

Gillespie County

Office 365 Two-factor Verification

Roger Bunker
8-10-2021

Contents

What is Two-factor Verification?	Page 2
Access the Additional security verification page	Page 2
Set up a mobile device as your two-factor verification method	Page 4
Set up an office phone as your two-factor verification method	Page 7
Set up an authenticator app as your two-factor verification method	Page 9
Change your two-factor verification method and settings	Page 16
Manage app passwords for two-step verification	Page 20
Sign in using two-step verification or security info	Page 27

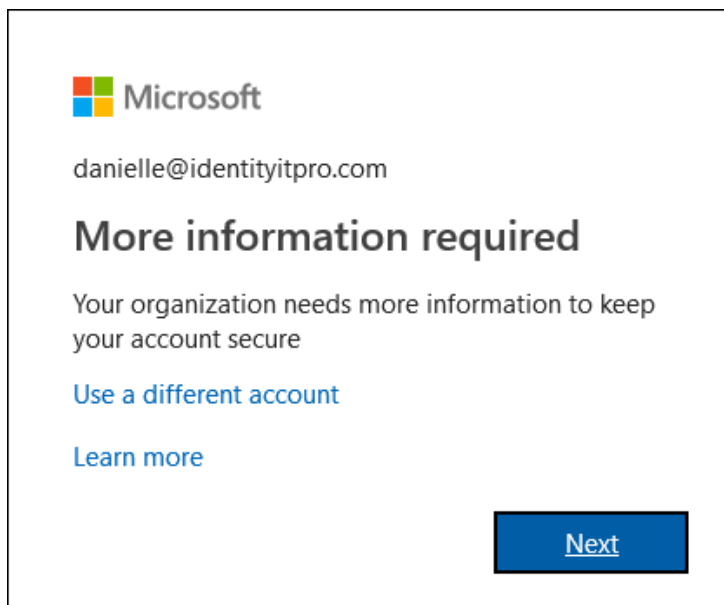
What is Two-factor Verification (MFA/2FA)?

You have received an email from IT saying Multi Factor Authentication (MFA) is being activated in Gillespie County. So, what does that mean? It means the County is taking extra steps to make sure you are who you say you are when you sign in. This extra verification, also known as two-factor authentication (2FA), is done through a combination of your username, your password, and a mobile device or phone.

Two-factor verification is more secure than just a password because it relies on two forms of authentication: something you know, and something you have with you. The something you know is your password. The something you have with you is a phone or device that you commonly have with you. Two-factor verification can help to stop malicious hackers from pretending to be you, because even if they have your password, odds are that they don't have your device, too.

Access the Additional security verification page

After IT turns on and sets up two-factor verification, you will get a prompt telling you to provide more information to help keep your account secure.



To access the Additional security verification page

1. Select **Next** from the **More information required** prompt.

The **Additional security verification** page appears.

2. From the **Additional security verification** page, you must decide which two-factor verification method to use to verify you are who you say you are after signing into your work account. You can select:

Contact method	Description
Mobile app	<ul style="list-style-type: none"> ○ Receive notifications for verification. This option pushes a notification to the authenticator app on your smartphone or tablet. View the notification and, if it is legitimate, select Authenticate in the app. Your work may require that you enter a PIN before you authenticate. ○ Use verification code. In this mode, the authenticator app generates a verification code that updates every 30 seconds. Enter the most current verification code in the sign-in screen. The Microsoft Authenticator app is available for Android and iOS.
Authentication by cell phone	<ul style="list-style-type: none"> ○ Phone call places an automated voice call to the phone number you provide. Answer the call and press the pound key (#) on the phone keypad to authenticate. ○ Text message sends a text message containing a verification code. Following the prompt in the text, either reply to the text message or enter the verification code provided into the sign-in interface.
Office phone	Microsoft Places an automated voice call to the phone number you provide. Answer the call and press the pound key (#) on the phone keypad to authenticate.

Next steps

After you have accessed the **Additional security verification** page, you must select and set up your two-factor verification method:

Set up a mobile device as your two-factor verification method

You can set up your mobile device to act as your two-factor verification method. Your mobile phone can either receive a text message with a verification code or receive a phone call.

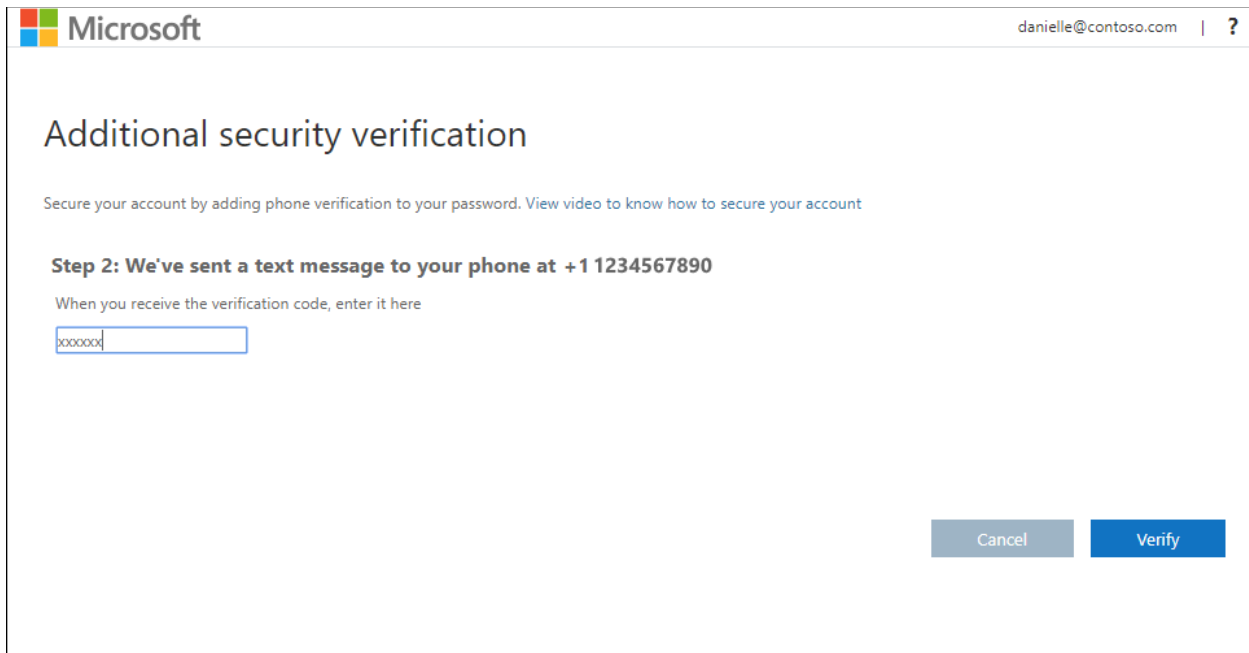
Note

If the authentication phone option is greyed out, it is possible that your organization doesn't allow you to use a phone number or text message for verification. In this case, you will need to select another method or contact your administrator for more help.

