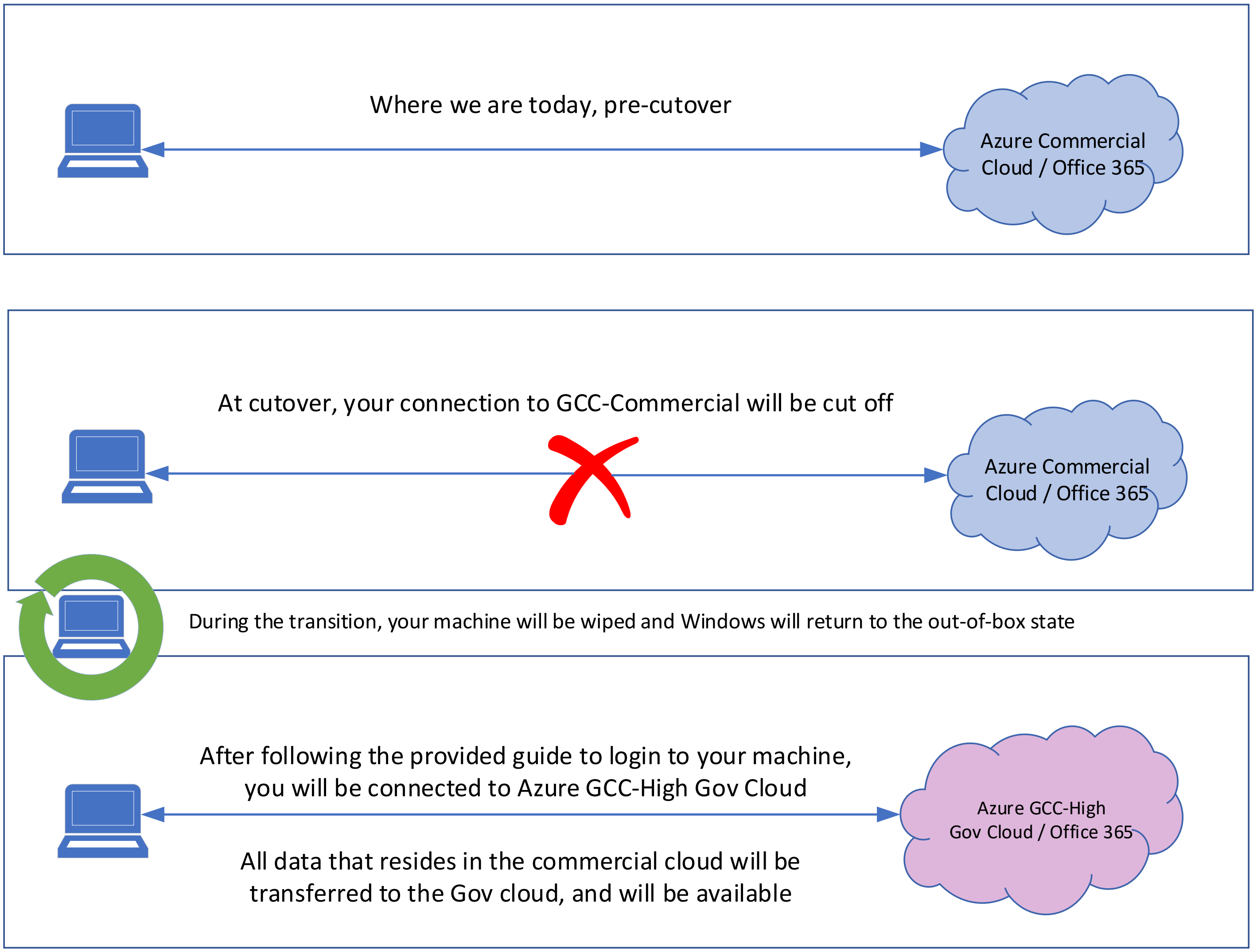
Informational Sheet #1

Microsoft Azure GCC High Transition

Q: What is happening here?

Today Trideum operates in the Azure commercial cloud. To satisfy data protection requirements imposed by the DoD, we are moving from an Azure commercial cloud to Azure GCC-High Gov Cloud. The following steps are necessary for a clean transition.



Where we are today, pre-cutover

At cutover, your connection to GCC-Commercial will be cut off

During the transition, your machine will be wiped and Windows will return to the out-of-box state

After following the provided guide to login to your machine, you will be connected to Azure GCC-High Gov Cloud

All data that resides in the commercial cloud will be transferred to the Gov cloud, and will be available

Azure Commercial Cloud / Office 365
Azure Commercial Cloud / Office 365
Azure GCC-High Gov Cloud / Office 365

See detailed step by step guidance in the following pages

Windows Workstation Fresh Start Walkthrough

Follow the 22 steps below to successfully complete a fresh start of your Tridem Computer. These instructions use screenshots from a Windows 11 laptop. The steps for a Windows 10 system device are similar.

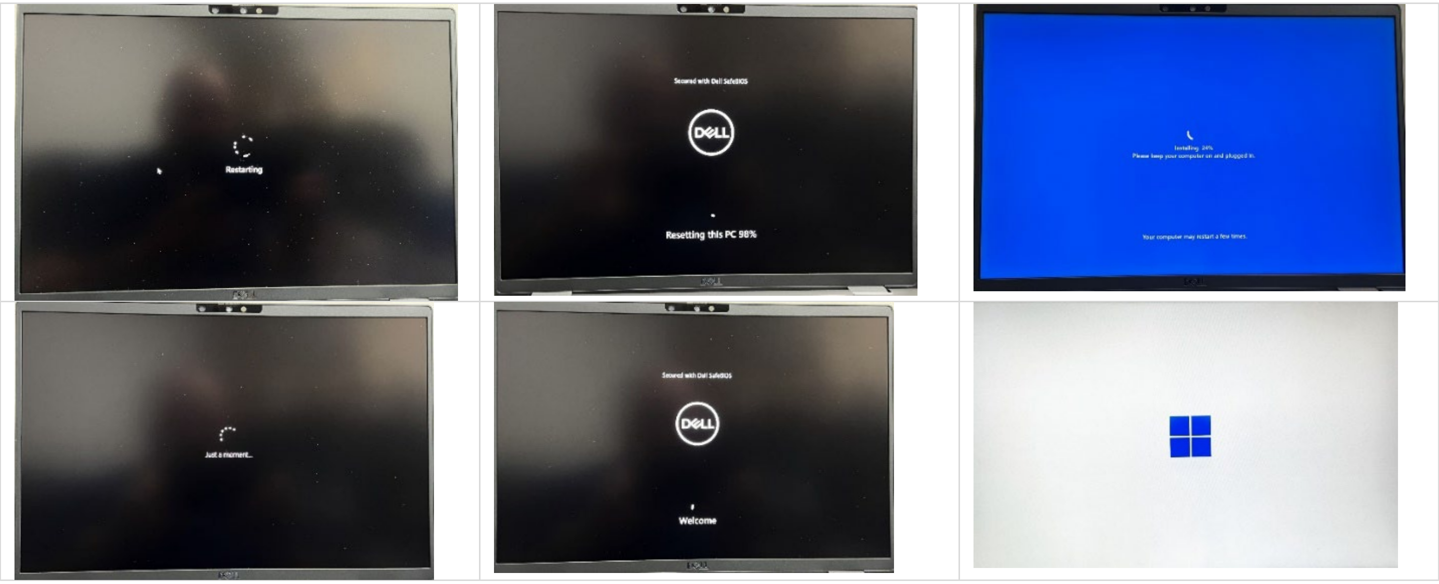
At the Work Freeze (3pm ET 6 September 2024), IT will issue a command to reinstall Windows on all Trideum computers.

IMPORTANT: This will erase and wipe all data on the computer.

Note for users with Software Development Machines and non-Windows users The wipe command only erases the hard drive where the Windows OS resides, if you have a second data drive it will not be impacted – Machines running Linux as the only OS will not be wiped – Apple machines will not be wiped*

Windows developers see additional bitlocker step at the end of this guide

The pictures below show what you can expect your device to look like as it completes the reinstall Windows command.


Restarting
Secured with Dell SafeBIOS
Resetting this PC 98%
Installing 24%
Please keep your computer on and plugged in.
Your computer may restart a few times.
Just a moment...
Secured with Dell SafeBIOS
Welcome

Once the machine has successfully reloaded you will see the screen shown in step 1.

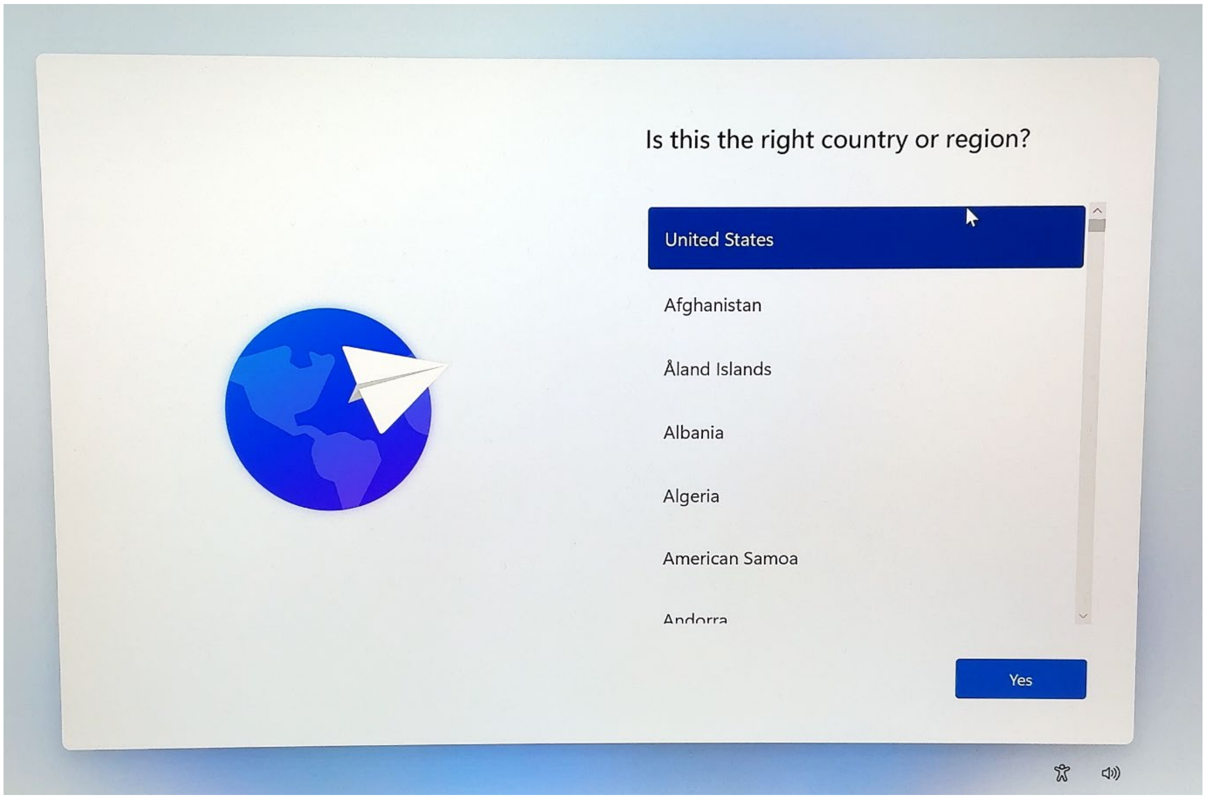
Important: Leave the machine on this screen until Monday 9/9/24

Important: Leave the machine on this screen until Monday 9 September 2024

Step #1: Select United States and click **Yes**

The screen pictured below will ask about your country or region.

1



Is this the right country or region?

United States

Afghanistan

Åland Islands

Albania

Algeria

American Samoa

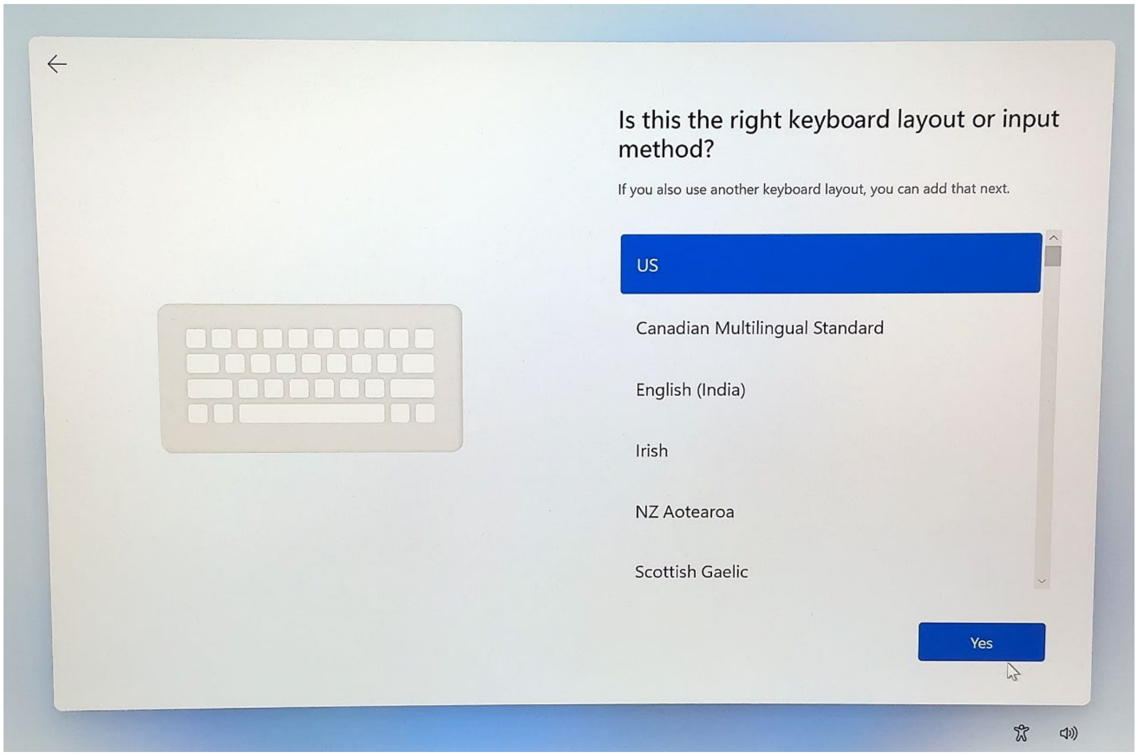
Andorra

Step 2 – Keyboard 1

Step #2: Select US and click **Yes**

The screen pictured below will ask about keyboard layout.

2



Is this the right keyboard layout or input method?

If you also use another keyboard layout, you can add that next.

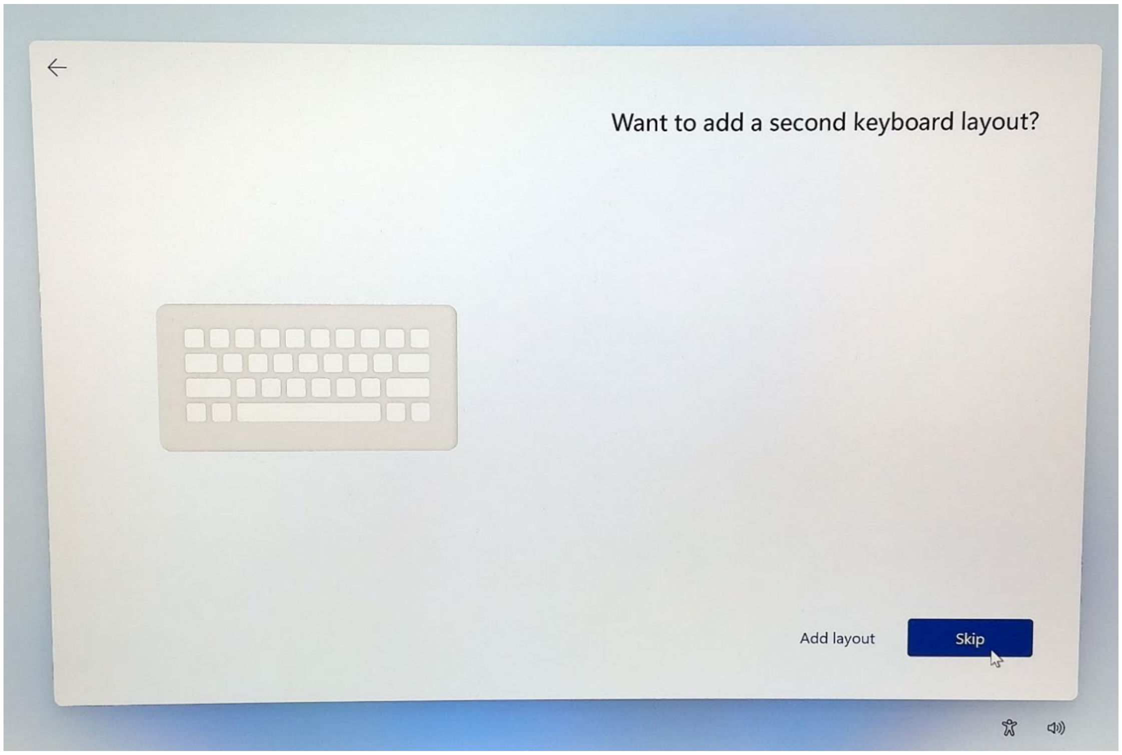
- US
- Canadian Multilingual Standard
- English (India)
- Irish
- NZ Aotearoa
- Scottish Gaelic

Step 3 – Keyboard 2

Step #3: Select **Skip** to continue

The screen pictured below will ask about a second keyboard.

