

Follow the instructions below to setup security information and an MFA (Multi-Factor Authentication) token for Port password management services. Both methods are required to properly utilize MFA.

Prerequisites:

To complete setup, **you must have the following functional devices with you:**

- Your primary mobile device with an active phone number (to receive SMS texts).
- A computer with internet access.

IMPORTANT: Which Authentication Method Should I Use?

As the instructions indicate, **IT recommends using the Authenticator app** available for iOS and Android devices. Not only is this easy to set up and use, but it's more secure than a text message. Review steps 6—13 below for setup instructions.

Backup Authentication Methods:

It's important to have a backup method to authenticate. By default, Port employees will have a mobile device registered in as a phone authentication method if they have one. You can also add more contact numbers and methods too.

<p>1</p> <ul style="list-style-type: none"> • Visit the Port of Portland password assistance portal (https://account.portofportland.com/) using the Google Chrome, Firefox, or Safari browser (neither Microsoft Edge or Microsoft Internet Explorer function correctly). • Click on the Configure button to start the setup process for your security information. 	<div style="border: 1px solid #ccc; padding: 10px;"> <p style="text-align: center; margin: 0;">Multi-Factor Registration and Management</p> <p style="text-align: center; margin: 10px 0 0 0;">Need to register or change your security information for self-service password management and multi-factor authentication? Click below to login and configure.</p> <p style="text-align: center; margin: 10px 0 0 0;">Step-by-Step Guide</p> <div style="text-align: center; margin: 10px 0 0 0;"> <div style="background-color: #0070c0; color: white; padding: 10px 20px; display: inline-block; border-radius: 5px;">Configure</div> </div> </div>
---	---

- Sign in with your Port account information (e-mail address and password).
- On the resulting "Security info" page, you will need to do the following:
 - Add your mobile phone number (this should be the number for your primary mobile phone)
 - Setup a multi-factor authenticator app on your smart phone
- Click on the **Add method** button.

Security info

These are the methods you use to sign into your ac

Default sign-in method: Microsoft Authenticator -



 Phone

 Office phone

 Microsoft Authenticator

2

- In the "Add a method" pop-up window, click on "Choose a method" and then choose **Phone**.
 - Click "Add" to continue adding your phone number.
- Note:** Some of this information may be pre-populated so please confirm the listed number/devices are correct.
- Select Change to edit existing entries if needed.

Add a method

Which method would you like to add?

Phone

Cancel

Add

3

- In the resulting "Phone" pop-up window, enter your mobile phone number.
- Ensure that the "Text me a code" option is checked, and then click **Next**.

Phone

Which phone number would you like to use?

+1  5558675309

Text me a code

Call me

Cancel

Next

- 4
- A code will be sent to your phone via text message.
 - Type the code into the "Phone" pop-up and click on **Next**.

Phone

We just sent a code to +1 5558675309

[Resend code](#)

Back
Next

- 5
- If you receive a "SMS verified successfully" message, click on "Done" and then move to step 6.
 - If you do not receive this message, verify that you have entered the correct phone number and/or the correct SMS code, and then try again.

Phone

✔ SMS verified successfully

Done

- 6
- Now that you have added your primary phone number, you will now setup your MFA token.
 - Click on the "Add method" button.
 - In the resulting "Add a method" pop-up window, click on "Choose a method" and then choose **Authenticator app**.
 - Click **Add** to continue setting up your MFA token.

Add a method

Which method would you like to add?

Cancel
Add

7

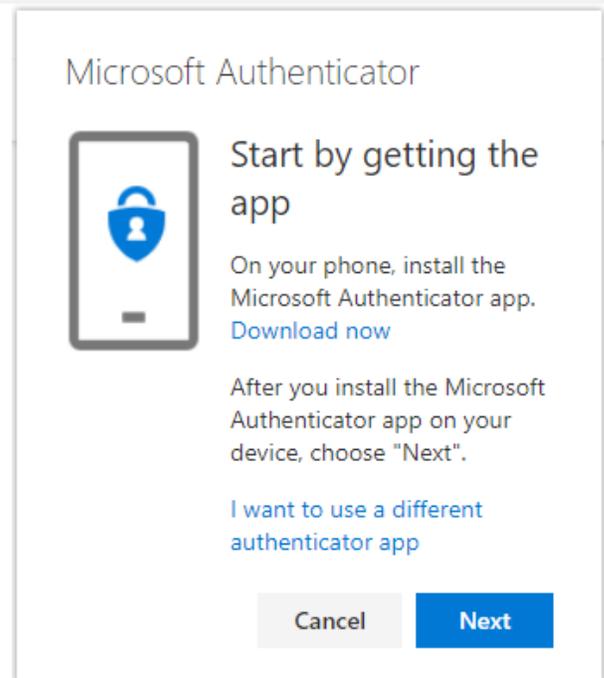
- **Install the Microsoft Authenticator app on your phone.** Follow the instructions below that apply to your device:

Corporate and BYOD iOS and Android Devices:

- Open the Apps@Work app (Port managed iOS devices) or Enterprise Google Play store (Port managed Android devices) on your device and select the VPN category.
- Install the Microsoft Authenticator App.

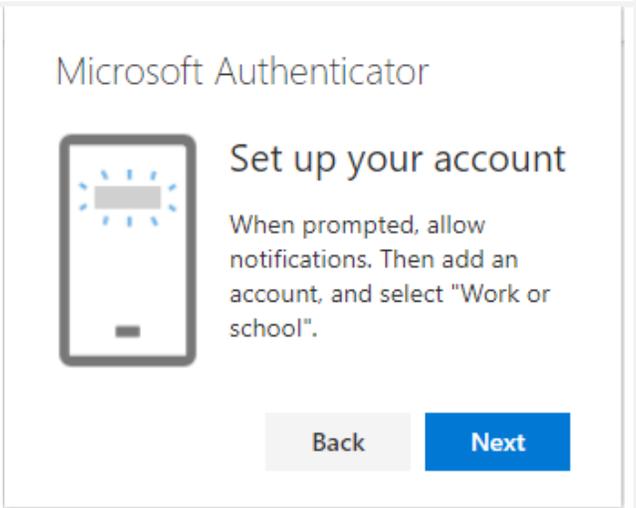
Personal Mobile Devices:

- If you are using a device that is not managed by the Port's Mobile Device Management (MDM) system, download the app through the Apple App Store (iOS devices) or the Google Play Store (Android devices).
- If you are unsure how to install the Microsoft Authenticator app on your phone, follow the instructions in the Microsoft Authenticator pop-up message.
- Once you have successfully installed the Microsoft Authenticator app on your phone, **click Next on the registration website.**



8

- Open the Microsoft Authenticator app on your mobile device.
- If prompted, select **Allow notifications**.
- Find the option in the app to **"Add account"**.
- Choose **Work or school account** on the next screen. This will bring up a camera window.
- **On your PC**, click **Next** in the Microsoft Authenticator window that displays.



- 9
- A new window will display a QR code.
 - Scan the QR code with your phone using the camera window to locate the code on screen.
 - Your phone should tell you that the token was setup successfully, and you should see a token in your app with the title "Port of Portland".
 - Once your token is setup, click **Next**.
 - **If the setup process appears to stall after you've scanned the QR code, refresh your browser and go through the token setup again starting at #7**

Microsoft Authenticator



Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

[Can't scan image?](#)

- 10
- You will be sent a pop-up message on your phone.
 - Click **Approve** on the pop-up.
 - If you do not receive a pop-up, click on "Resend notification" on your PC to get another message sent.
- NOTE:** Your phone must be connected to the Internet to properly receive the notification.
- Select **Done**.

Microsoft Authenticator



Let's try it out

Approve the notification we're sending to your app.

[Resend notification](#)

- 11
- If the approval completed successfully, you should receive the message "Notification approved".
 - Click **Done** on the message.

Microsoft Authenticator



Notification approved

- 12
- On your account security info page, verify that you now have an entry for "Phone" and for "Microsoft Authenticator" in the Security Info screen.
 - Once verified, click on **Change** next to the "Default sign-in method" option.

Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Microsoft Authenticator - notification [Change](#)

- 13
- In the resulting "Change default method" pop-up, choose **Microsoft Authenticator – notification** in the drop-down menu, and then click **Confirm**.
 - Once this step is complete, you are now setup and ready to use multi-factor authentication.

Change default method

Which method would you like to use to sign in?

Microsoft Authenticator - notificati...

Back

Confirm