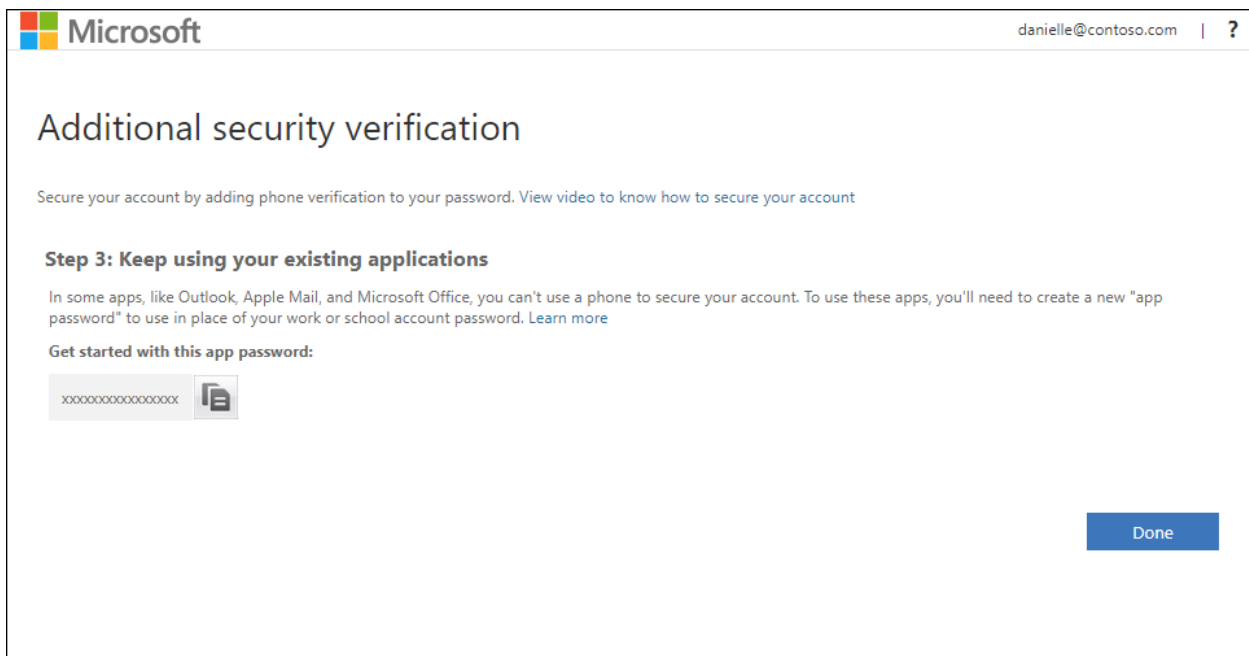
Set up your mobile device to use a text message as your verification method

1. On the **Additional security verification** page, select **Authentication phone** from the **Step 1: How should we contact you?** area, select your country or region from the drop-down list, and then type your mobile device phone number.
2. Select **Send me a code by text message** from the **Method** area, and then select **Next**.

3. Type the verification code from the text message sent from Microsoft into the **Step 2: We've sent a text message to your phone** area, and then select **Verify**.



4. From the **Step 3: Keep using your existing applications** area, copy the provided app password and paste it somewhere safe.



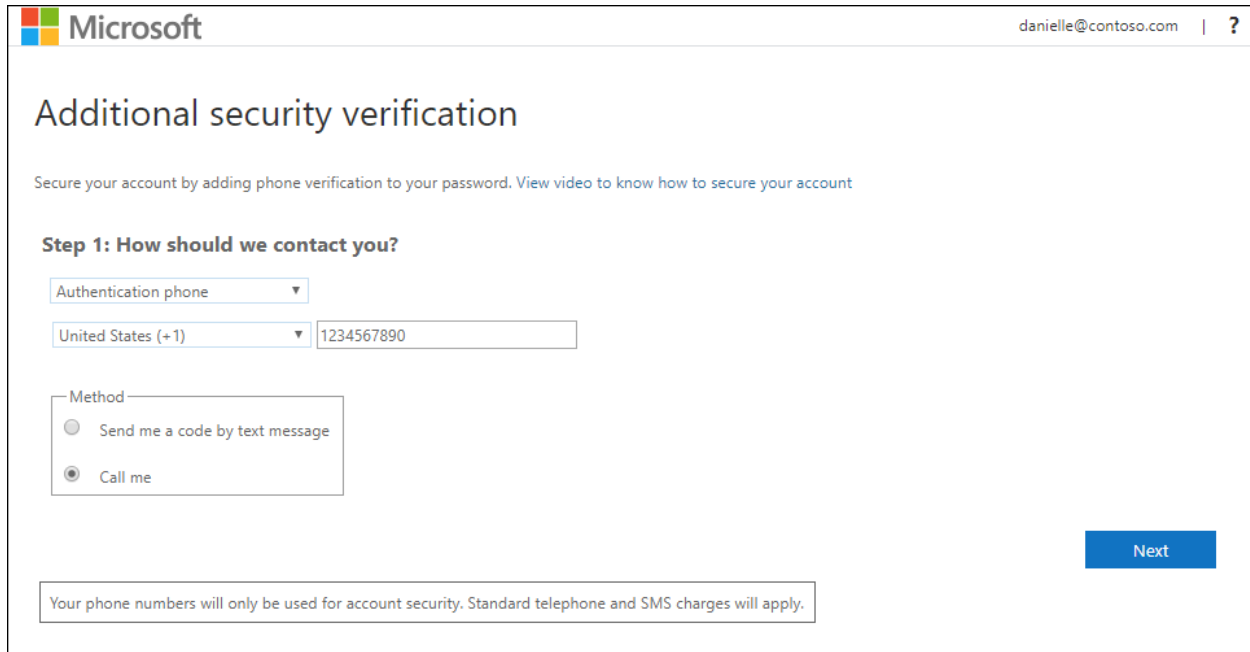
Note

For information about how to use the app password with your older apps, see [Manage app passwords](#). You only need to use app passwords if you are continuing to use older apps that don't support two-factor verification.

5. Select **Done**.

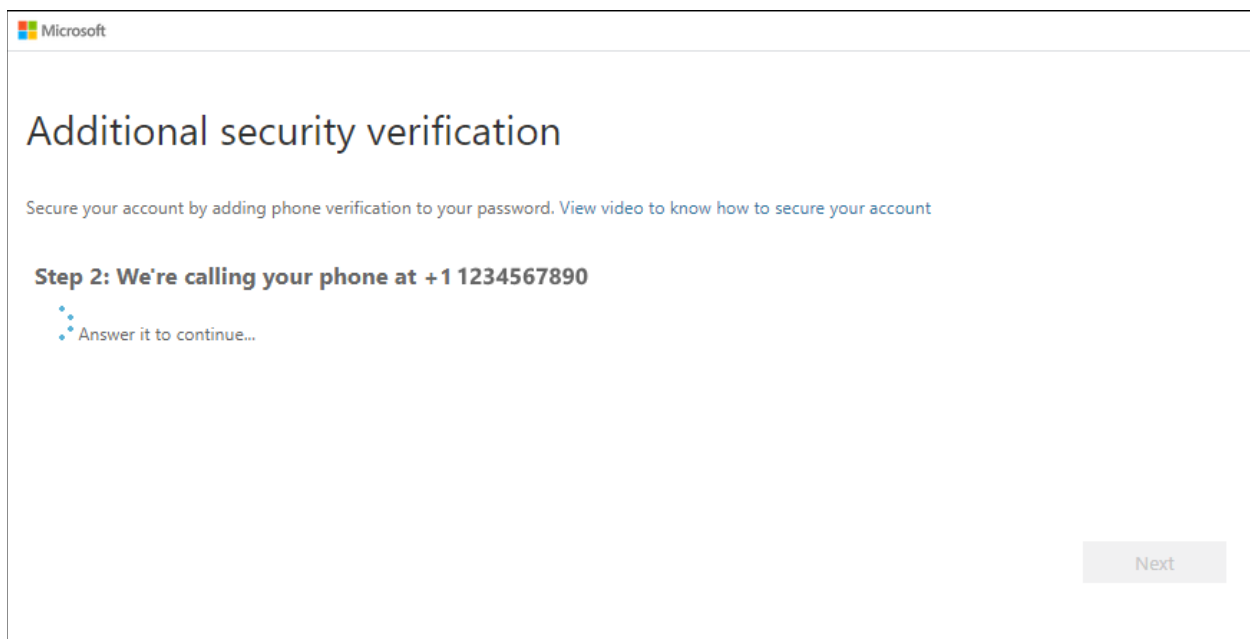
Set up your mobile device to receive a phone call

1. On the **Additional security verification** page, select **Authentication phone** from the **Step 1: How should we contact you?** area, select your country or region from the drop-down list, and then type your mobile device phone number.
2. Select **Call me** from the **Method** area, and then select **Next**.