3



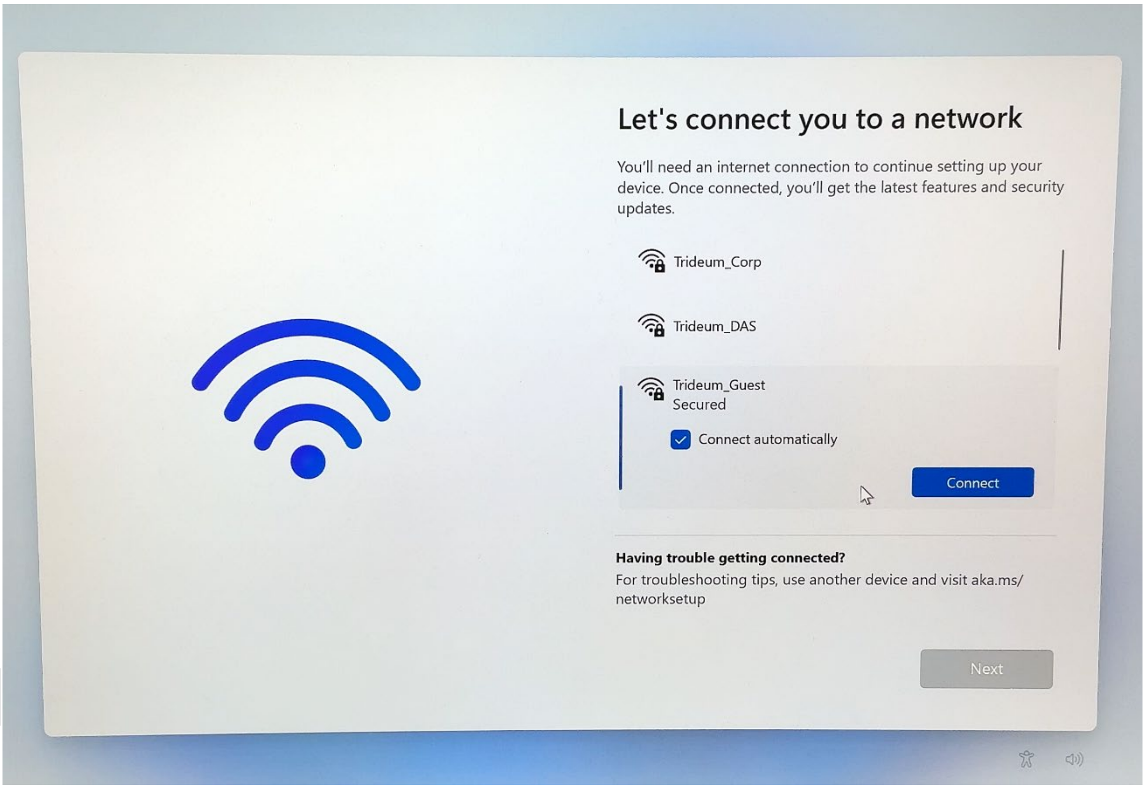
Want to add a second keyboard layout?

Step 4 –Network

<u>Step #4:</u> Choose **Trideum_Guest** if at a Trideum office or select your home network, enter the password and select **Next**

The screen pictured below will ask you to connect to a network.

4



Let's connect you to a network

You'll need an internet connection to continue setting up your device. Once connected, you'll get the latest features and security updates.

- Trideum_Corp
- Trideum_DAS
- Trideum_Guest
Secured

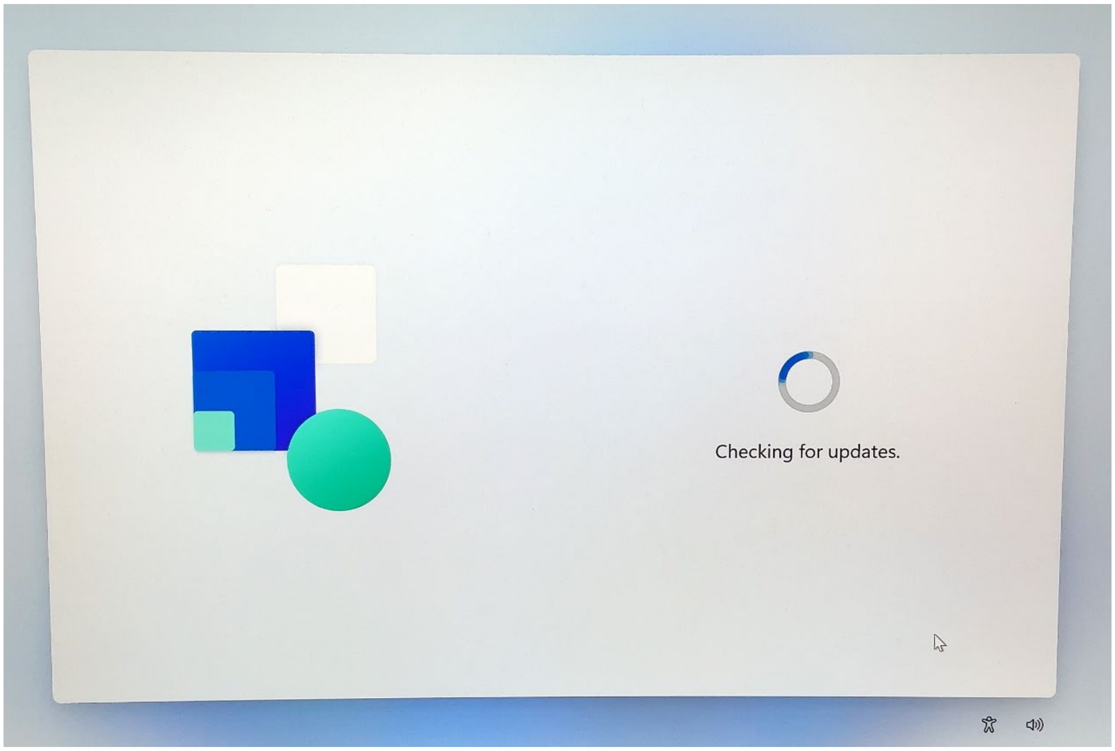
☑ Connect automatically

Having trouble getting connected?
For troubleshooting tips, use another device and visit aka.ms/networksetup

Step #5: Updates

At the screen pictured below the computer will check for updates to apply once connected to a network.

5

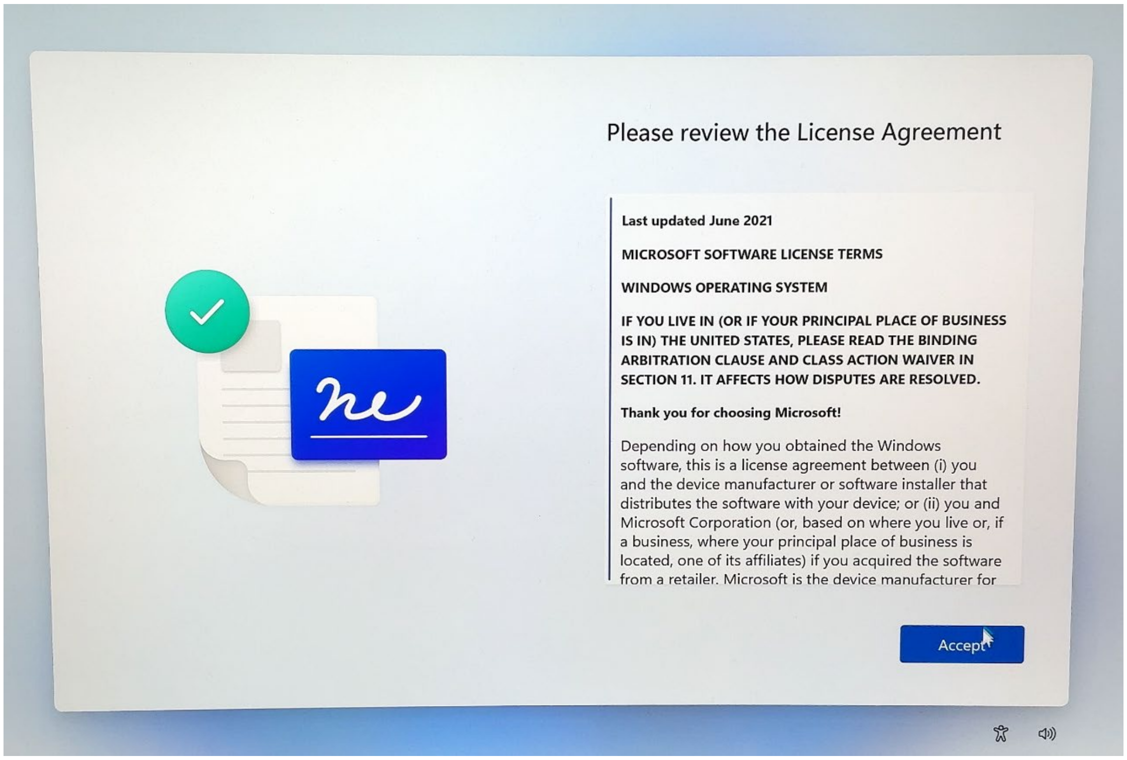


Checking for updates.

<u>Step #6:</u> Select **Accept** to continue

The screen pictured below will ask you to accept the Microsoft License agreement.

6



Please review the License Agreement

Last updated June 2021

MICROSOFT SOFTWARE LICENSE TERMS

WINDOWS OPERATING SYSTEM

IF YOU LIVE IN (OR IF YOUR PRINCIPAL PLACE OF BUSINESS IS IN) THE UNITED STATES, PLEASE READ THE BINDING ARBITRATION CLAUSE AND CLASS ACTION WAIVER IN SECTION 11. IT AFFECTS HOW DISPUTES ARE RESOLVED.

Thank you for choosing Microsoft!

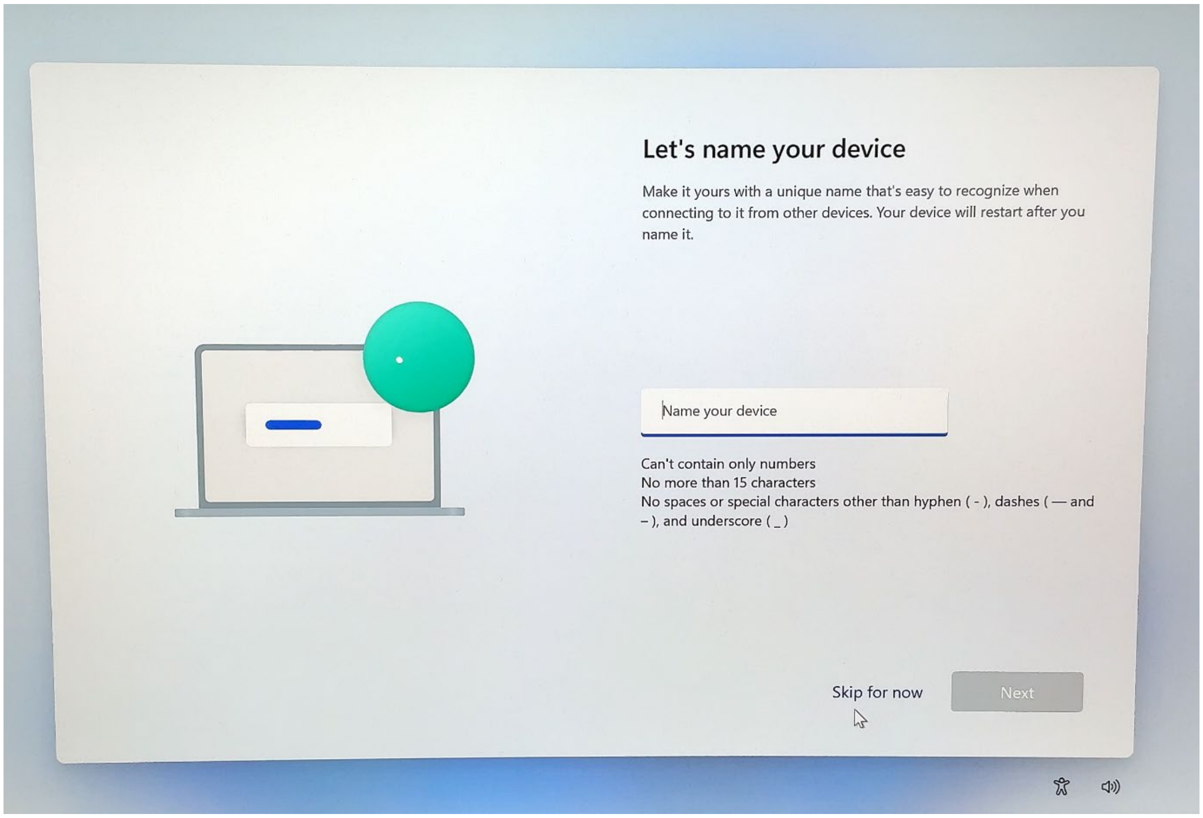
Depending on how you obtained the Windows software, this is a license agreement between (i) you and the device manufacturer or software installer that distributes the software with your device; or (ii) you and Microsoft Corporation (or, based on where you live or, if a business, where your principal place of business is located, one of its affiliates) if you acquired the software from a retailer. Microsoft is the device manufacturer for

Step 7 – Device Name

Step #7: Click **Skip for now** to continue

The screen pictured below will ask you to name your machine.

7



Let's name your device

Make it yours with a unique name that's easy to recognize when connecting to it from other devices. Your device will restart after you name it.

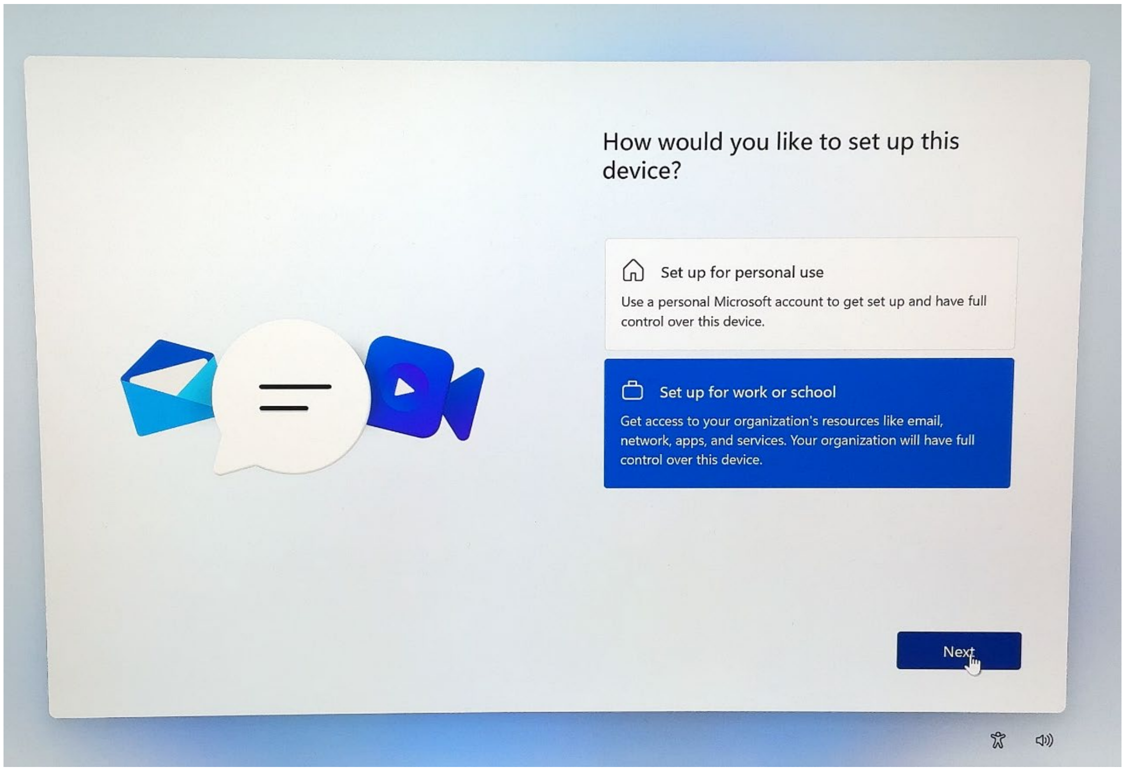
Name your device

Can't contain only numbers
No more than 15 characters
No spaces or special characters other than hyphen (-), dashes (— and –), and underscore (_)

Step #8: Choose **Set up for work or school** and select **Next**

The screen pictured below will ask if you are using the machine for work or school.

