AEROTRIX LABS

SUPPORT | GUIDES | SOLUTIONS

Microsoft 365

First Sign-In

MS365 > USER ONBOARDING

A step-by-step guide to signing in to your Microsoft 365 account for the first time and setting up your profile.

⏱️ Estimated time: 5–10 minutes

📊 Suitable for: All users

Arun Dutta-Plummer
AEROTRIX LABS LTD | SUPPORT.AEROTRIXLABS.COM

Table of Contents

Before you start ***2***

Where to find support ***2***

Step 1: Sign in to Microsoft 365 ..... ***3***

1.1 – First Log in **3**

1.2 – Changing the temporary password **4**

1.3 – Next Steps **5**

Step 2: Multi-Factor Authentication (MFA) Setup ***6***

2.1- Downloading the Microsoft Authenticator Application **6**

2.2- Linking Authenticator to your account **6**

2.3 – Accepting the first Authenticator MFA Code **7**

2.4 – Next Steps **7**

Welcome! This guide will help you sign in to your new Microsoft 365 account and setup two-factor authentication with the Authenticator mobile application.

Before you start

Before you begin this guide, you will need the following:

- Your new Microsoft 365 email address (e.g. yourname@yourcompany.com)
- Your temporary password (provided by your IT administrator)
- A smartphone for Multi-Factor Authentication (MFA)

Where to find support

Below are some ways to get some help if you cannot complete the actions within this guide.

The list is defined in order of priority:

1. Consult any internal company SOP documents
2. Raise the issue with an internal IT Administrator
3. Visit support.aerotrixlabs.com and search the Knowledge Base
4. Open a support ticket at support.aerotrixlabs.com to get in contact with your company's account manager

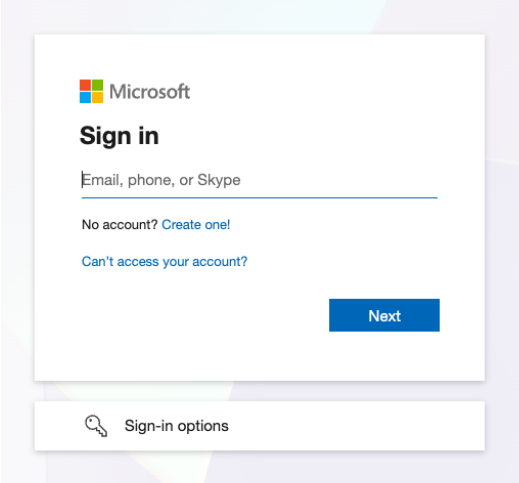
Step 1: Sign in to Microsoft 365

In this section, you will locate your username, log into your account for the first time, and change your password from the temporary one to something more secure that follows your company's password policies.

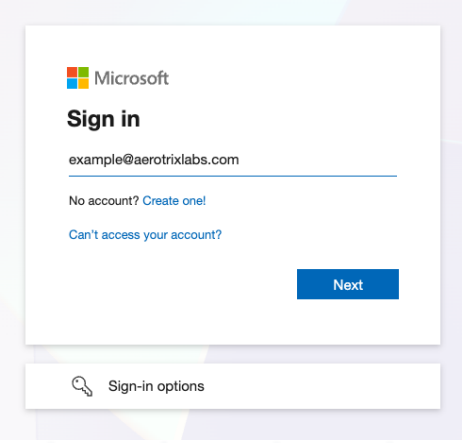
1.1 – First Log in

Firstly, open your web browser of choice (Google Chrome, Microsoft Edge, Safari, etc) and then head over to outlook.office.com.

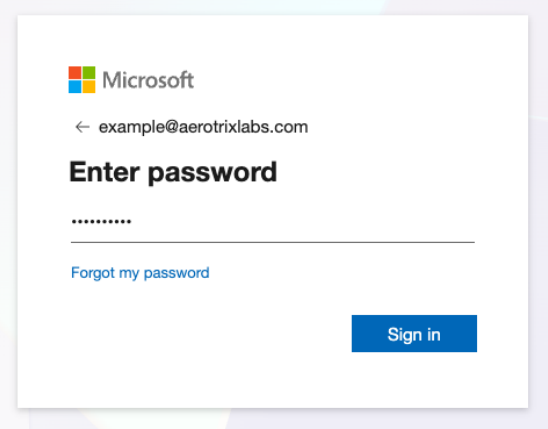
You will be redirected to a page like below:



Enter your new email address in the box (e.g. name@company.com) and click "Next".



Enter your temporary password (provided by your IT administrator) and click "Sign In". Ensure you have a note of your temporary password as it is required in the next step.



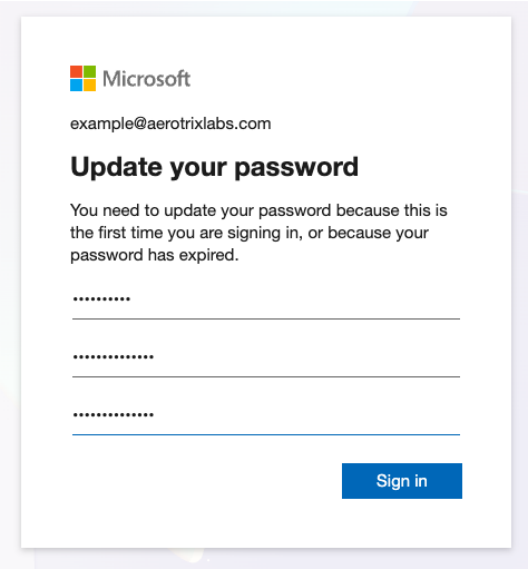
1.2 – Changing the temporary password

As this is your first time logging into the account, you will be presented with a form to update your password. Microsoft requires your password to have a minimum of 8 characters (and a maximum of 256), and a mixture of Uppercase, Lowercase, numbers, and symbols (3 of these 4 are required).