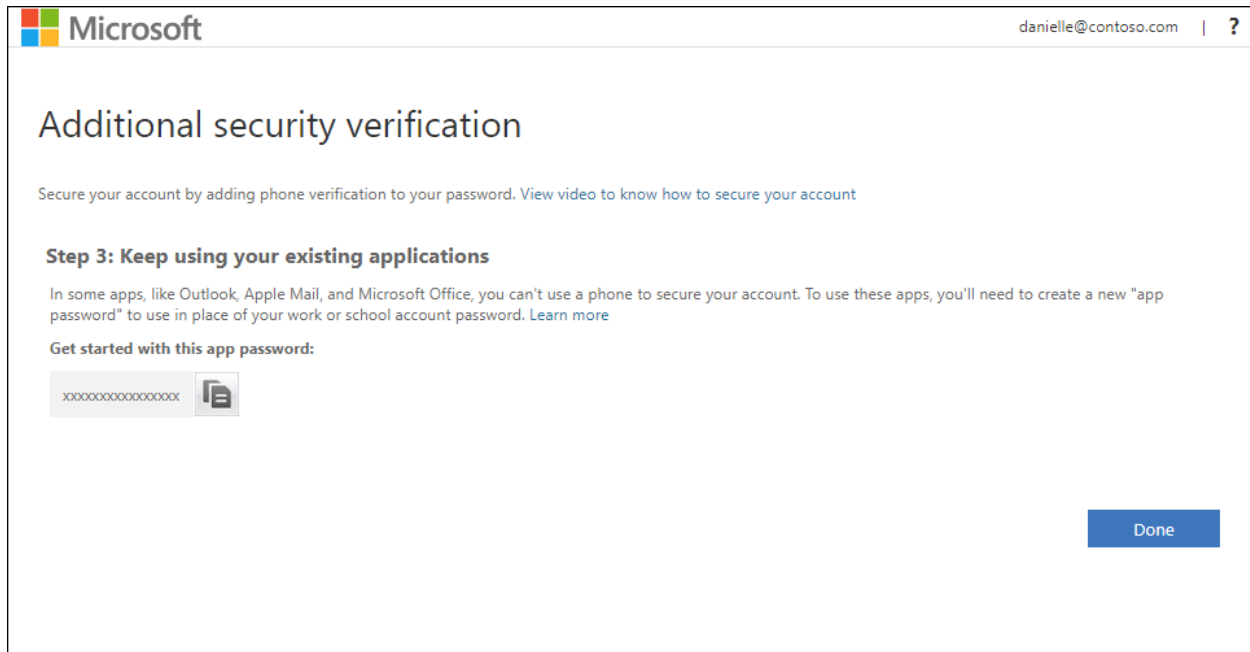
The screenshot shows the Microsoft 'Additional security verification' page. At the top left is the Microsoft logo, and at the top right is the email address 'danielle@contoso.com' and a question mark icon. The main heading is 'Additional security verification', followed by the sub-heading 'Step 1: How should we contact you?'. Below this, there are three input fields: a dropdown menu for 'Authentication phone' (set to 'Authentication phone'), a dropdown menu for 'United States (+1)', and a text input field containing '1234567890'. Below these fields is a 'Method' section with two radio button options: 'Send me a code by text message' (unselected) and 'Call me' (selected). A blue 'Next' button is located at the bottom right. At the bottom of the page, there is a small text box that reads: 'Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.'

3. You will receive a phone call from Microsoft, asking you press to the pound (#) sign on your mobile device to verify your identity.



The screenshot shows the Microsoft 'Additional security verification' page at Step 2. The heading is 'Additional security verification', followed by the sub-heading 'Step 2: We're calling your phone at +1 1234567890'. Below this, there is a small icon of a telephone handset and the text 'Answer it to continue...'. At the bottom right, there is a greyed-out 'Next' button.

4. From the **Step 3: Keep using your existing applications** area, copy the provided app password and paste it somewhere safe.



Note

For information about how to use the app password with your older apps, see [Manage app passwords](#). You only need to use app passwords if you are continuing to use older apps that don't support two-factor verification.

5. Select **Done**.

Set up an office phone as your two-factor verification method

You can set up your office phone to act as your two-factor verification method.

Note

If the Office phone option is greyed out, it is possible that your organization doesn't allow you to use an office phone number for verification. In this case, you will need to select another method or contact your administrator for more help.

Set up your office phone number as your verification method

1. On the **Additional security verification** page, select **Office phone** from the **Step 1: How should we contact you?** area, select your country or region from the drop-down list, type your office phone number, and then type your extension, if you have one.

Microsoft

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Office phone

United States (+1) Extension

Contact your admin if you need to update your office number. Do not use a Lync phone.

[Next](#)

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


2. You will receive a phone call from Microsoft, asking you to press the pound (#) sign on your office phone to verify your identity.

Microsoft

Additional security verification

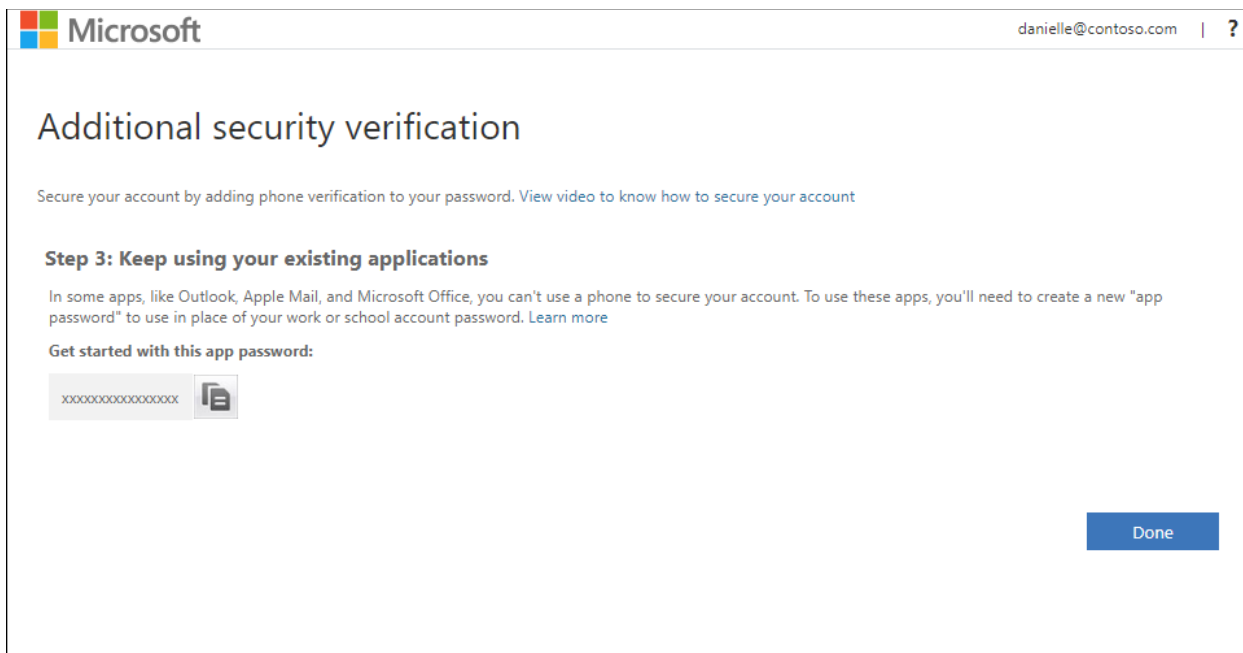
Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 2: Let's make sure that we can reach you on your Office Phone

 We are now trying to reach your office phone at +11234567890. Please follow the instructions on your phone.

[Next](#)

3. From the **Step 3: Keep using your existing applications** area, copy the provided app password and paste it somewhere safe.



Note

For information about how to use the app password with your older apps, see [Manage app passwords](#). You only need to use app passwords if you are continuing to use older apps that don't support two-factor verification.