8



How would you like to set up this device?

Set up for personal use

Use a personal Microsoft account to get set up and have full control over this device.

Set up for work or school

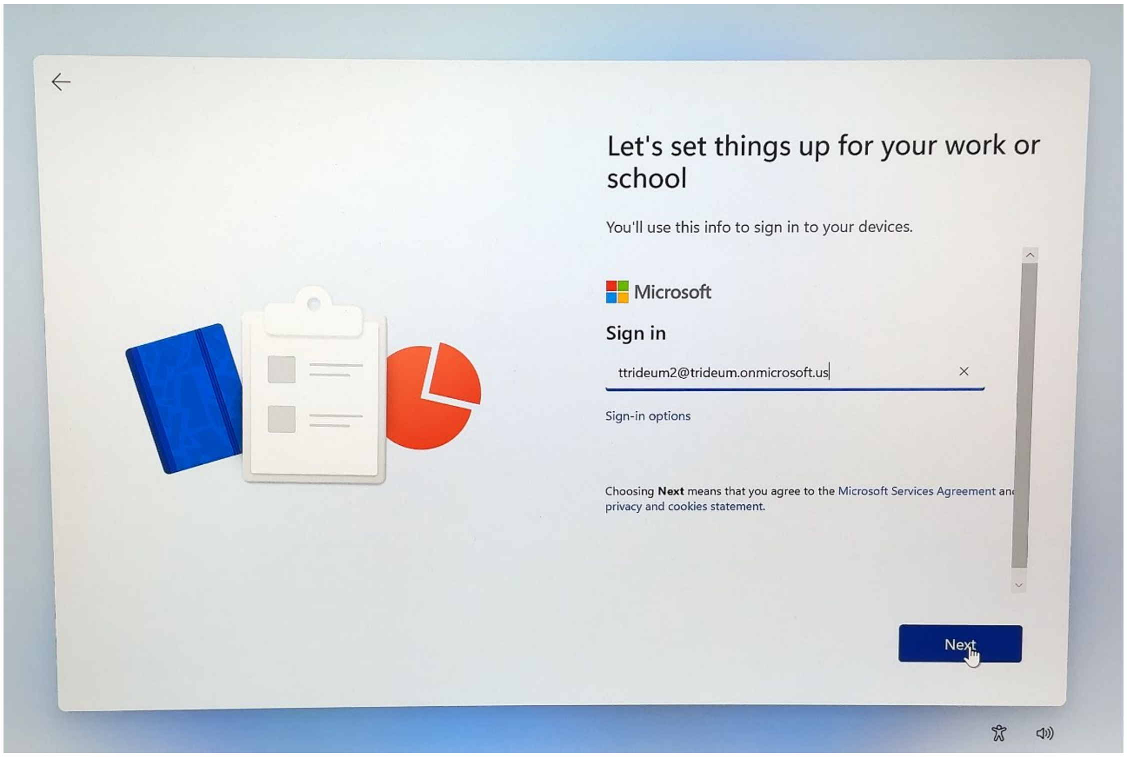
Get access to your organization's resources like email, network, apps, and services. Your organization will have full control over this device.

Step 9 – Sign in

Step #9: Use your full **@trideum.com** email address as the username and click **Next**

The screen pictured below will prompt you for a username.

9



Let's set things up for your work or school

You'll use this info to sign in to your devices.

Sign in

ttrideum2@trideum.onmicrosoft.us

Sign-in options

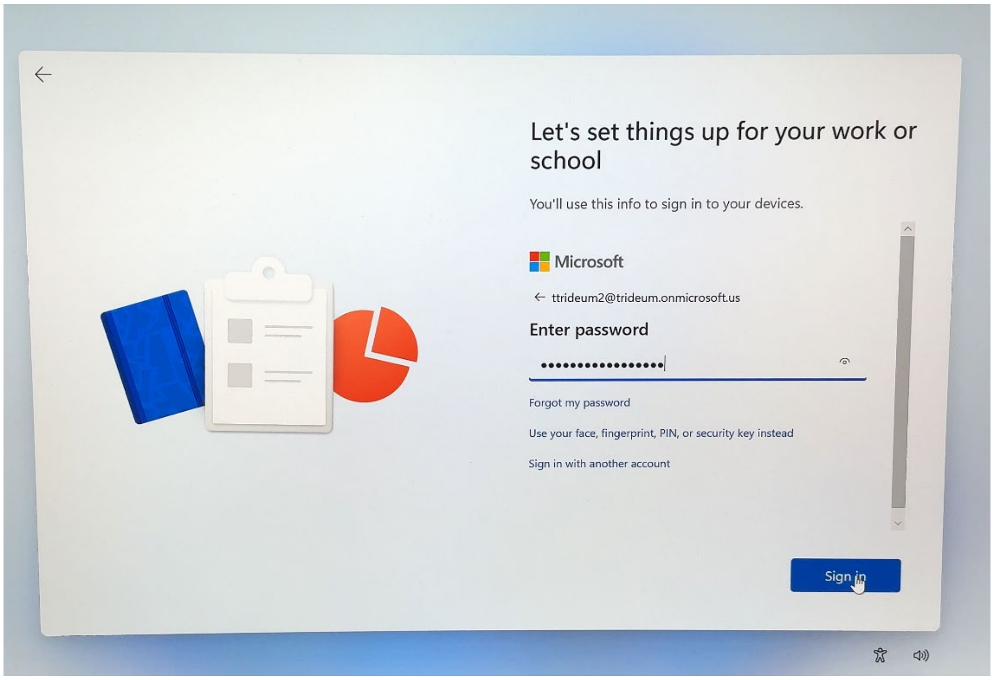
Choosing **Next** means that you agree to the Microsoft Services Agreement an privacy and cookies statement.

Step 10 – Password

Step #10: Your password has not changed, enter it and select **Sign in**

The screen pictured below is the password prompt.

10



Let's set things up for your work or school

You'll use this info to sign in to your devices.

Microsoft

← ttrideum2@trideum.onmicrosoft.us

Enter password

•••••••••••••••••

Forgot my password

Use your face, fingerprint, PIN, or security key instead

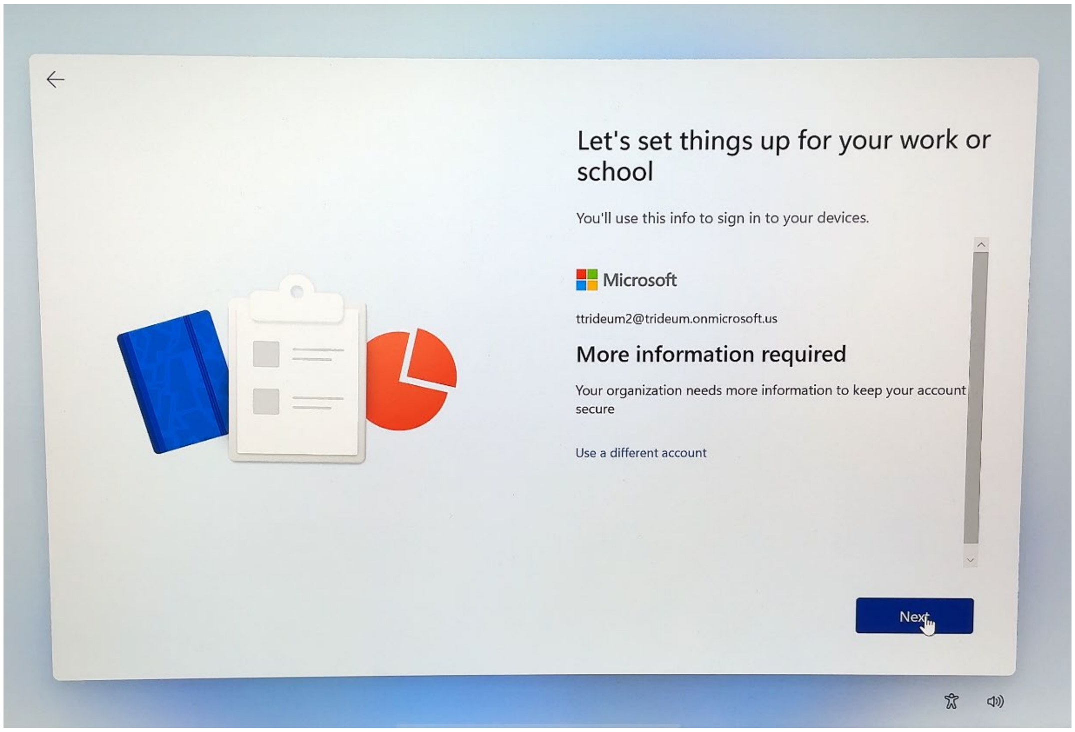
Sign in with another account

Step 11 – More info

<u>**Step #11:**</u> Select **Next** to acknowledge and continue

The screen pictured below will inform you of additional Trideum requirements.

11



Let's set things up for your work or school

You'll use this info to sign in to your devices.

Microsoft

ttrideum2@trideum.onmicrosoft.us

More information required

Your organization needs more information to keep your account secure

Use a different account

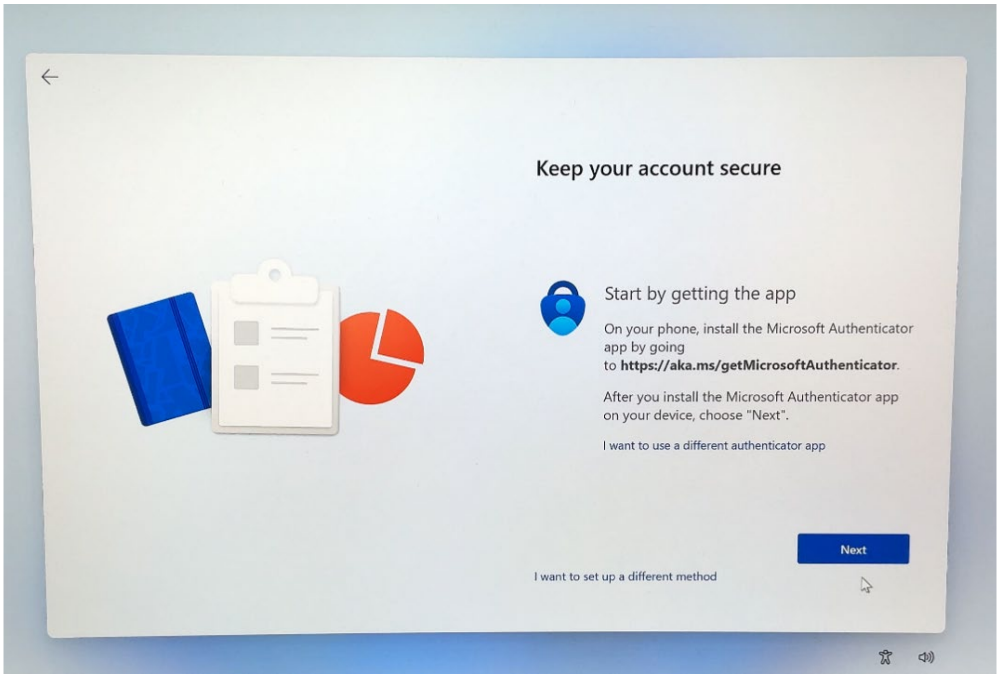
Step 12 – New Authenticator Install

If you already have Microsoft Authenticator installed click Next at the Windows prompt pictured below and skip to Step# 12a

Step #12: Install Microsoft Authenticator. Scan a QR code below and select **Next** once the app is installed

The screen pictured below will prompt you to download the **Microsoft Authenticator** mobile app to your phone.

12



Keep your account secure

Start by getting the app

On your phone, install the Microsoft Authenticator app by going to **https://aka.ms/getMicrosoftAuthenticator**.

After you install the Microsoft Authenticator app on your device, choose "Next".

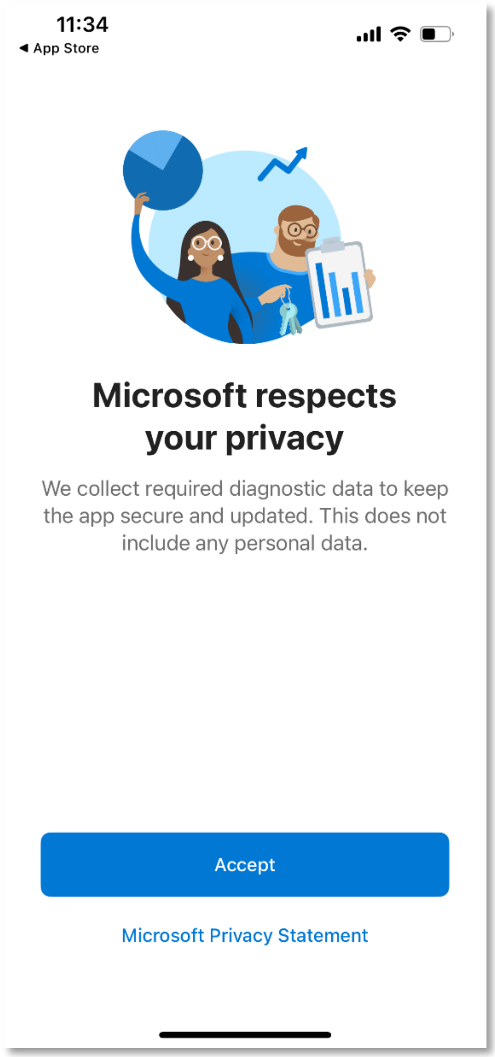
I want to use a different authenticator app

I want to set up a different method

Step 12 – New Authenticator Install

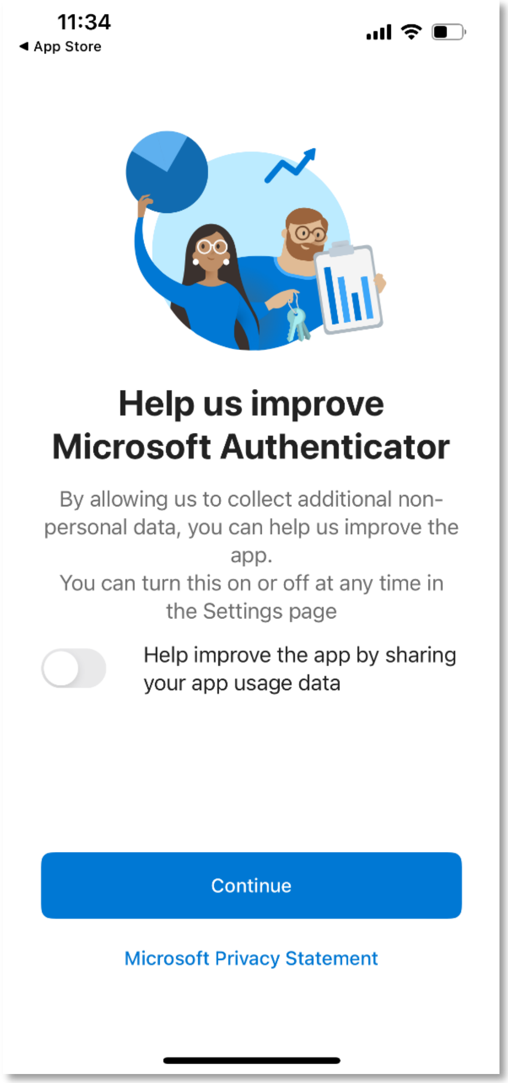
Open the Microsoft Authenticator app on your mobile device, you will see the screens pictured below.

Click **Accept** on the Microsoft Privacy Statement and click **Continue** on the following screen



Microsoft respects your privacy

We collect required diagnostic data to keep the app secure and updated. This does not include any personal data.