Microsoft also bans commonly used or easily guessed passwords such as “password” or even a password that includes your name.

Please Note: Your IT system administrator may have set other password policies such as history requirements, expiration dates, and other requirements. Speak to them if you cannot successfully create a legal password.

After a suitable password has been set, click “Sign In”.



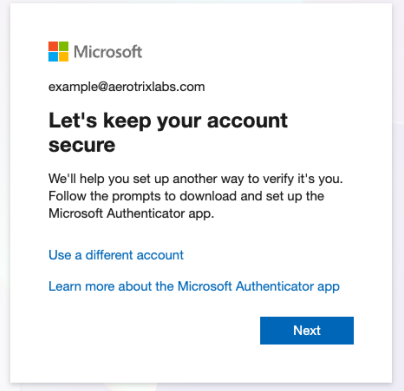
1.3 – Next Steps

You have now completed Step 1 of setting up your new Microsoft Business account. We have found our username (email address), logged in, and changed our password from the default temporary password to a legal one based on your organizational Policies.

Next you will secure your account using Multi-Factor Authentication (MFA)

Step 2: Multi-Factor Authentication (MFA) Setup

After successfully logging into your account for the first time and updating your password, you will be presented with a MFA setup message. Click the “Next” button.



2.1- Downloading the Microsoft Authenticator Application

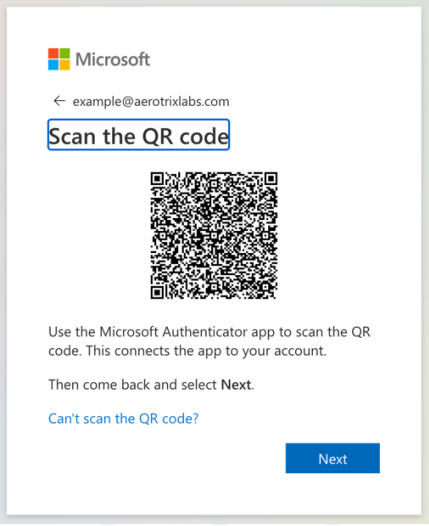
Download the Microsoft Authenticator application on your mobile device (from either the Apple App Store or the Google Play Store).

App Store: https://apps.apple.com/us/app/microsoft-authenticator/id983156458

Play Store: https://play.google.com/store/apps/details?id=com.azure.authenticator

2.2- Linking Authenticator to your account

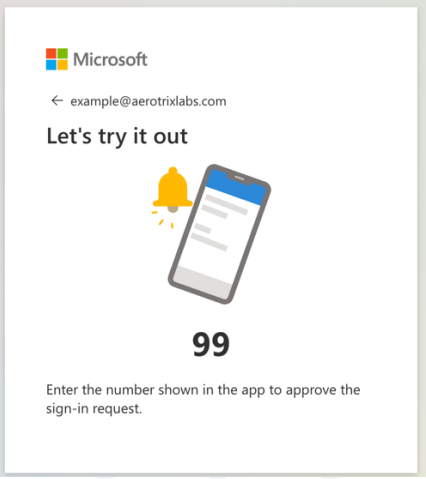
In the Authenticator app, click the blue QR code icon in the bottom right corner and scan the QR Code presented to you by the setup page. Then click “Next”.



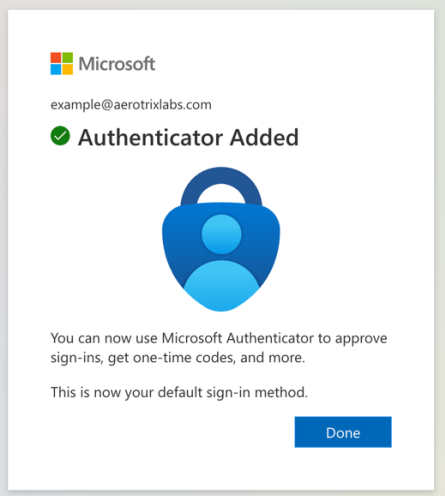
2.3 – Accepting the first Authenticator MFA Code

Microsoft will then present you with a 2 digit number code and send a notification to your authenticator app. You must enter this code into the prompt and click “Yes”.

Important Note: If you did not request an authenticator code and think the request if fraudulent, click the “No, it’s not me” button to ensure that login request is shut down. Your internal IT department, nor MSP, will ever ask you to input an authenticator code to approve a login request.



Upon successful completion of the first authenticator request, you will be presented with a message that everything is set up and the authenticator app has been set as your default MFA provider. You can update this later in your account settings.



2.4 – Next Steps

You have now successfully found your account details, logged into it, changed your password, and setup Multi-Factor Authentication (MFA). Your account is now officially set up. The next steps below are optional and allow you to customize your experience with your new account and are not mandatory to follow.