4. Select **Done**.

Set up an authenticator app as your two-factor verification method

You can set up an authenticator app to send a notification to your mobile device or to send you a verification code as your security verification method. You aren't required to use the Microsoft Authenticator app, and you can select a different app during the set up process. However, this article uses the Microsoft Authenticator app.

Important

Before you can add your account, you must download and install the Microsoft Authenticator app. If you haven't done that yet, follow the steps in the [Download and install the app](#) article.

Note

If the Mobile app option is greyed out, it is possible that your organization doesn't allow you to use an authentication app for verification. In this case, you will need to select another method or contact your administrator for more help.

Set up the Microsoft Authenticator app to send notifications

1. On the **Additional security verification** page, select **Mobile app** from the **Step 1: How should we contact you?** area.
2. Select **Receive notifications for verification** from the **How do you want to use the mobile app?** area, and then select **Set up**.

Microsoft

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Mobile app ▼

How do you want to use the mobile app?

Receive notifications for verification

Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Set up


Next

The **Configure mobile app** page appears.

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for [Windows Phone](#), [Android](#) or [iOS](#).
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.



[Configure app without notifications](#)

If you are unable to scan the image, enter the following information in your app.
Code: 857 634 999
Url: <https://co1pfpad16.phonefactor.net/pad/648069390>

If the app displays a six-digit code, you are done!

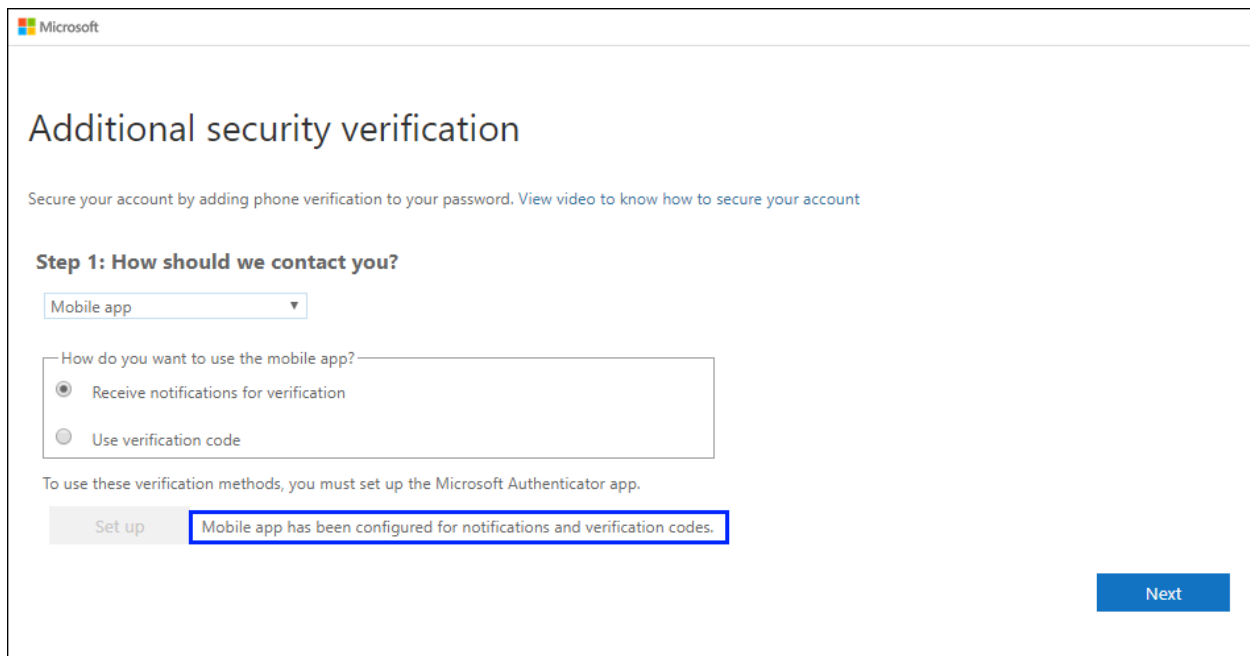
Next cancel

3. Open the Microsoft Authenticator app, select **Add account** from the **Customize and control** icon in the upper-right, and then select **Work or school account**.

Note

If this is the first time you are setting 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 will need to add the code information manually. For information about how to add the code manually, see [Manually add an account to the app](#).

4. Use your device's camera to scan the QR code from the **Configure mobile app** screen on your computer, and then choose **Next**.
5. Return to your computer and the **Additional security verification** page, make sure you get the message that says your configuration was successful, and then select **Next**.



The screenshot shows the 'Additional security verification' page. At the top, it says 'Secure your account by adding phone verification to your password. View video to know how to secure your account'. Below this is 'Step 1: How should we contact you?'. There is a dropdown menu set to 'Mobile app'. Underneath, a question asks 'How do you want to use the mobile app?' with two radio button options: 'Receive notifications for verification' (which is selected) and 'Use verification code'. A note states 'To use these verification methods, you must set up the Microsoft Authenticator app.' At the bottom, there is a 'Set up' button and a message box that says 'Mobile app has been configured for notifications and verification codes.' A blue 'Next' button is located in the bottom right corner.

The authenticator app will send a notification to your mobile device as a test.

6. On your mobile device, select **Approve**.
7. On your computer, add your mobile device phone number to the **Step 3: In case you lose access to the mobile app** area, and then select **Next**.

We strongly suggest adding your mobile device phone number to act as a backup if you are unable to access or use the mobile app for any reason.

8. From the **Step 4: Keep using your existing applications** area, copy the provided app password and paste it somewhere safe.

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 3: Keep using your existing applications

In some apps, like Outlook, Apple Mail, and Microsoft Office, you can't use a phone to secure your account. To use these apps, you'll need to create a new "app password" to use in place of your work or school account password. [Learn more](#)

Get started with this app password:

xxxxxxxxxxxxxxxxx 

Done

Note

For information about how to use the app password with your older apps, see [Manage app passwords](#). You only need to use app passwords if you are continuing to use older apps that don't support two-factor verification.

9. Select **Done**.

Set up the Microsoft Authenticator app to use verification codes

1. On the **Additional security verification** page, select **Mobile app** from the **Step 1: How should we contact you?** area.
2. Select **Use verification code** from the **How do you want to use the mobile app?** area, and then select **Set up**.

Microsoft

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Mobile app ▾

How do you want to use the mobile app?

Receive notifications for verification

Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

[Set up](#)


[Next](#)

The **Configure mobile app** page appears.

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for [Windows Phone](#), [Android](#) or [iOS](#).
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.



[Configure app without notifications](#)

If you are unable to scan the image, enter the following information in your app.

Code: 857 634 999

Url: <https://co1pfpad16.phonefactor.net/pad/648069390>

If the app displays a six-digit code, you are done!