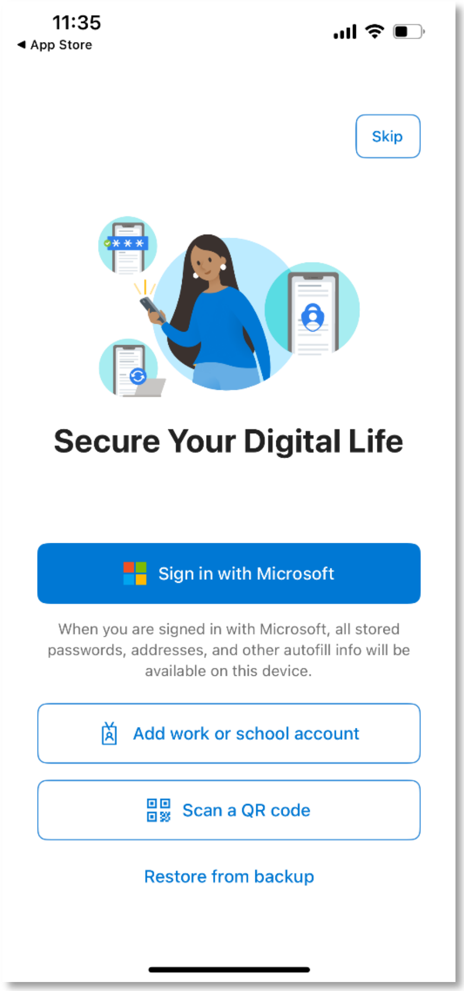
Help us improve Microsoft Authenticator

By allowing us to collect additional non-personal data, you can help us improve the app.
You can turn this on or off at any time in the Settings page

○ Help improve the app by sharing your app usage data

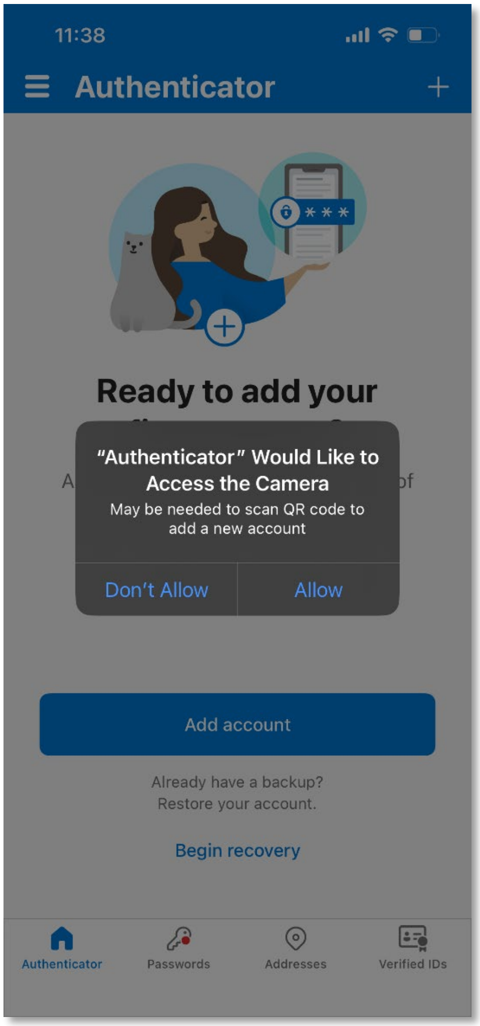
Step 12 – New Authenticator Install

At the screens pictured below, click **Scan a QR code** and click **Allow** to permit access to the camera



Secure Your Digital Life

When you are signed in with Microsoft, all stored passwords, addresses, and other autofill info will be available on this device.



Ready to add your

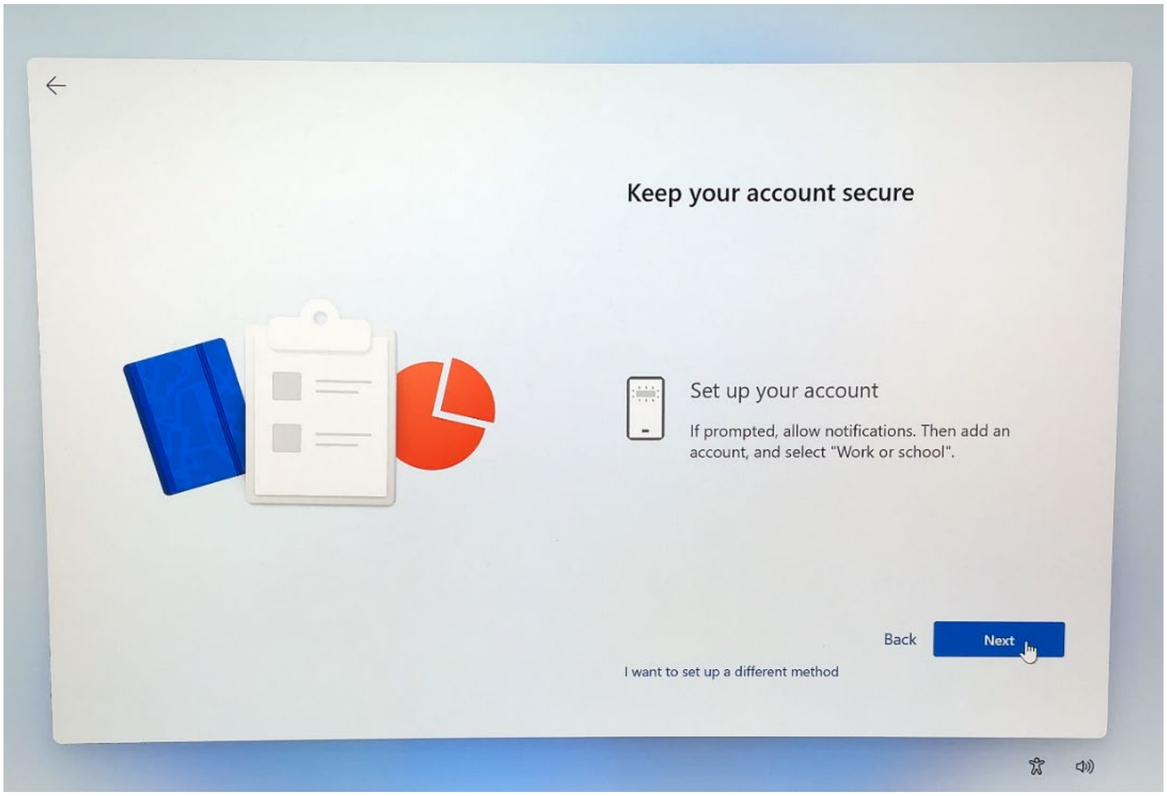
"Authenticator" Would Like to Access the Camera

May be needed to scan QR code to add a new account

Already have a backup? Restore your account.

Step 12 – New Authenticator Install

Select **Next** on the screen below for the QR code

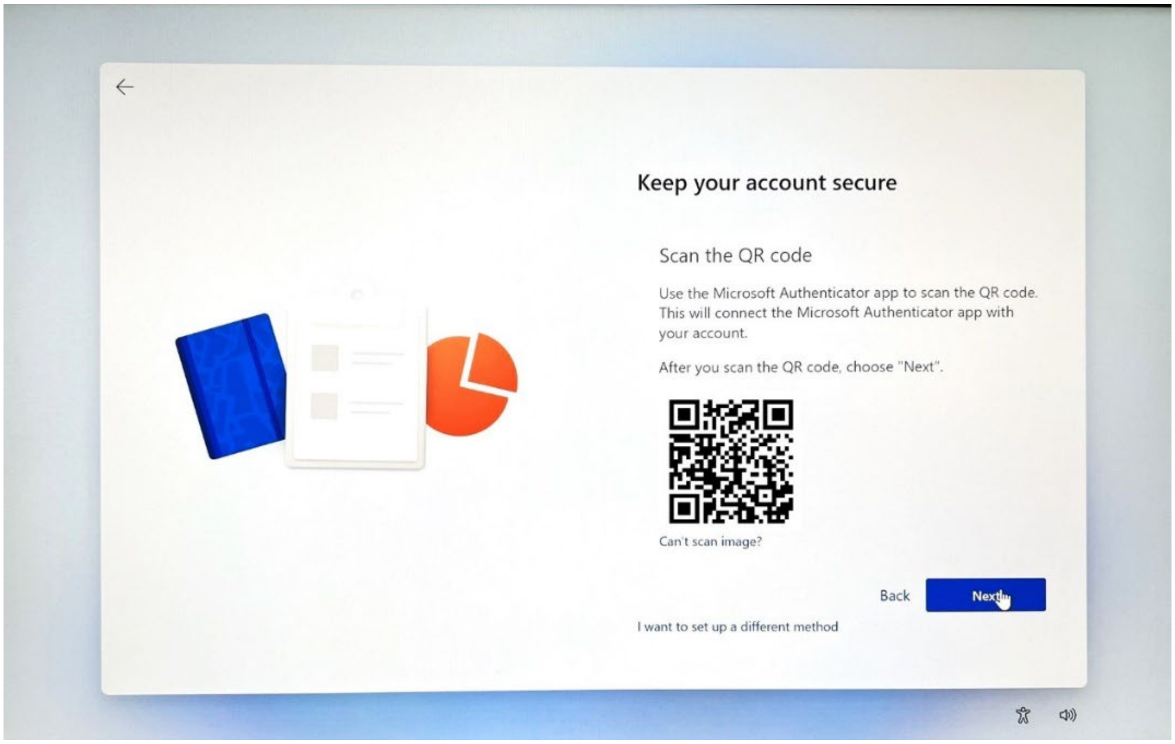


Keep your account secure

Set up your account

If prompted, allow notifications. Then add an account, and select "Work or school".

Aim your phone camera at the QR code displayed



Keep your account secure

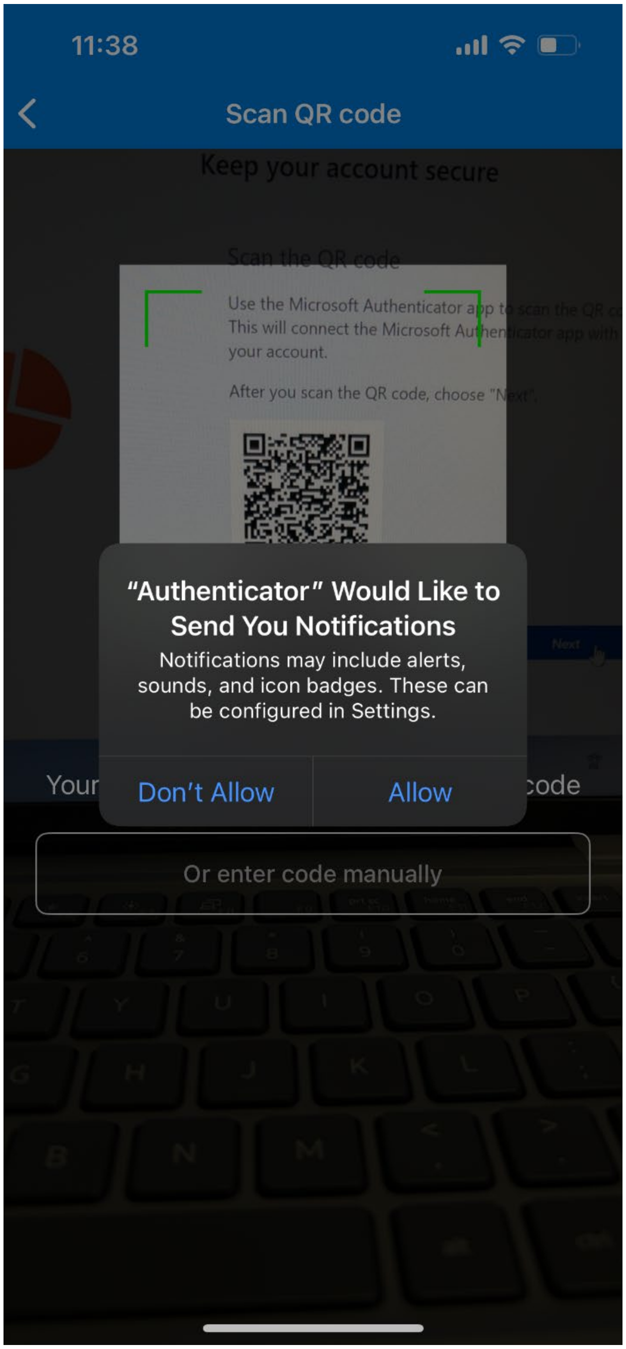
Scan the QR code

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

After you scan the QR code, choose "Next".

Step 12 – New Authenticator Install

You will be prompted to allow notifications as shown below. It is recommended that you Allow Notifications from Authenticator.


11:38
Scan QR code
Keep your account secure
Scan the QR code
Use the Microsoft Authenticator app to scan the QR co
This will connect the Microsoft Authenticator app with
your account.
After you scan the QR code, choose "Next".
Next
Your
code

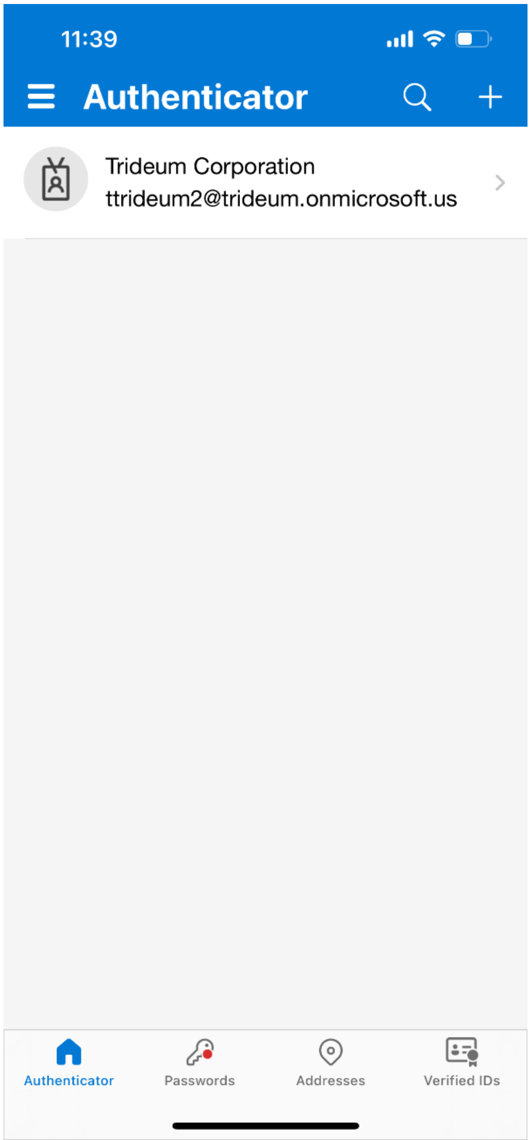
“Authenticator” Would Like to Send You Notifications

Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.

Don’t Allow
Allow
Or enter code manually

Step 12 – New Authenticator Install

When you reach the screen pictured below, you are ready to click **Next** on your workstation.

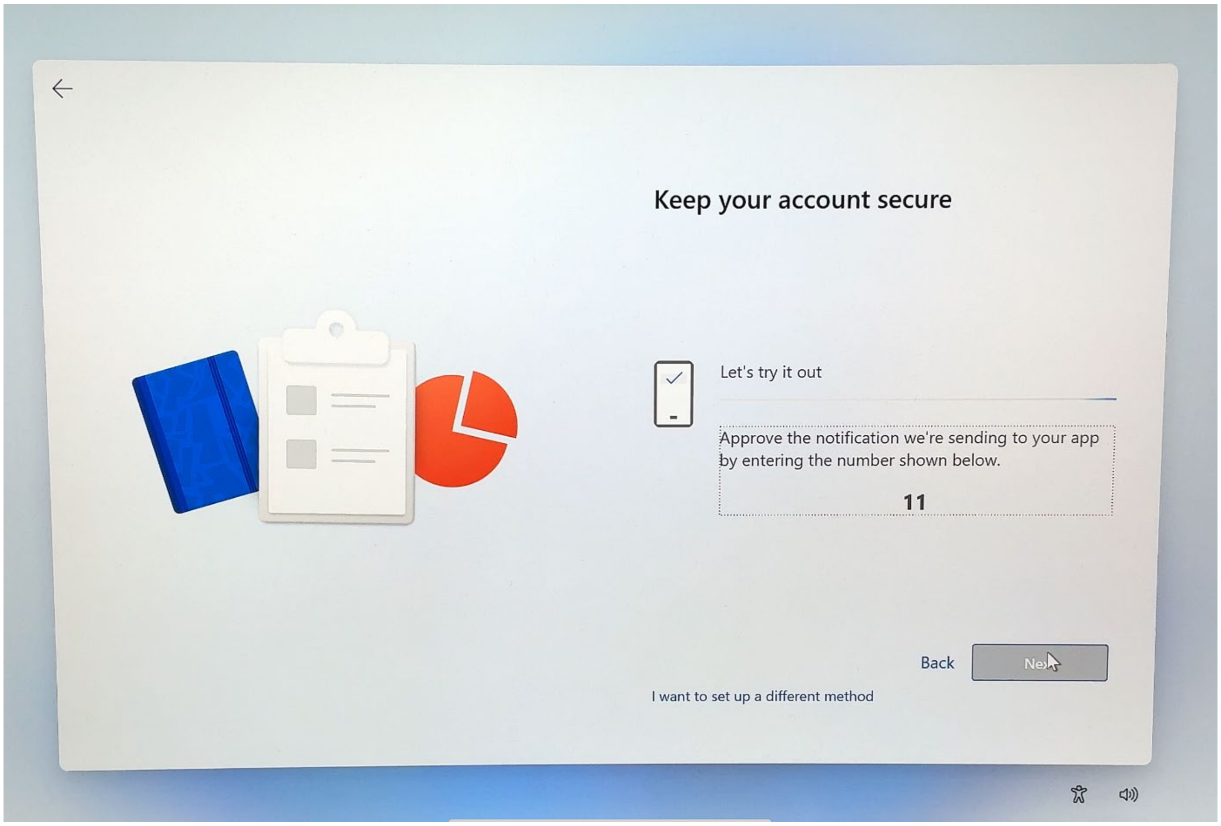


Trideum Corporation
ttrideum2@trideum.onmicrosoft.us

Step 12 – New Authenticator Install

Enter the number you are presented with into Microsoft Authenticator and click **Yes**

You will receive a push notification from Microsoft Authenticator as shown below.

