add an account to the app</u>.
- 10. Select **Next** on the **Scan the QR code** page on your computer. A notification is sent to the Microsoft Authenticator app on your mobile device, to test your account.

	Let's try it out		
-	Approve the notification w Resend notification	ve're sending	to your app.
		Back	Next



11. Approve the notification in the Microsoft Authenticator app, and then select **Next**. Your security info is updated to use the Microsoft Authenticator app by default to verify your identity when using two-step verification or password reset.

Microsoft Authenticator			
	Back	Next	

You will be asked to authenticate every 7 days when off network or on any personal device when using MFA