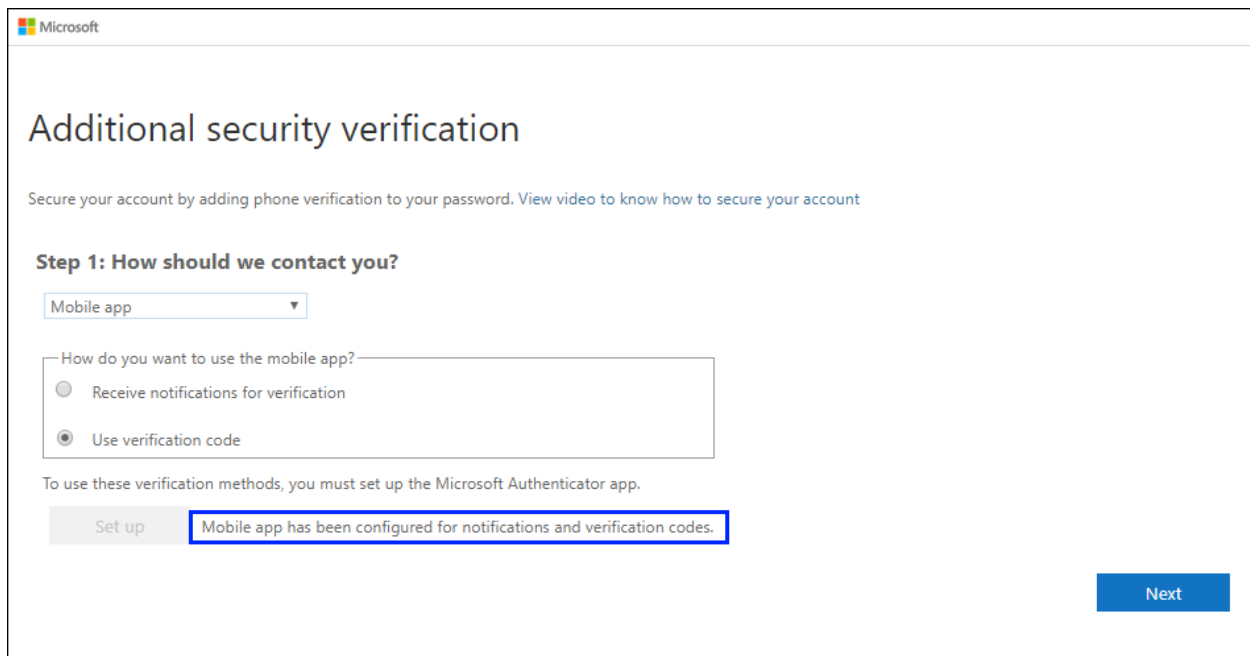
[Next](#) [cancel](#)

3. Open the Microsoft Authenticator app, select **Add account** from the **Customize and control** icon in the upper-right, and then select **Work or school account**.

Note

If this is the first time you are setting 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 will need to add the code information manually. For information about how to add the code manually, see [Manually add an account to the app](#).

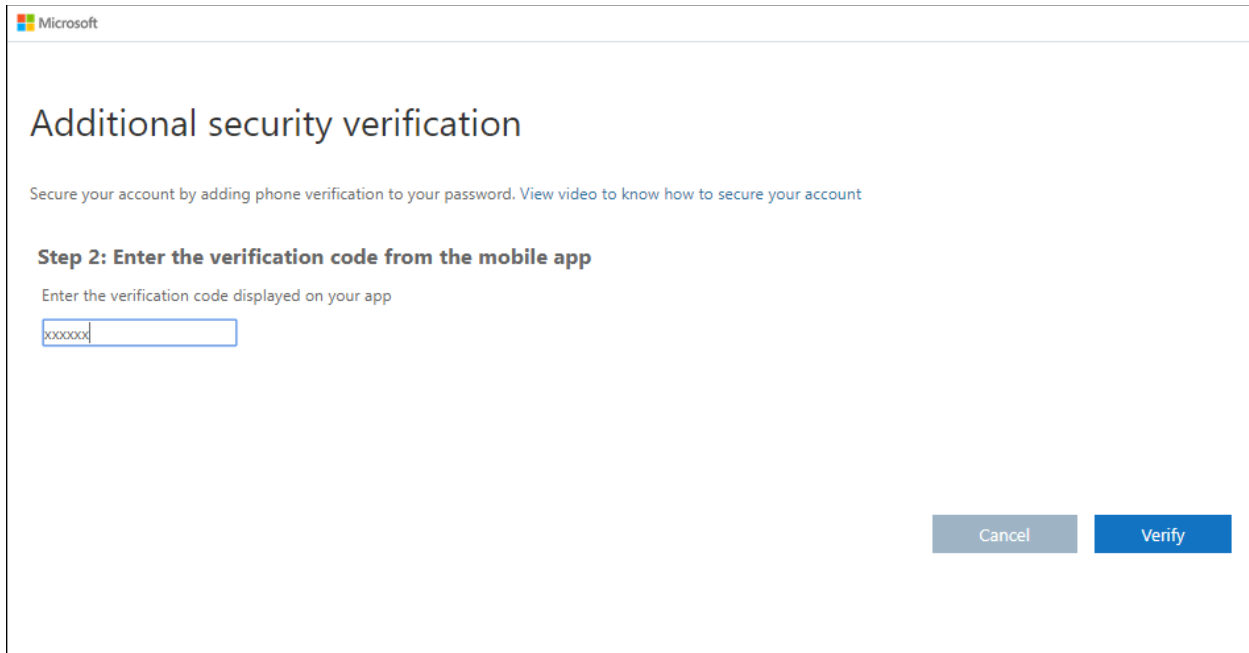
4. Use your device's camera to scan the QR code from the **Configure mobile app** screen on your computer, and then choose **Next**.
5. Return to your computer and the **Additional security verification** page, make sure you get the message that says your configuration was successful, and then select **Next**.



The screenshot shows the 'Additional security verification' page. At the top, it says 'Secure your account by adding phone verification to your password. View video to know how to secure your account'. Below this is 'Step 1: How should we contact you?'. There is a dropdown menu set to 'Mobile app'. Underneath, a question asks 'How do you want to use the mobile app?' with two radio button options: 'Receive notifications for verification' and 'Use verification code'. The 'Use verification code' option is selected. Below the options, a message states 'To use these verification methods, you must set up the Microsoft Authenticator app.' At the bottom left, there is a 'Set up' button and a status message: 'Mobile app has been configured for notifications and verification codes.' At the bottom right, there is a blue 'Next' button.

The authenticator app will ask for a verification code as a test.

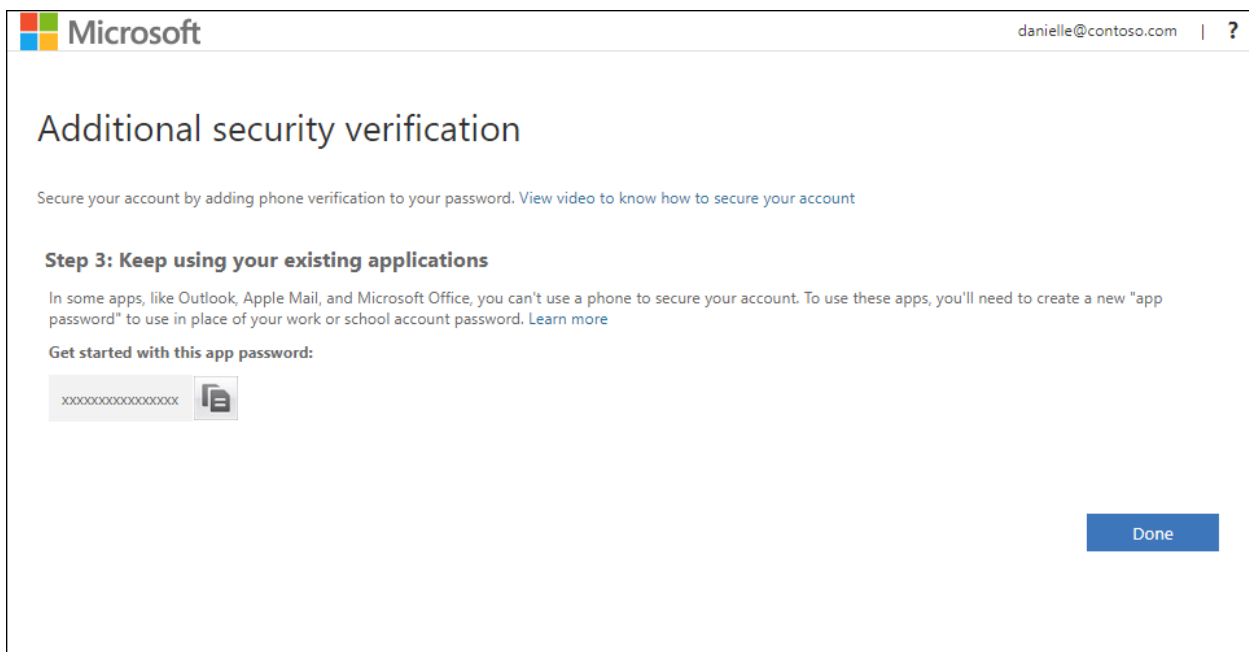
6. From the Microsoft Authenticator app, scroll down to your work or school account, copy and paste the 6-digit code from the app into the **Step 2: Enter the verification code from the mobile app** box on your computer, and then select **Verify**.