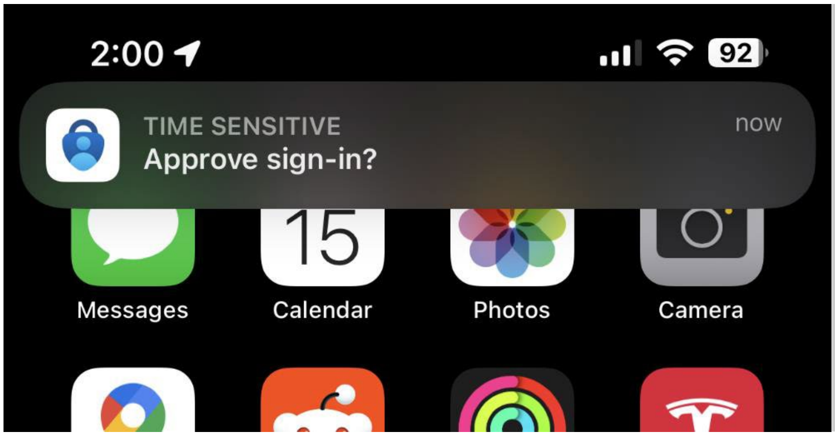


Keep your account secure

Let's try it out

Approve the notification we're sending to your app by entering the number shown below.

11

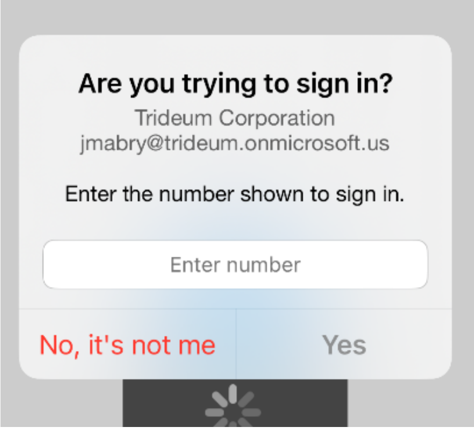


2:00

TIME SENSITIVE

Approve sign-in?

now



Are you trying to sign in?

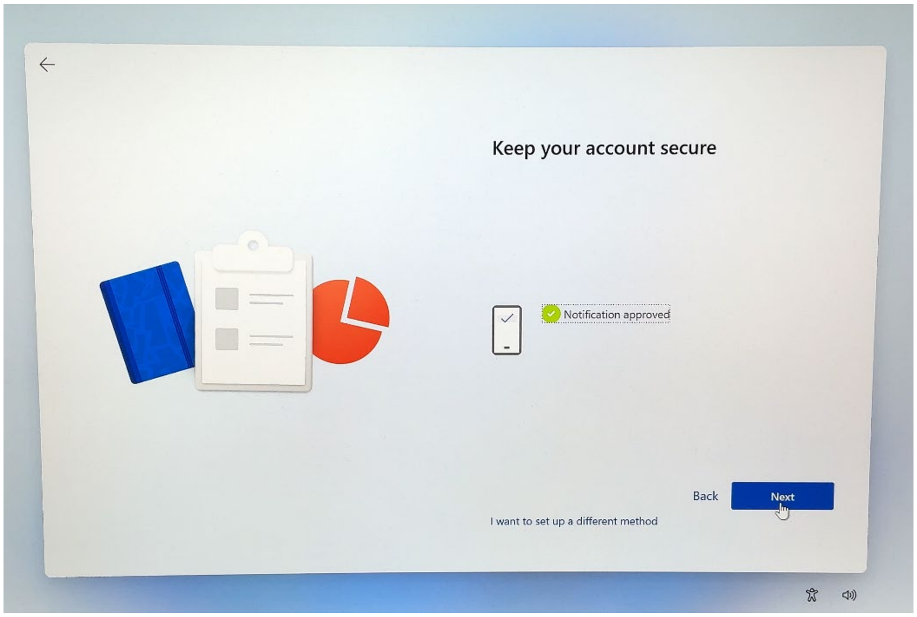
Trideum Corporation

jmabry@trideum.onmicrosoft.us

Enter the number shown to sign in.

Step 12 – New Authenticator Install

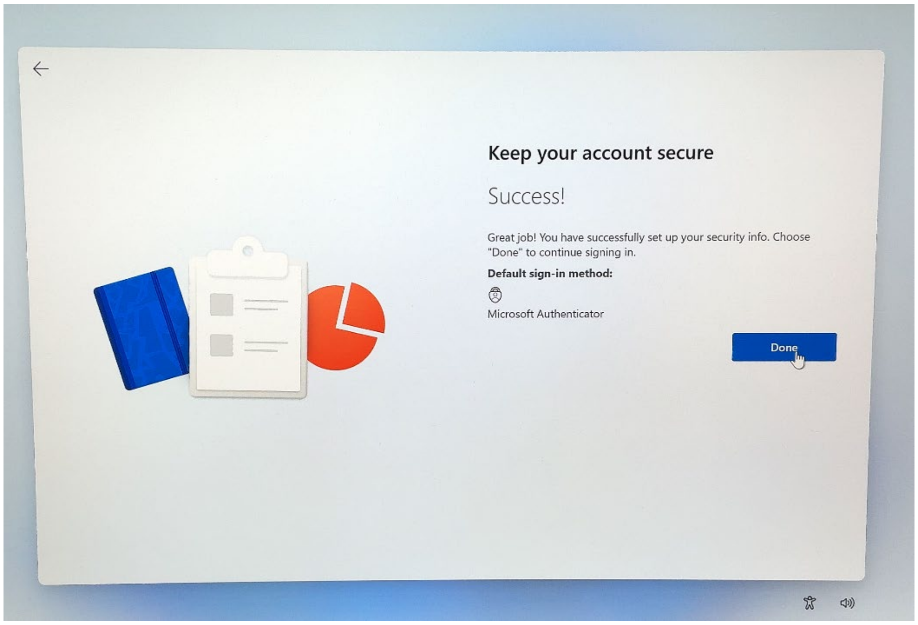
After a successful Authenticator challenge, select **Next** on the screen shown below.



Keep your account secure

Notification approved

Click **Next** on the screen shown below to acknowledge and continue.



Keep your account secure

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:

Microsoft Authenticator

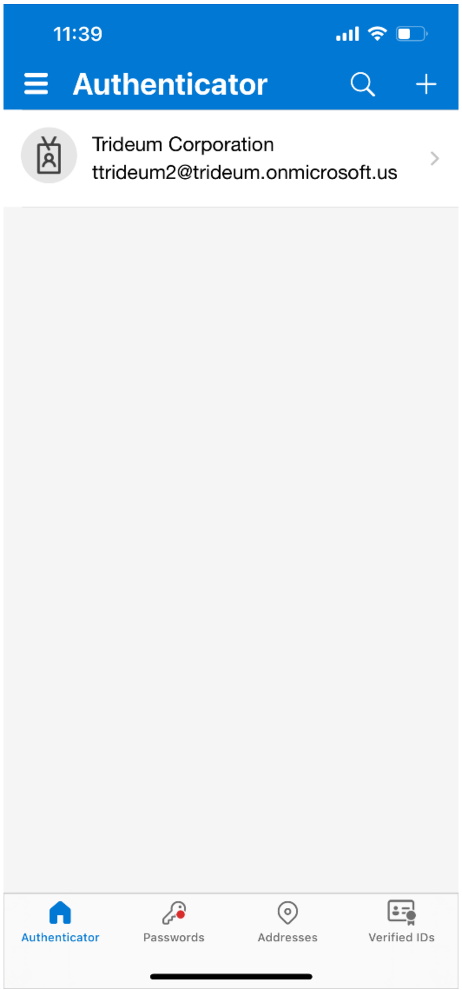
Authenticator is now setup. Select **Done** and move on to step 13

Step 12a – Authenticator Previously Installed

Step #12a: (For users already using Authenticator) Delete your old Trideum Profile and reinstall

Open Authenticator and **click on your Trideum profile**

12a



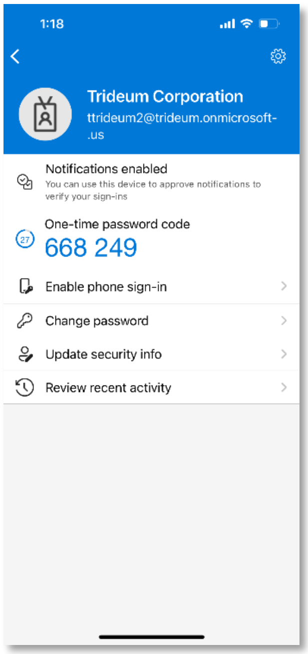
11:39

Authenticator

Trideum Corporation
ttrideum2@trideum.onmicrosoft.us

Step 12a – Authenticator Previously Installed

Click the gear in the top right corner > Click **Remove account** > Click **Continue**



1:18

Trideum Corporation
ttrideum2@trideum.onmicrosoft-.us

Notifications enabled
You can use this device to approve notifications to verify your sign-ins

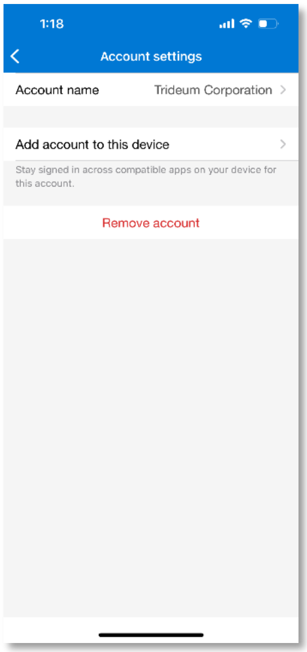
One-time password code
668 249

Enable phone sign-in

Change password

Update security info

Review recent activity



1:18

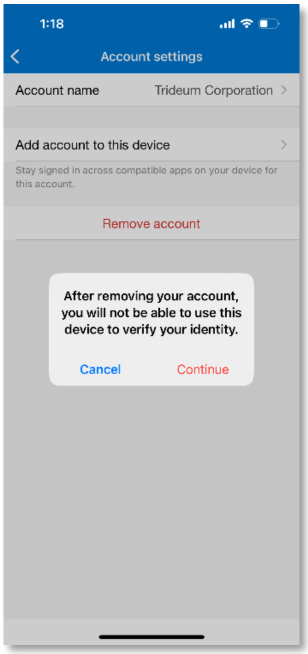
Account settings

Account name — Trideum Corporation

Add account to this device

Stay signed in across compatible apps on your device for this account.

Remove account



1:18

Account settings

Account name — Trideum Corporation

Add account to this device

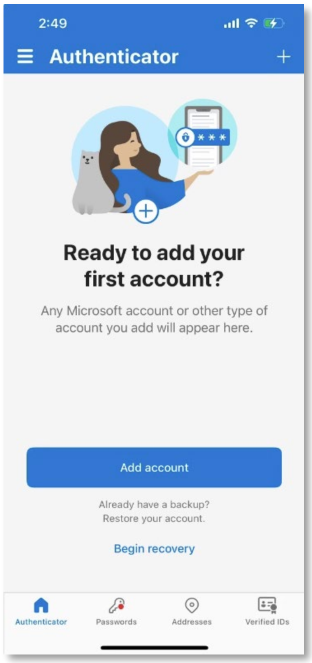
Stay signed in across compatible apps on your device for this account.

Remove account

After removing your account, you will not be able to use this device to verify your identity.

Cancel — Continue

Now Click **Add account** > **Work or school account** > **Scan QR code**



2:49

Authenticator

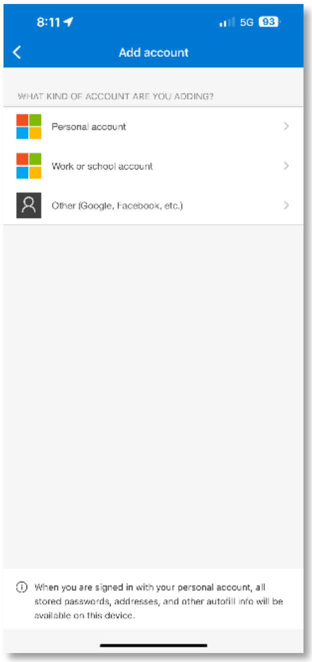
Ready to add your first account?

Any Microsoft account or other type of account you add will appear here.

Add account

Already have a backup?
Restore your account.

Begin recovery



8:11

Add account

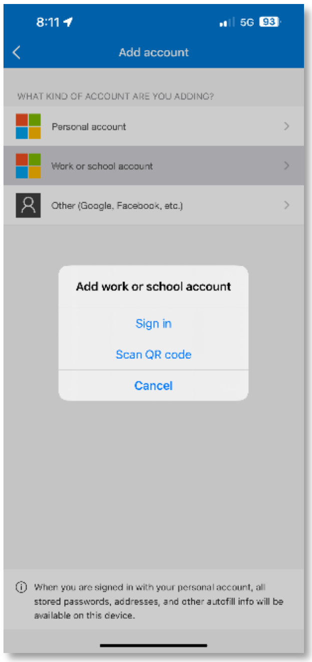
WHAT KIND OF ACCOUNT ARE YOU ADDING?

Personal account

Work or school account

Other (Google, Facebook, etc.)

When you are signed in with your personal account, all stored passwords, addresses, and other autofill info will be available on this device.



8:11

Add account

WHAT KIND OF ACCOUNT ARE YOU ADDING?

Personal account

Work or school account

Other (Google, Facebook, etc.)

Add work or school account

Sign in

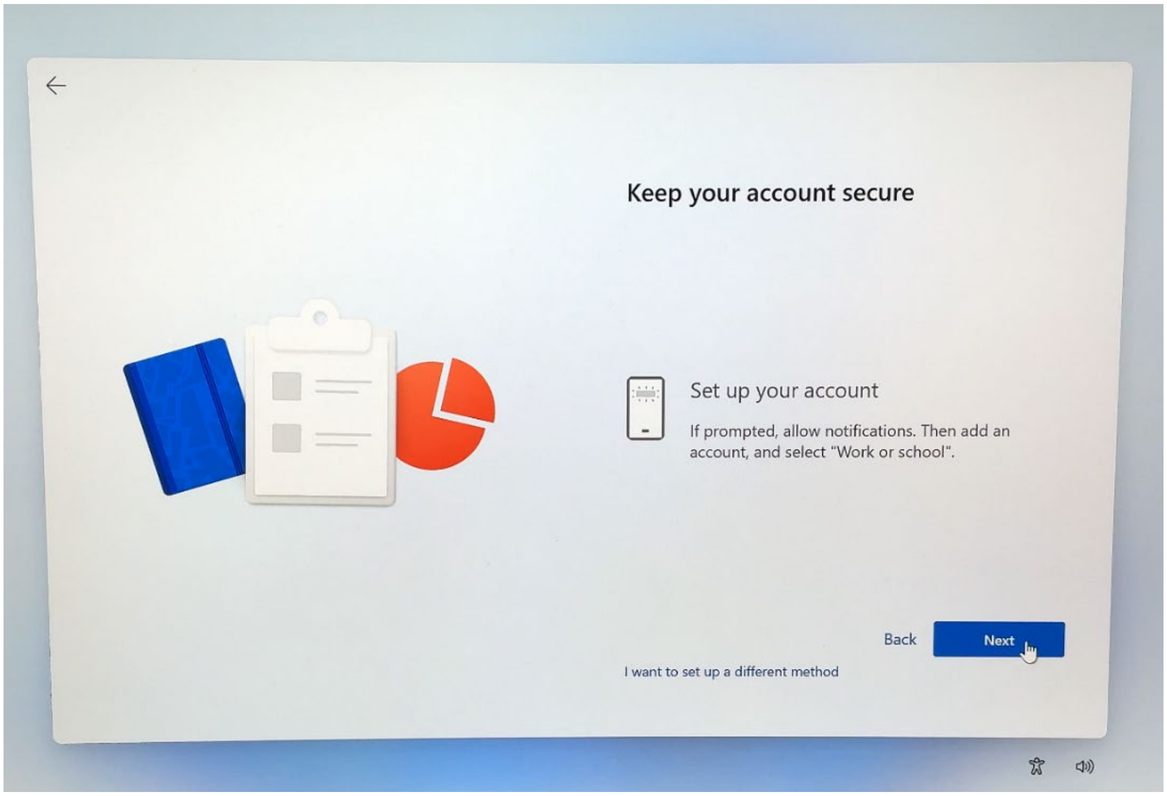
Scan QR code

Cancel

When you are signed in with your personal account, all stored passwords, addresses, and other autofill info will be available on this device.