7. On your computer, add your mobile device phone number to the **Step 3: In case you lose access to the mobile app** area, and then select **Next**.

Gillespie County IT strongly suggests adding your mobile device phone number to act as a backup if you are unable to access or use the mobile app for any reason.

8. From the **Step 4: Keep using your existing applications** area, copy the provided app password and paste it somewhere safe.



Note

For information about how to use the app password with your older apps, see [Manage app passwords](#). You only need to use app passwords if you are continuing to use older apps that don't support two-factor verification.

9. Select **Done**.

Change your two-factor verification method and settings

After you set up your security verification methods for your work account, you can update any of the related details, including:

- Choosing your default security verification method.
- Adding or updating your security verification method details, like your phone number.
- Setting up a new authenticator app or deleting a device from the authenticator app.

Using the Additional security verification page

If Gillespie County IT provided you with specific steps about how to turn on and manage your two-factor verification, you should follow those instructions. Otherwise, you can get to your security verification method settings from the [Additional security verification](#) page.

Note

If what you are seeing on your screen doesn't match what's being covered in this document, it means that either Gillespie County IT has turned on the Security info (preview) experience or that Gillespie County IT has their own custom portal. For more information about the security info experience, see [Security info \(preview\) overview](#).

To get to the Additional security verification page

- Go to the [Additional security verification](#) page.

Microsoft alain@contoso.com | ?

Additional security verification App Passwords

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password. [View video to know how to secure your account](#)

what's your preferred option?

We'll use this verification option by default.

Notify me through app ▼

how would you like to respond?

Set up one or more of these options. [Learn more](#)

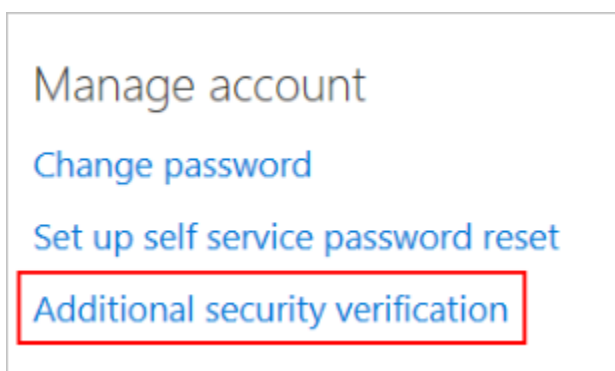
<input checked="" type="checkbox"/> Authentication phone	United States (+1) ▼	1234567890
<input type="checkbox"/> Office phone	Select your country or region ▼	
<input type="checkbox"/> Alternate authentication phone	Select your country or region ▼	Extension
<input checked="" type="checkbox"/> Authenticator app or Token	Set up Authenticator app	
Authenticator app - XX-XXXX	Delete	

[Save](#) [cancel](#)

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

If clicking that link doesn't work for you, you can also get to the **Additional security verification** page by following these steps:

1. Sign in to <https://myapps.microsoft.com>.
2. Select your account name in the top right, then select **profile**.
3. Select **Additional security verification**.



Note

For information about using the **App passwords** section of **Additional security verification** page, see [Manage app passwords for two-factor verification](#). App passwords should only be used for apps that don't yet support two-factor verification.

Change your default security verification method

After you sign into your work account with your username and password, you will automatically be presented with your chosen security verification method. Depending on your organization's requirements, this can be a notification or verification code through an authenticator app, a text message, or a phone call.

If you decide that you want to change the default security verification method you are using, you can do it from here.

To change your default security verification method

1. From the **Additional security verification** page, select the method to use from the **What's your preferred option?** drop-down list. You will see all the options, but you will only be able to choose the ones that are available to you by your organization.
 - **Notify me through app.** You will be notified through your authenticator app that you have a waiting verification prompt.
 - **Call my authentication phone.** You will get a phone call on your mobile device, asking you to verify your information.
 - **Text code to my authentication phone.** You will get a verification code as part of a text message on your mobile device. You must enter this code into the verification prompt for your work account.
 - **Call my office phone.** You will get a phone call on your office phone, asking you to verify your information.
 - **Use verification code from app.** You will use your authenticator app to get a verification code you will type into the prompt from your work account.
2. Select **Save**.

Add or change your phone number

You can add new phone numbers, or update existing numbers, from the **Additional security verification** page.

Important

Gillespie County IT strongly recommends that you add a secondary phone number to help prevent being locked out of your account if your primary phone is lost or stolen, or if you get a new phone and no longer have your original, primary phone number.

To change your phone numbers

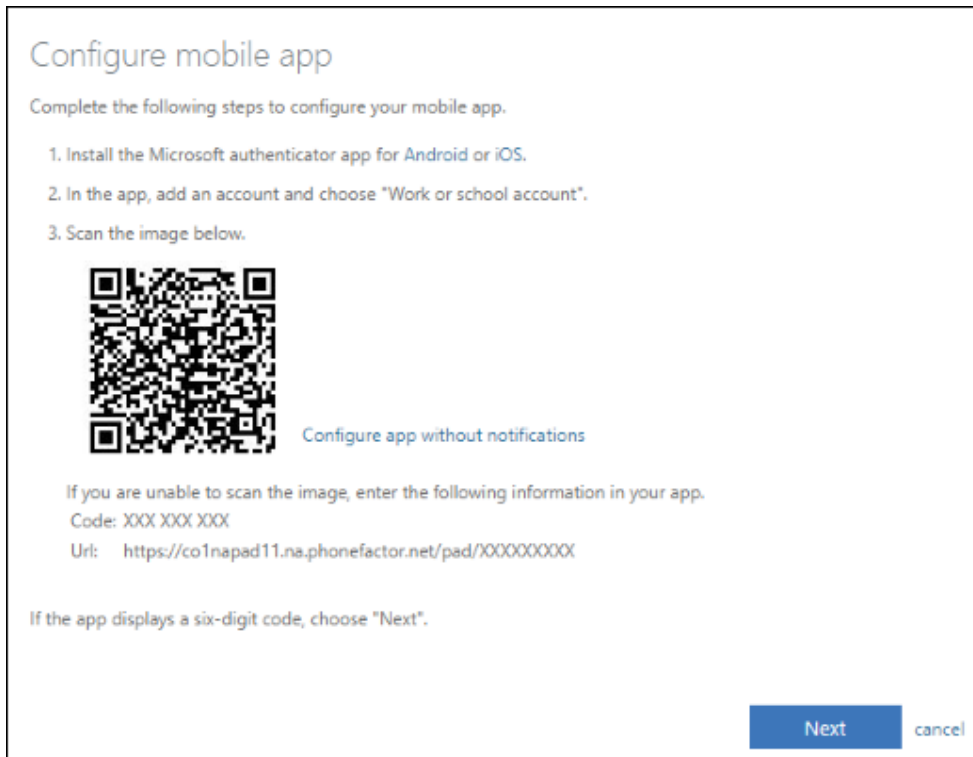
1. From the **How would you like to respond?** section of the **Additional security verification** page, update the phone number information for your **Authentication phone** (your primary mobile device) and your **Office phone**.
2. Select the box next to the **Alternate authentication phone** option, and then type in a secondary phone number where you can receive text messages or phone calls if you can't access your primary device.
3. Select **Save**.

Add a new account to the Microsoft authenticator app

You can set up your work account on the Microsoft Authenticator app for [Android](#) or [iOS](#).

If you have previously set up your work or school account in the Microsoft Authenticator app, you don't need to do it again.

1. From the **How would you like to respond?** section of the **Additional security verification** page, select the **Set up Authenticator app** button.



2. Follow the on-screen instructions, including using your mobile device to scan the QR code, and then select **Next**.

You will be asked to approve a notification through the Microsoft Authenticator app, to verify your information.

3. Select **Save**.

Delete your account or device from the Microsoft Authenticator app

You can delete your account from the Microsoft Authenticator app, and you can delete your device from your work account. Typically, you delete your device to permanently remove a lost, stolen, or old device from your account, and you delete your account to try to fix some connection issues or to address an account change, such as a new username.

To delete your device from your work account

1. From the **How would you like to respond?** section of the **Additional security verification** page, select the **Set up Authenticator app** button.
2. Select **Save**.

To delete your account from the Microsoft Authenticator app

- From the Microsoft Authenticator app, select the **Delete** button next to the device you want to delete.

Turn on two-factor verification prompts on a trusted device

Depending on your organization settings, you may see a check box that says **Don't ask again for X days** when you perform two-factor verification on your browser. If you have checked this box to stop two-factor verification prompts, and then you lose your device or your device is potentially compromised, you should turn the two-factor verification prompts back on to help protect your account. Unfortunately, you can't turn the prompts back on for a single device. You must turn the prompts on for all your devices at the same time.

To turn two-factor verification prompts back on for your devices

- From the **Additional security verification** page, select **Restore multi-factor authentication on previously trusted devices**.

The next time you sign in on any device, you will be prompted to perform two-factor verification.

Manage app passwords for two-step verification

Important

Gillespie County IT may not allow you to use app passwords. If you don't see **App passwords** as an option, they're not available in your organization.

When using app passwords, it is important to remember:

- App passwords are auto-generated, and should be created and entered once per app.
- There's a limit of 40 passwords per user. If you try to create one after that limit, you will be prompted to delete an existing password before being allowed to create the new one.

Note

Office 2013 clients (including Outlook) support new authentication protocols and can be used with two-step verification. This support means that after two-step verification is turned on, you will no longer need app passwords for Office 2013 clients. For more info, see the [How modern authentication works for Office 2013 and Office 2016 client apps](#) article.

Create new app passwords

During your initial two-factor verification registration process, you are provided with a single app password. If you require more than one, you will have to create them yourself. You can create app passwords from multiple areas, depending on how two-factor verification is set up in your organization. For more information about registering to use two-factor verification with your work account, see [Overview for two-factor verification and your work account](#) and its related articles.

Where to create and delete your app passwords

You can create and delete app passwords, based on how you use two-factor verification:

- **Your organization uses two-factor verification and the Additional security verification page.** If you are using your work account (for example, alain@contoso.com) with two-factor verification in your organization, you can manage your app passwords from the [Additional security verification page](#). For detailed instructions, see [Create and delete app passwords using the Additional security verification page](#) in this article.
- **Your organization uses two-factor verification and the Office 365 portal.** If you are using your work account (for example, alain@contoso.com), two-factor verification, and Office 365 apps in your organization, you can manage your app passwords from the [Office 365 portal page](#). For detailed instructions, see [Create and delete app passwords using the Office 365 portal](#) in this article.
- **You are using two-factor verification with a personal Microsoft account.** If you are using a personal Microsoft account (for example, alain@outlook.com) with two-factor verification, you can manage your app passwords from the [Security basics page](#). For detailed instructions, see [Using app passwords with apps that don't support two-step verification](#).

Create and delete app passwords from the Additional security verification page

You can create and delete app passwords from the **Additional security verification** page for your work or school account.

1. Sign in to the [Additional security verification page](#), and then select **App passwords**.

Microsoft alain@identityitpro.com | ?

additional security verification **app passwords**

To sign into Outlook, Lync or other apps installed on your computer or smart phone, you'll need to create an app password. When prompted by the app, enter the app password instead of your work or school account password.

You can use the same app password with multiple apps or create a new app password for each app. [How do I get my apps working with app passwords?](#)


Note: If you are an admin of a Microsoft service, we recommend not using app passwords.

[Bookmark this page](#)

[create](#)

NAME	DATE CREATED	
Initial app password20190812174937	8/12/2019	Delete

2. Select **Create**, type the name of the app that requires the app password, and then select **Next**.



Create app password

Enter a name to help you remember where you use this password.

Name:

[next](#) [Cancel](#)

3. Copy the password from the **Your app password** page, and then select **Close**.

Your app password

Name: Outlook 2010
Password: XXXXXXXXXXXXXXXXXXXX

Note: This password will not be displayed again.

copy password to clipboard

close

4. From the **App passwords** page, make sure your app is listed.

Microsoft alain@identityitpro.com | ?

additional security verification app passwords

To sign into Outlook, Lync or other apps installed on your computer or smart phone, you'll need to create an app password. When prompted by the app, enter the app password instead of your work or school account password.

You can use the same app password with multiple apps or create a new app password for each app. [How do I get my apps working with app passwords?](#)

Note: If you are an admin of a Microsoft service, we recommend not using app passwords.

[Bookmark this page](#)

create

NAME	DATE CREATED	
Initial app password20190812174937	8/12/2019	Delete
Outlook 2010	8/14/2019	Delete

5. Open the app you created the app password for (for example, Outlook 2010), and then paste the app password when asked for it. You should only have to do this once per app.

To delete an app password using the App passwords page

1. From the **App passwords** page, select **Delete** next to the app password you want to delete.

Microsoft | alain@identityitpro.com | ?

additional security verification app passwords

To sign into Outlook, Lync or other apps installed on your computer or smart phone, you'll need to create an app password. When prompted by the app, enter the app password instead of your work or school account password.

You can use the same app password with multiple apps or create a new app password for each app. [How do I get my apps working with app passwords?](#)

Note: If you are an admin of a Microsoft service, we recommend not using app passwords.

[Bookmark this page](#)

[create](#)

NAME	DATE CREATED	
Initial app password20190812174937	8/12/2019	Delete
Outlook 2010	8/14/2019	Delete

2. Select **Yes** to confirm you want to delete the password, and then select **Close**.

The app password is successfully deleted.

Create and delete app passwords using the Office 365 portal

If you use two-step verification with your work or school account and your Office 365 apps, you can create and delete your app passwords using the Office 365 portal.

To create app passwords using the Office 365 portal

1. Sign in to Office 365 and then go to the [My account page](#), select **Security & privacy**, and then expand **Additional security verification**.

My account

Security & privacy

Additional security verification
Your admin has turned on additional security verification to better secure your account.

To sign in to Office 365, you need to enter a password and reply back to the security message that is sent to your phone.
[Update your phone numbers used for account security.](#)

To sign into some apps installed on your computer or smart phone, you'll need to create an app password. When prompted by the app, enter the app password instead of your work or school account password.
[Create and manage app passwords](#)

2. Select the text that says, **Create and manage app passwords** to open the **App passwords** page.

Microsoft alain@identityitpro.com | ?

additional security verification **app passwords**

To sign into Outlook, Lync or other apps installed on your computer or smart phone, you'll need to create an app password. When prompted by the app, enter the app password instead of your work or school account password.

You can use the same app password with multiple apps or create a new app password for each app. [How do I get my apps working with app passwords?](#)


Note: If you are an admin of a Microsoft service, we recommend not using app passwords.

[Bookmark this page](#)

[create](#)

NAME	DATE CREATED	
Initial app password20190812174937	8/12/2019	Delete

3. Select **Create**, type the name of the app that requires the app password, and then select **Next**.



Create app password

Enter a name to help you remember where you use this password.

Name:

[next](#) [Cancel](#)

4. Copy the password from the **Your app password** page, and then select **Close**.

Your app password

Name: Outlook 2010
Password: XXXXXXXXXXXXXXXXXXXX

Note: This password will not be displayed again.

copy password to clipboard

close

- From the **App passwords** page, make sure your app is listed.

Microsoft | alain@identityitpro.com | ?

additional security verification app passwords

To sign into Outlook, Lync or other apps installed on your computer or smart phone, you'll need to create an app password. When prompted by the app, enter the app password instead of your work or school account password.