Step 12 – New Authenticator Install

Select **Next** on the screen below for the QR code

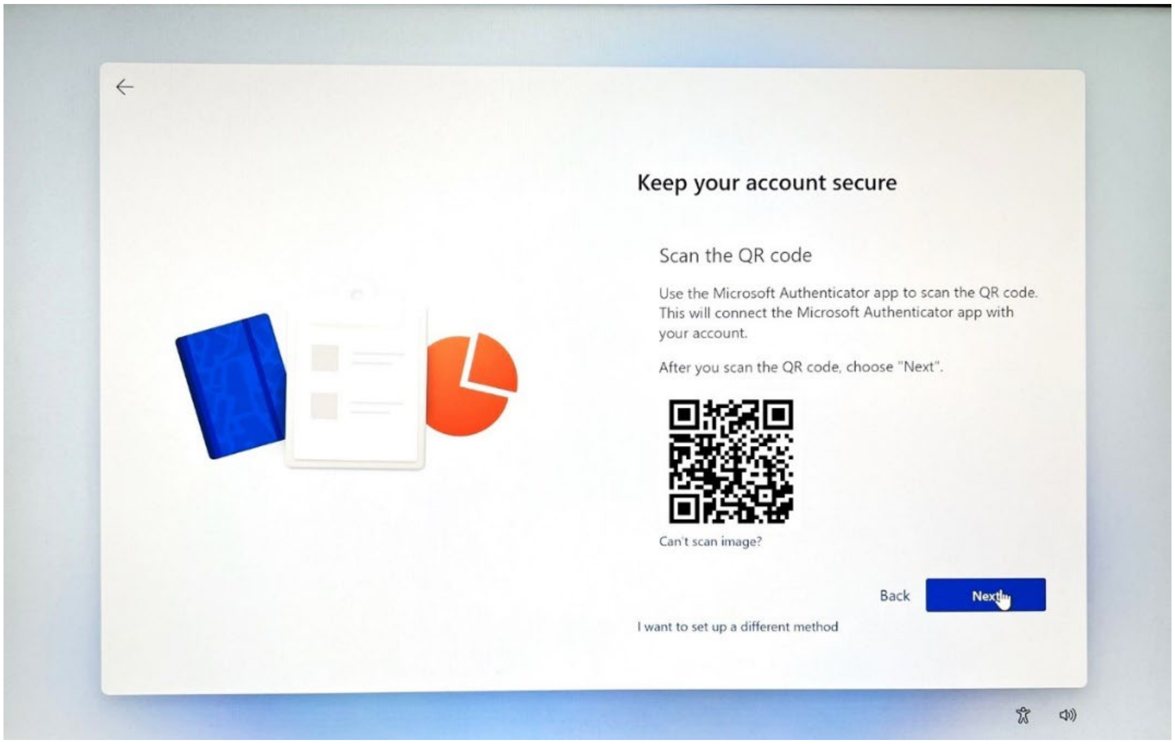


Keep your account secure

Set up your account

If prompted, allow notifications. Then add an account, and select "Work or school".

Aim your phone camera at the QR code displayed



Keep your account secure

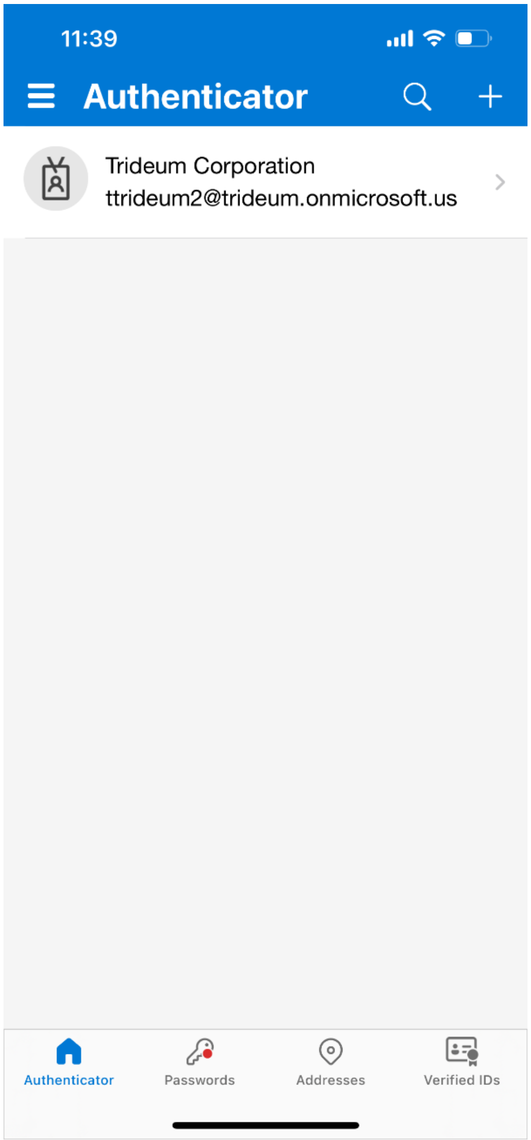
Scan the QR code

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

After you scan the QR code, choose "Next".

Step 12a – Authenticator Previously Installed

When you reach the screen below, you are ready to click **Next** on your workstation.



11:39

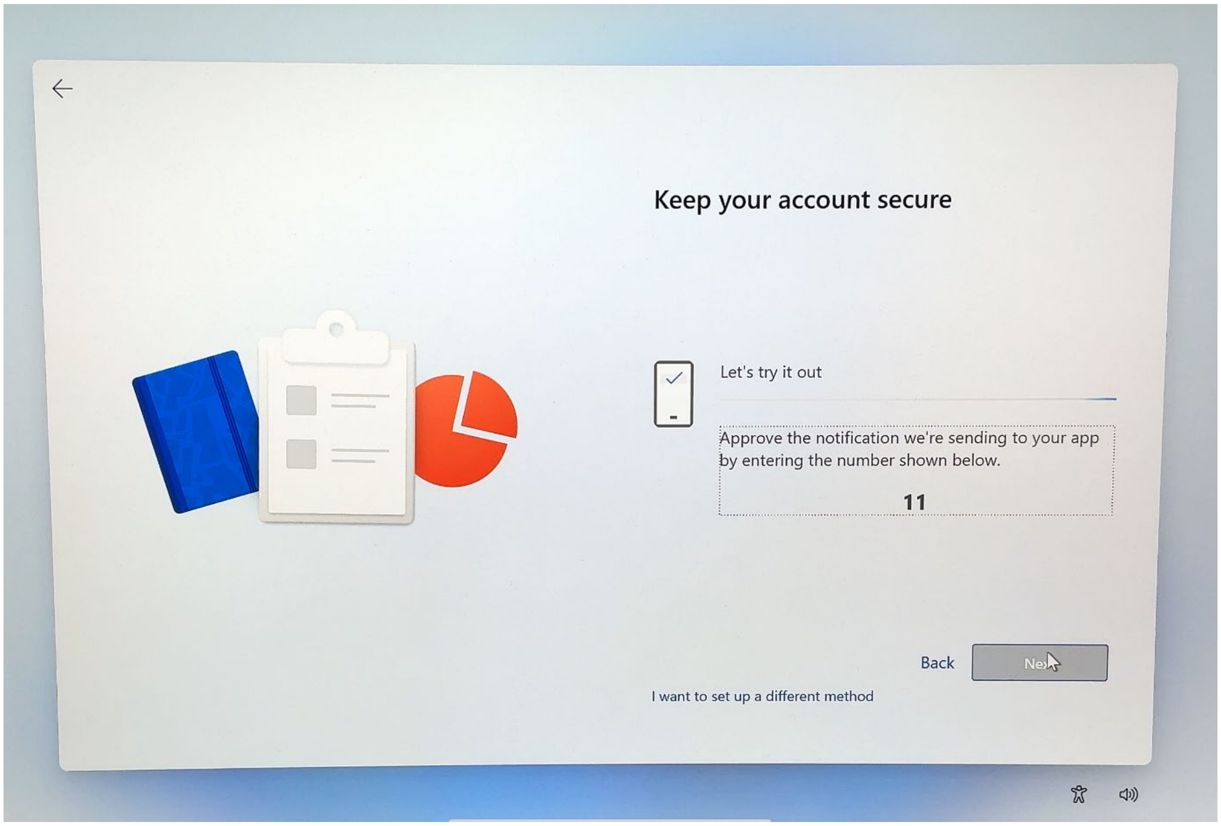
Authenticator

Trideum Corporation
ttrideum2@trideum.onmicrosoft.us

Step 12a – Authenticator Previously Installed

Enter the number you are presented with into Microsoft Authenticator and click **Yes**

You will receive a push notification from Microsoft Authenticator as shown below.

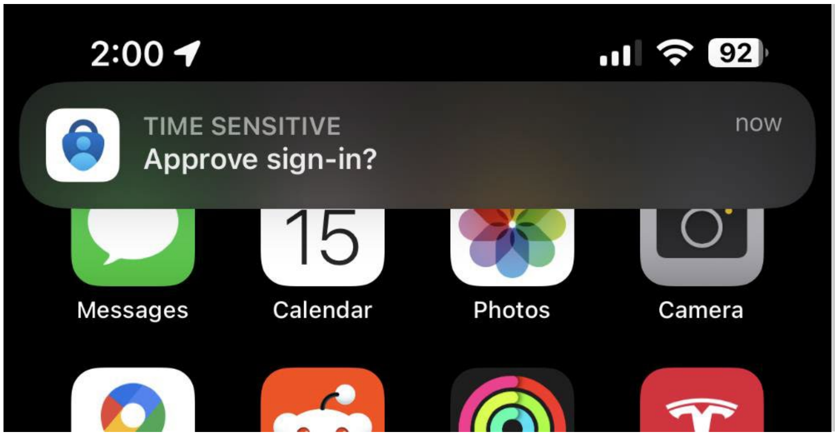


Keep your account secure

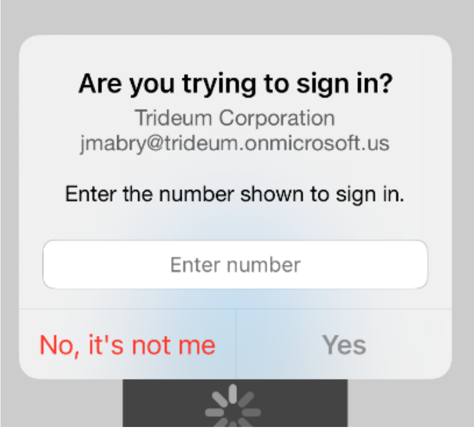
Let's try it out

Approve the notification we're sending to your app by entering the number shown below.

11



Approve sign-in?



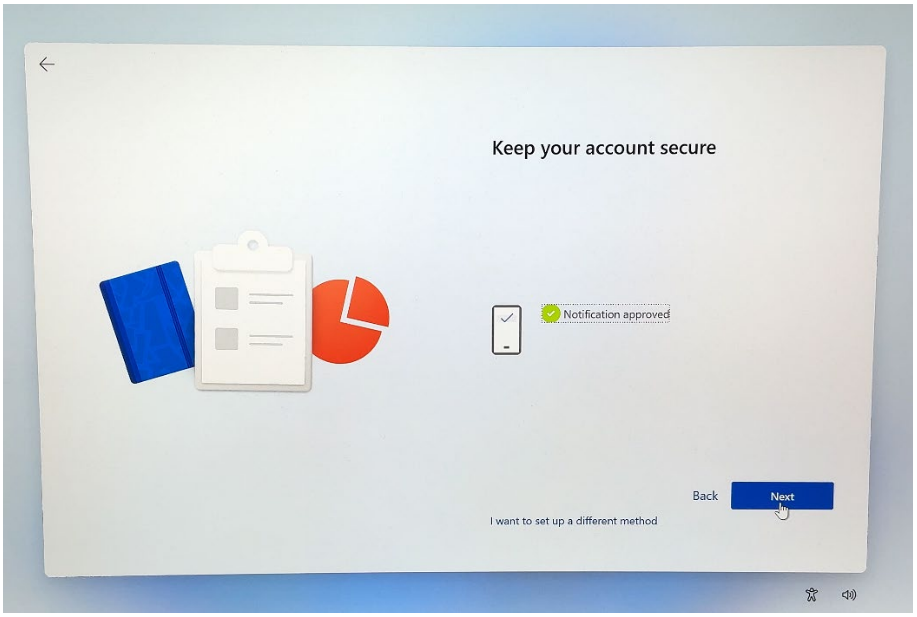
Are you trying to sign in?

Trideum Corporation
jmabry@trideum.onmicrosoft.us

Enter the number shown to sign in.

Step 12a – Authenticator Previously Installed

After a successful Authenticator challenge, select **Next** on the screen shown below.

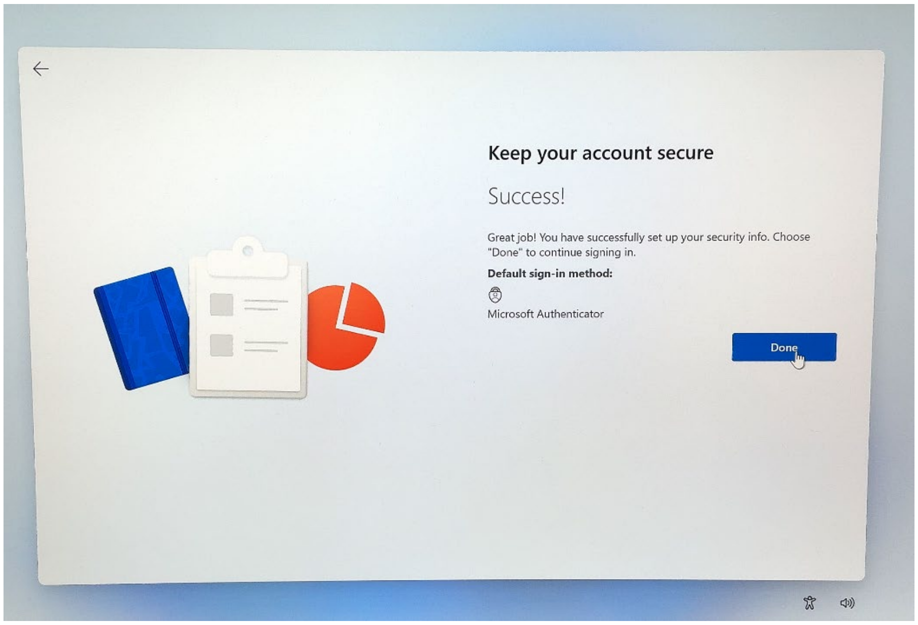


Keep your account secure

Notification approved

I want to set up a different method

Click **Next** on the screen shown below to acknowledge and continue.



Keep your account secure

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:

Microsoft Authenticator

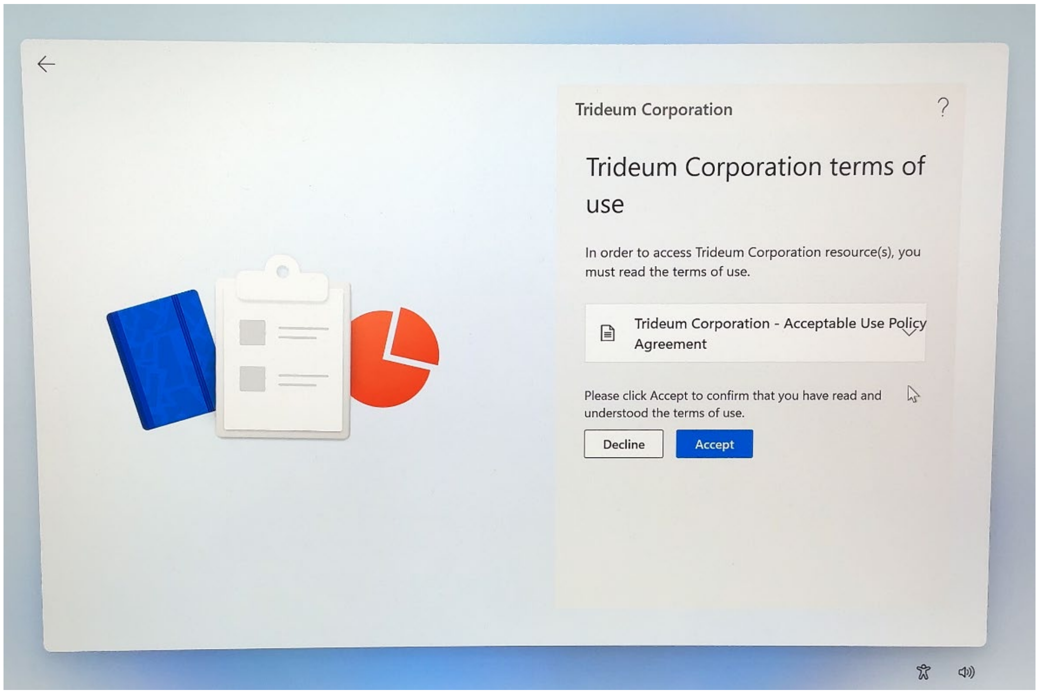
You have successfully setup Authenticator, move on to step 13

Step 13 – AUP

<u>Step #13:</u> **click the drop-down** menu to view the Acceptable Use Policy

The screen pictured below will present the Trideum Acceptable Use Policy.