You can use the same app password with multiple apps or create a new app password for each app. [How do I get my apps working with app passwords?](#)

Note: If you are an admin of a Microsoft service, we recommend not using app passwords.

[Bookmark this page](#)

create

NAME	DATE CREATED	
Initial app password20190812174937	8/12/2019	Delete
Outlook 2010	8/14/2019	Delete

- Open the app you created the app password for (for example, Outlook 2010), and then paste the app password when asked for it. You should only have to do this once per app.

To delete app passwords using the App passwords page

- From the **App passwords** page, select **Delete** next to the app password you want to delete.

Microsoft alain@identityitpro.com | ?

additional security verification app passwords

To sign into Outlook, Lync or other apps installed on your computer or smart phone, you'll need to create an app password. When prompted by the app, enter the app password instead of your work or school account password.

You can use the same app password with multiple apps or create a new app password for each app. [How do I get my apps working with app passwords?](#)

Note: If you are an admin of a Microsoft service, we recommend not using app passwords.

[Bookmark this page](#)

[create](#)

NAME	DATE CREATED	
Initial app password20190812174937	8/12/2019	Delete
Outlook 2010	8/14/2019	Delete

2. Select **Yes** in the confirmation box, and then select **Close**.

The app password is successfully deleted.

If your app passwords aren't working properly

Make sure you typed your password correctly. If you are sure you entered your password correctly, you can try to sign in again and create a new app password. If neither of those options fix your problem, contact for Gillespie County IT so they can delete your existing app passwords, letting you create brand-new ones.

Sign in using two-step verification or security info

After you set up two-step verification or security info, you will be able to sign in to your account using your specified verification method.

Note

If you are still using the two-step verification experience, you will need to set up your verification methods by following the instructions in the [Set up my account for two-step verification](#) article.

If your administrator has turned on the security info experience, you will need to set your verification methods using these step-by-step articles:

- [Set up security info to use an authentication app](#)
- [Set up security info to use text messaging](#)
- [Set up security info to use a phone call](#)

- [Set up security info to use a security key](#)

Sign in using an authenticator app notification on your mobile device

1. Sign in to your account with your username and password.
2. Select **Approve** from the approval notification sent to your mobile device.

Sign in using an authenticator app code on your mobile device

1. Sign in to your account with your username and password.
2. Open your authenticator app and type the randomly generated code for your account into the **Enter code** box.

Sign in using your phone number

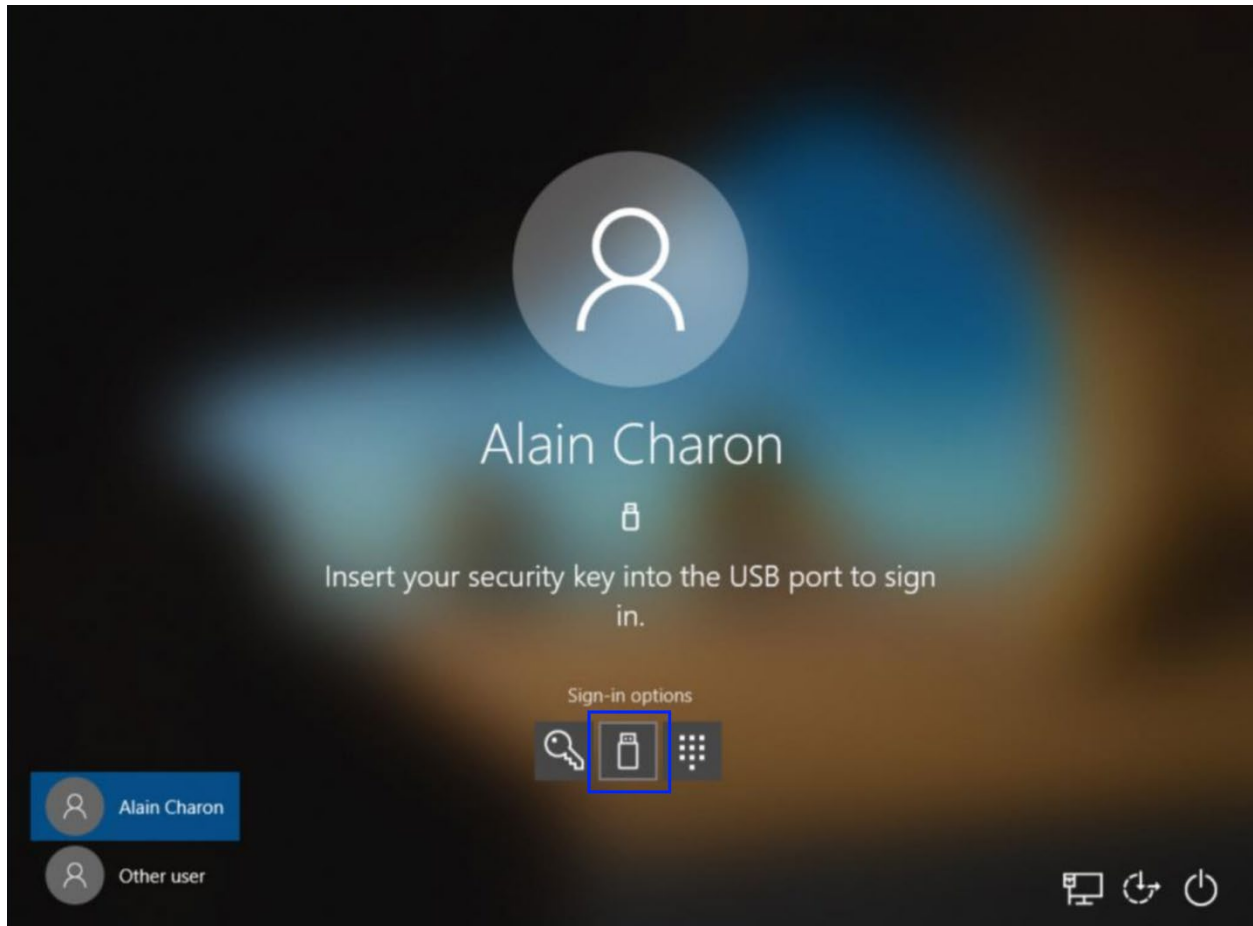
1. Sign in to your account with your username and password.
2. Answer your phone and follow the instructions.

Sign in using a text message

1. Sign in to your account with your username and password.
2. Open the text message and type the code from your text message into the **Enter code** box.

Sign in using a security key at the lock screen

1. After you have registered your security key, select the security key image from the Windows 10 lock screen.
2. Insert your security key into your device's USB port and sign in to Windows using your security key PIN.



Sign in using a security key and the Microsoft Edge browser

1. After you have registered your security key, open the Microsoft Edge browser.
2. When prompted to sign-in, insert your security key into your device's USB port and sign in to Windows using your security key PIN.



Note

For information about signing in using the Microsoft Authenticator app see the article [Sign in to your accounts using the Microsoft Authenticator app](#).

Sign in using another verification method


If for some reason you are unable to use your primary sign-in method, you can use another previously set up verification method.

1. Sign in to your account normally, and then choose the **Sign in another way** link on the **Two-step verification** page.

Microsoft

kelly@contoso.com

Enter code

 We texted your phone +X XXXXXXXXX21. Please enter the code to sign in.

Code

Don't ask again for 60 days

Having trouble? [Sign in another way](#)

[More information](#)

Verify

Note

If you don't see the **Sign in another way** link, it means that you haven't set up any other verification methods and that you will have to contact your administrator for help signing into your account. After your administrator helps you to sign in, make sure you add additional verification methods. For more info about adding verification methods, see the [Manage your settings for two-step verification](#) article.

If you see the **Sign in another way** link, but still don't see any other verification methods, you will have to contact your administrator for help signing in to your account.

2. Choose your alternative verification method and continue with the two-step verification process.
3. After you are back in your account, you can update your verification methods (if necessary). For more info about add or changing your methods, see the [Manage your settings for two-step verification](#) article.