13



Trideum Corporation

Trideum Corporation terms of use

In order to access Trideum Corporation resource(s), you must read the terms of use.

Trideum Corporation - Acceptable Use Policy Agreement

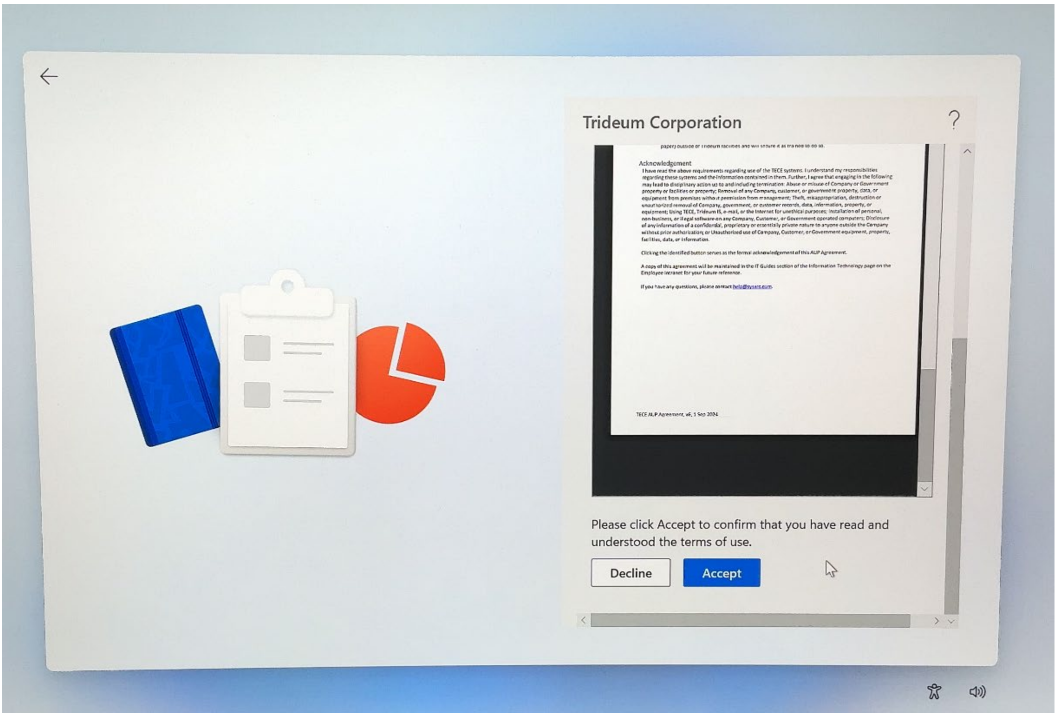
Please click Accept to confirm that you have read and understood the terms of use.

Step 14 – Accept AUP

Step #14: Read the AUP, Select **Accept** to continue

Read Trideum Acceptable Use Policy on the screen pictured below.

14



Trideum Corporation

paper) outside of Trideum facilities and will secure it as trained to do so.

Acknowledgement

I have read the above requirements regarding use of the TECE systems. I understand my responsibilities regarding these systems and the information contained in them. Further, I agree that engaging in the following may lead to disciplinary action up to and including termination: Abuse or misuse of Company or Government property or facilities or property; Removal of any Company, customer, or government property, data, or equipment from premises without permission from management; Theft, misappropriation, destruction or unauthorized removal of Company, government, or customer records, data, information, property, or equipment; Using TECE, Trideum IS, e-mail, or the Internet for unethical purposes; Installation of personal, non-business, or illegal software on any Company, Customer, or Government operated computers; Disclosure of any information of a confidential, proprietary or essentially private nature to anyone outside the Company without prior authorization; or Unauthorized use of Company, Customer, or Government equipment, property, facilities, data, or information.

Clicking the identified button serves as the formal acknowledgement of this AUP Agreement.

A copy of this agreement will be maintained in the IT Guides section of the Information Technology page on the Employee intranet for your future reference.

If you have any questions, please contact help@sysarc.com.

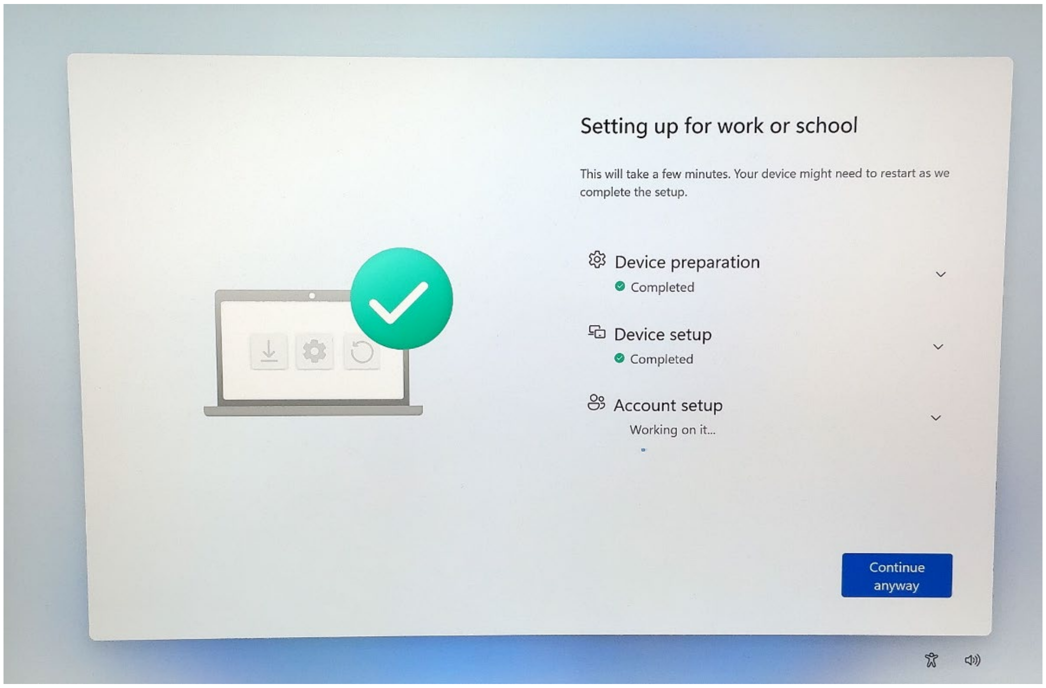
TECE AUP Agreement, v6, 1 Sep 2024

Please click Accept to confirm that you have read and understood the terms of use.

Step #15: Standby for setup…

The workstation will now register with GCC High, apply policy and install applications. This process takes time, please do not click "Continue anyway" unless it gets stuck on this screen for more than 90 minutes.

15



Setting up for work or school

This will take a few minutes. Your device might need to restart as we complete the setup.

Device preparation
Completed

Device setup
Completed

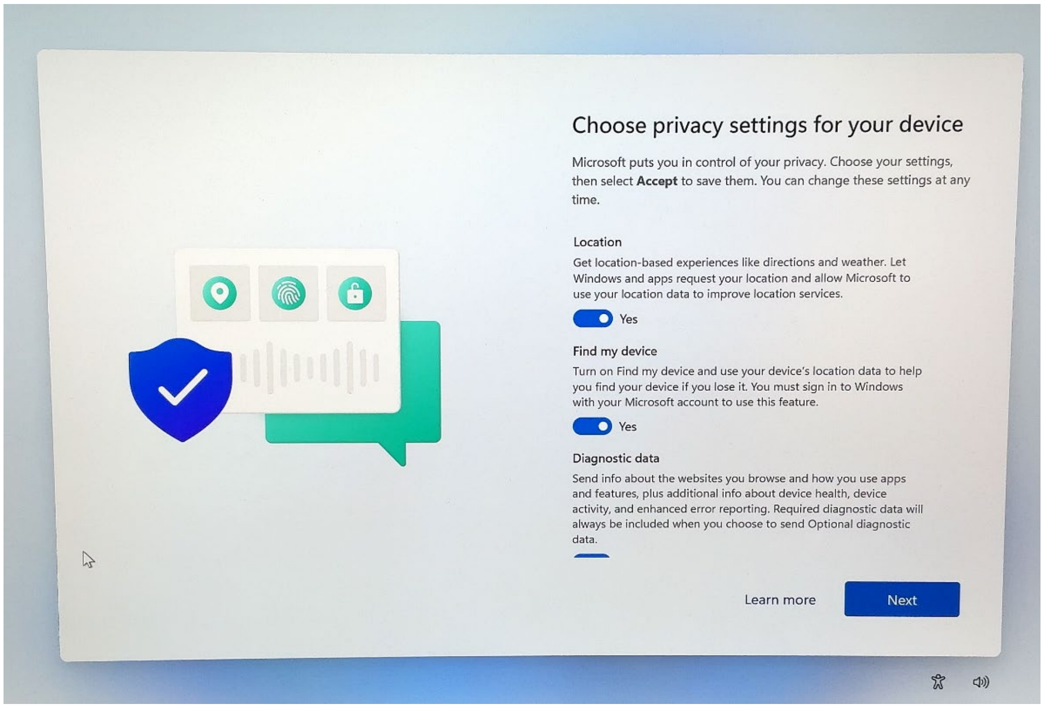
Account setup
Working on it...

Step 16 – Privacy Settings

Step #16: Click **Next** to accept the default settings

On the screen shown below you will be asked to choose privacy settings.

16



Choose privacy settings for your device

Microsoft puts you in control of your privacy. Choose your settings, then select **Accept** to save them. You can change these settings at any time.

Location

Get location-based experiences like directions and weather. Let Windows and apps request your location and allow Microsoft to use your location data to improve location services.

● Yes

Find my device

Turn on Find my device and use your device's location data to help you find your device if you lose it. You must sign in to Windows with your Microsoft account to use this feature.

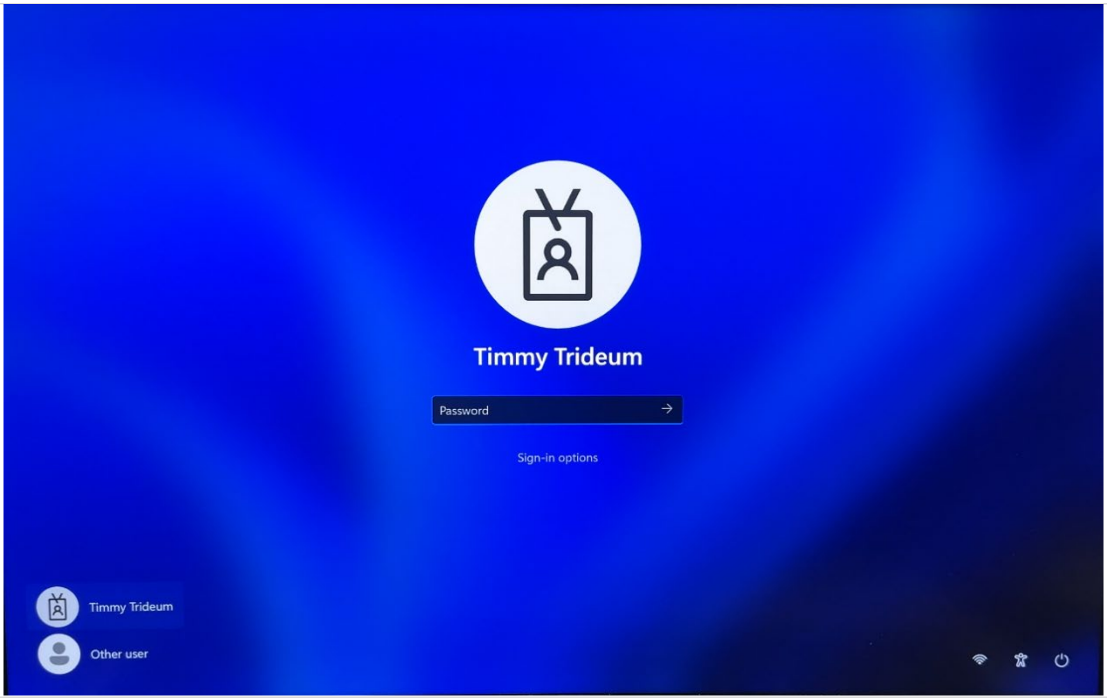
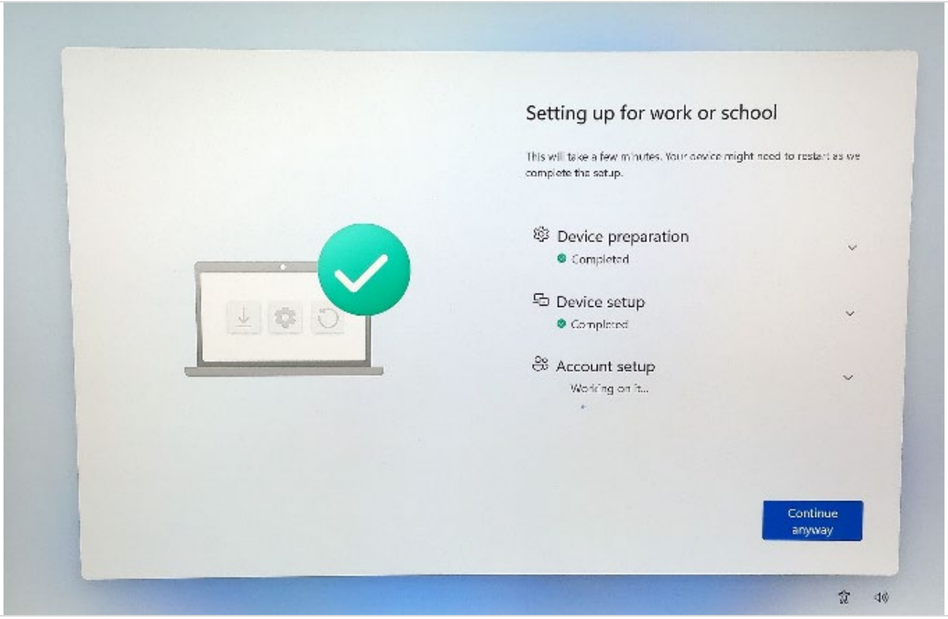
● Yes

Diagnostic data

Send info about the websites you browse and how you use apps and features, plus additional info about device health, device activity, and enhanced error reporting. Required diagnostic data will always be included when you choose to send Optional diagnostic data.

Step #17: Continue to standby…

During this process the workstation will restart.

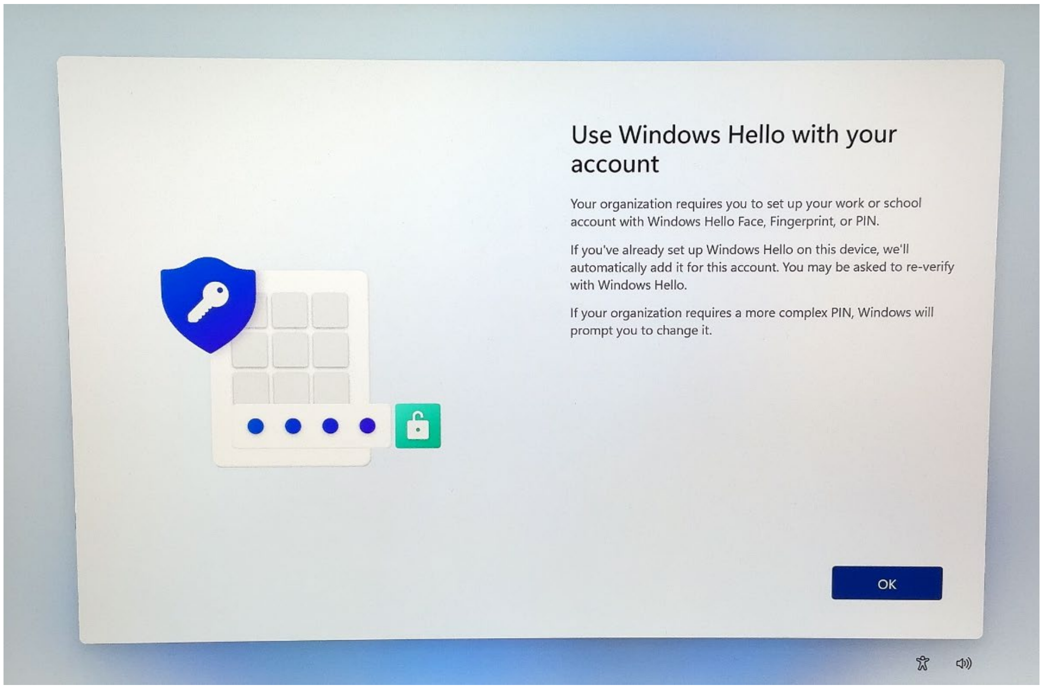
17	 Timmy Trideum Password Sign-in options Timmy Trideum Other user
If you login you will find the setup process is still running as shown below This is expected behavior.	 Setting up for work or school This will take a few minutes. Your device might need to restart as we complete the setup. Device preparation Completed Device setup Completed Account setup Working on it...

Step 18 – Hello

Step #18: Select **OK** to continue

Once the process is complete, you will be prompted to create a “Windows Hello” PIN

18



Use Windows Hello with your account

Your organization requires you to set up your work or school account with Windows Hello Face, Fingerprint, or PIN.

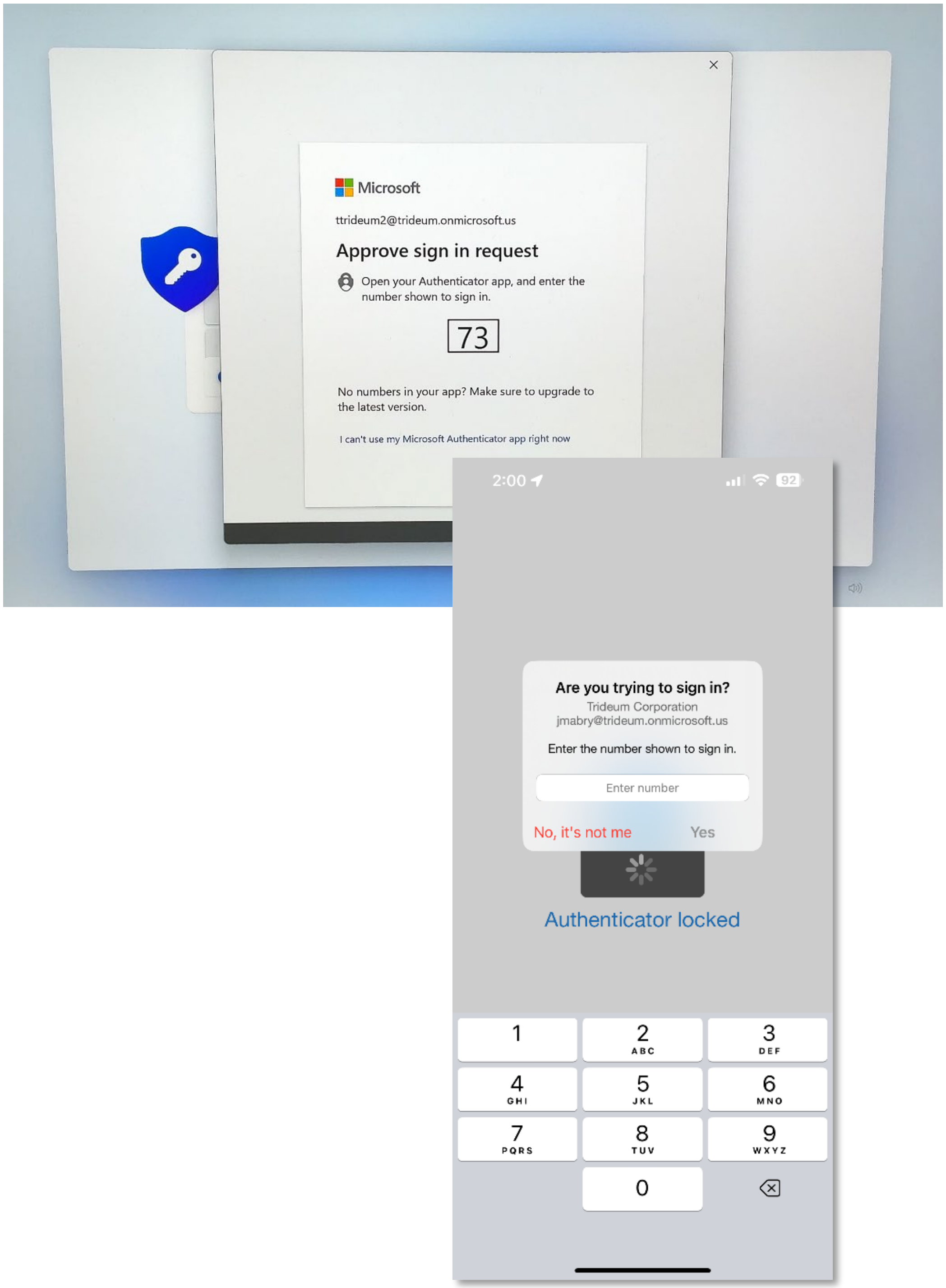
If you've already set up Windows Hello on this device, we'll automatically add it for this account. You may be asked to re-verify with Windows Hello.

If your organization requires a more complex PIN, Windows will prompt you to change it.

Step #19: Enter the number into the Microsoft Authenticator prompt on your phone

You will receive a multi-factor authentication challenge before setting the Hello PIN.

19



Microsoft

ttrideum2@trideum.onmicrosoft.us

Approve sign in request

Open your Authenticator app, and enter the number shown to sign in.

73

No numbers in your app? Make sure to upgrade to the latest version.

I can't use my Microsoft Authenticator app right now

Are you trying to sign in?

Trideum Corporation

jmabry@trideum.onmicrosoft.us

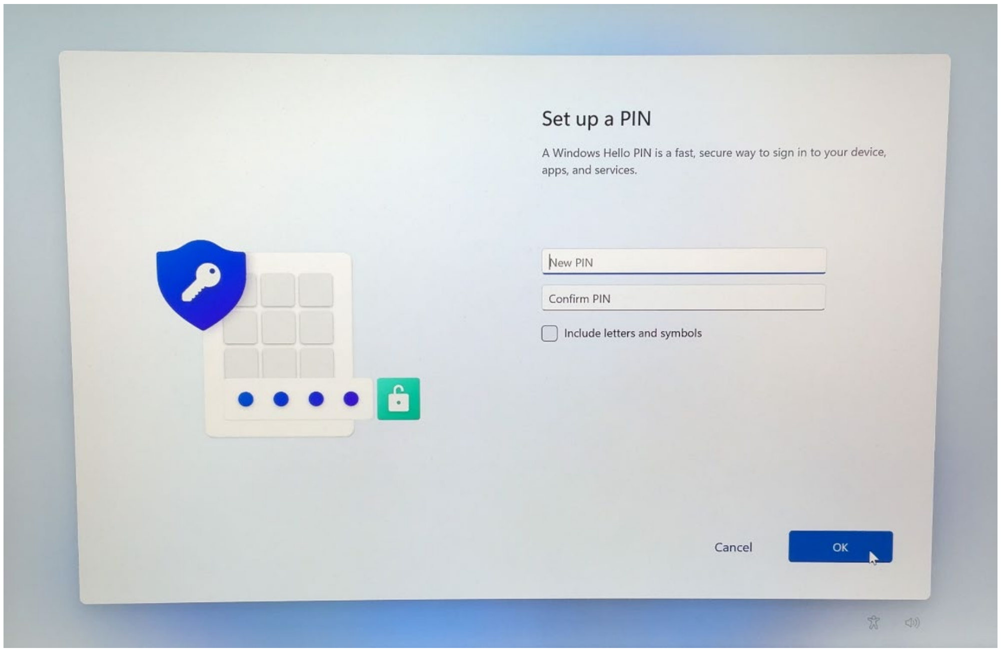
Enter the number shown to sign in.

Step 20 – Set PIN

Step #20: Set Hello PIN (must be 6 digits minimum, but can be as complex as you prefer)

The screen pictured below will prompt you to create a Windows Hello PIN

20



Set up a PIN

A Windows Hello PIN is a fast, secure way to sign in to your device, apps, and services.

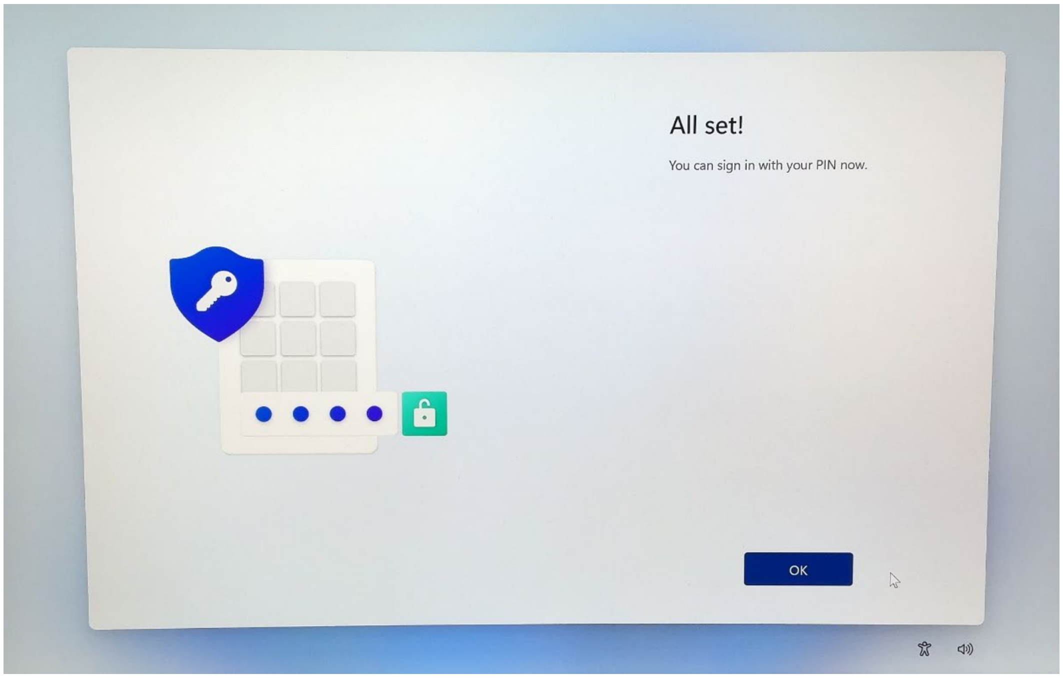
Note this PIN is a secure multi-factor authentication method that binds to your machine only, it will not be available on other machines you may login to

Step 21 – PIN Set

Step #21: Click **OK** to proceed

When you reach the screen pictured below, the process is complete.

21



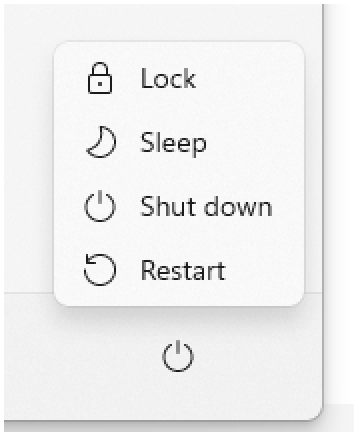
All set!

You can sign in with your PIN now.

Step #22: Wait 5 minutes and restart your computer

5min

22



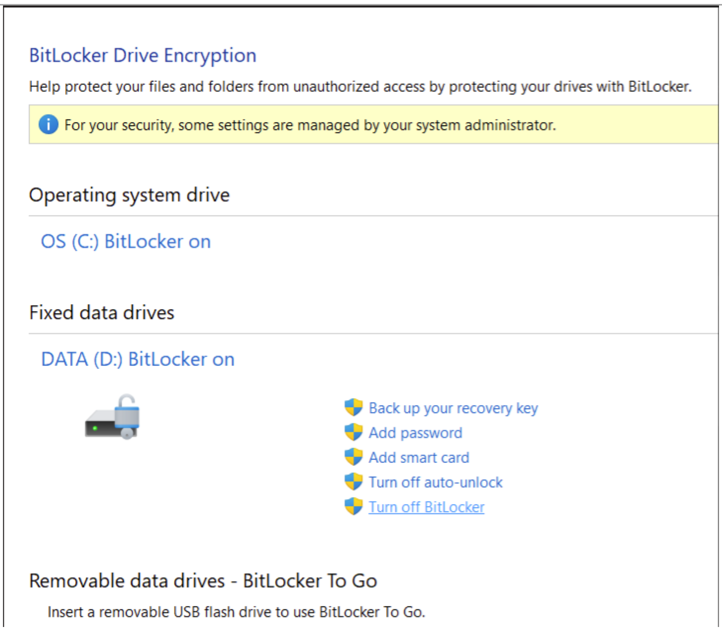
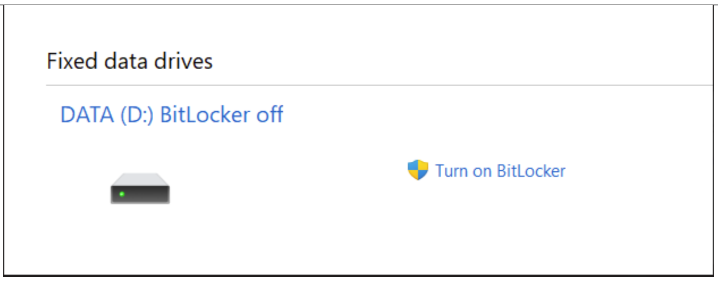
Standard users, You’re done

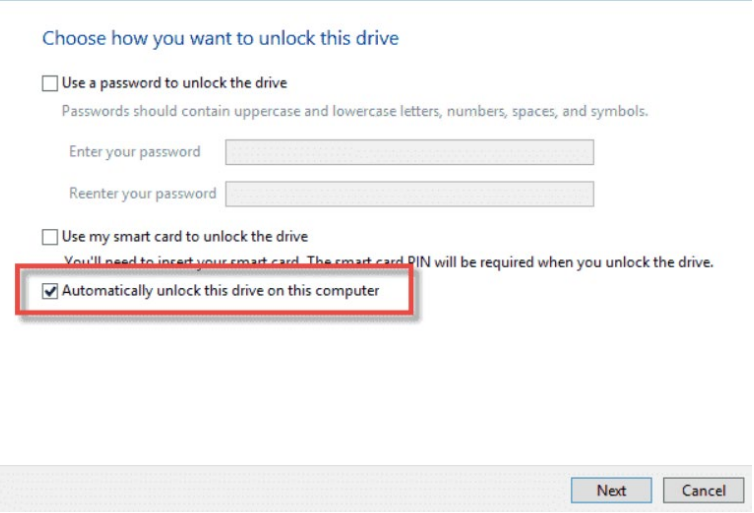
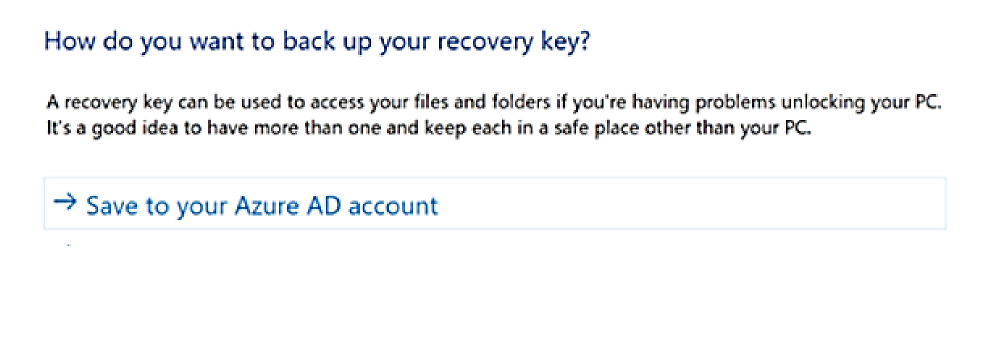
*Developers, Designers, MBSE Team, and others with “Local Admin” privileges >> See the next steps!

DEVELOPERS

You will need your local admin privileges restored before this can be completed.

During Fresh Start see one of the local IT Team or contact SysArc (if you're remote) and they'll help

Step 1 of 8	In **File Explorer** >>	
Step 2	go to "**This PC**" >>	
Step 3	**right click** on the **D: drive** >>	
Step 4	**Manage BitLocker** >>	
Step 5	**Turn off BitLocker** >>	 BitLocker Drive Encryption Help protect your files and folders from unauthorized access by protecting your drives with BitLocker. For your security, some settings are managed by your system administrator. Operating system drive OS (C:) BitLocker on Fixed data drives DATA (D:) BitLocker on Back up your recovery key Add password Add smart card Turn off auto-unlock Turn off BitLocker Removable data drives - BitLocker To Go Insert a removable USB flash drive to use BitLocker To Go.
Step 6	then immediately **Turn on BitLocker** >>	 Fixed data drives DATA (D:) BitLocker off Turn on BitLocker

Step 7	Choose **Automatically unlock this drive on this computer** >>	 Choose how you want to unlock this drive ☐ Use a password to unlock the drive Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols. Enter your password Reenter your password ☐ Use my smart card to unlock the drive You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive. ☑ Automatically unlock this drive on this computer
Step 8 of 8	**Save to your Azure AD account** *This will ensure the new policy is deployed - your drive will be encrypted with AES 256 and the recovery key uploaded to Azure*	 How do you want to back up your recovery key? A recovery key can be used to access your files and folders if you're having problems unlocking your PC. It's a good idea to have more than one and keep each in a safe place other than your PC. → Save to your Azure AD account