

- AWS GA is targeted at 4<sup>th</sup> May 2022.
- If and when we talk about Native Services, we will probably cite **AWS only** as these are gearing towards AWS GA preparation.
- Information on Azure will be shared in coming months (to recap, Azure GA will be by Q3 2022).
- All slides will be shared and most of the documentation will also be translated to either Developers Portal (accessible by everyone) or Docs Portal (only accessible by for TechPass account holders).
- All the slides can be shared with existing contractors who are required to manage Projects on GCC as deemed fit by Agencies.
- The series of “Brown Bag” lunch time tech talk is arranged so as to ensure more people can join us in view that some will clash with your meetings. Please feel free to have your lunch while you join us.



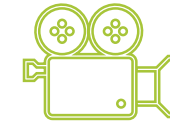
## For Your Info

- You will be put on mute by default.
- Video should be turned off.



## Q&A Segment

- Type in message box when you want to ask a question.
- Wait to be acknowledged by the presenter before speaking.
- Unmute your microphone and state your name and agency clearly.



## Session Recording

- Please note that the series of GCC 2.0 Tech Talks will be recorded.
- The video recordings will be made available (in SharePoint).

# Let Us Know Your Feedback!



<https://form.gov.sg/625cbd578a621f0012fa9bac>

- Let us know what went well and how we can improve.
- We want to ensure that we are bringing the right contents to you so as to help Agencies.
- If you have any questions, please reach out to us at [Ask\\_CODEX@tech.gov.sg](mailto:Ask_CODEX@tech.gov.sg)



# Self-service Onboarding SEED and TechPass for Public Officers and Vendors

Kellyn, Kok Pin  
GDS Central

Date : 4<sup>th</sup> May 2022

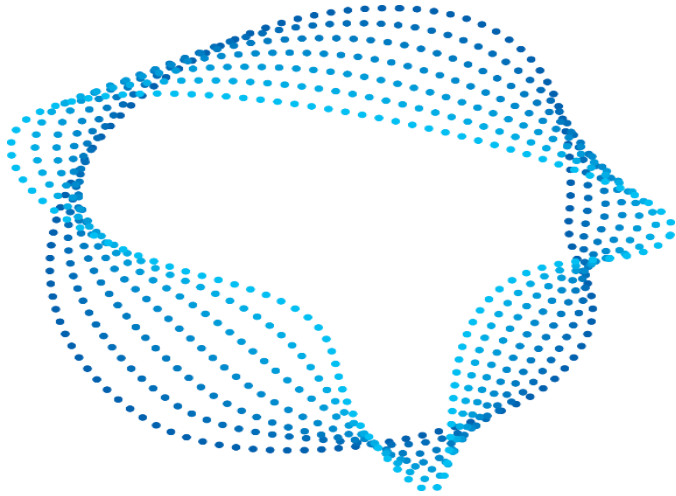


**GOVTECH**  
SINGAPORE

## TABLE OF CONTENTS

1. Why You Should Onboard to SEED
2. Onboarding Flow
  - TechPass for Public Officers
  - TechPass for Vendors
  - Onboarding to SEED
3. Offboarding Process
4. Incident Support
5. TIPS on How to have a smooth onboarding journey to SEED
6. DEMO
7. Q&A

# Why You Should Onboard to SEED



# SEED (Security Suite for Engineering Endpoint Devices)

*- Identity and Access Management (IAM) platform for the GCC2.0 environment*

SEED comprise of the following components:

1. **TechPass** – Identity Service to allow single set of credentials for SG Tech Stack/GCC2.0 services.
2. **CloudFlare Teams** –Enforces Zero trust network access. Comprises of Cloudflare WARP, Cloudflare Gateway and Cloudflare Access.
3. **DEEP (Development Environment Endpoint Posture)** – DEEP is the device management layer of the MDM. It manages the following:
  - a. **Microsoft Intune** – Provides device and application management, including remote application deployment and selective device wipe.
  - b. **MDATP (Microsoft Defender Advanced Threat Prevention)** – Enterprise class vulnerability management, threat detection and response security solution.
  - c. **Tanium** – Endpoint assets and posture management. Works with Cloudflare to ensure posture based conditional access.

# Why You Should Onboard to SEED

**Security Suite for Engineering Endpoint Devices (SEED)** is a suite of tools consisting of **Cloudflare Teams**, **TechPass**, and **Developers' Environment Endpoint Posture (DEEP)**, which will be used to protect against unauthorised access to Government engineering resources.

## Benefits of SEED

- Full Self-Service signup process.
- Visibility on onboarded personnel, their device(s) and their compliance status.
- Access DEEP Dashboard (via Cloudflare WARP) to update your Internet Devices' security.
- SEED Single Sign-On coverage for other SGTS products and Developer Services.
- Onboarding to SEED now allows you to have a smoother transition when migrating to GCC2.0 in future, as your device will already have the access prerequisites for GCC2.0.

## Budget and Cost of SEED

Licenses for Intune, Defender, Tanium and Cloudflare will be centrally procured. Agencies **do not need to put up purchase for these licenses**. The associated costs will be recovered by GovTech via SMF. However, Agency **may need to budget and procure** internet machines to be onboarded as Government Managed Devices for access of GCC2.0.

## SEED

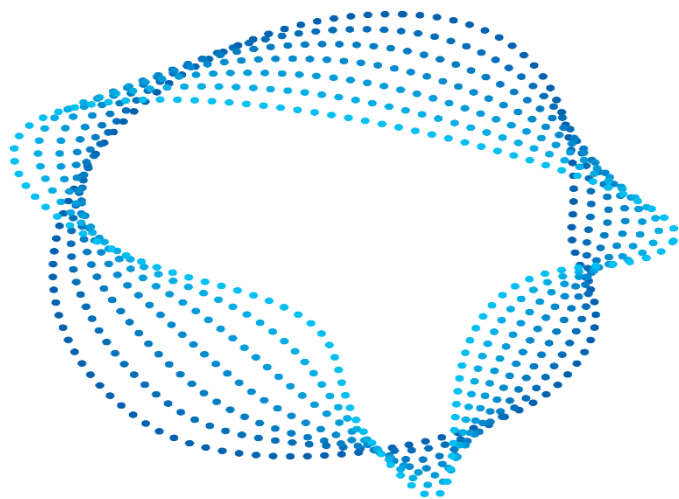
Real-time periodic posture checks with capability to terminate only individual services

Real-time secured identity (with MFA) and device posture through an encrypted channel to access apps

A single identity, streamlined on/off boarding and simplified access to apps and services

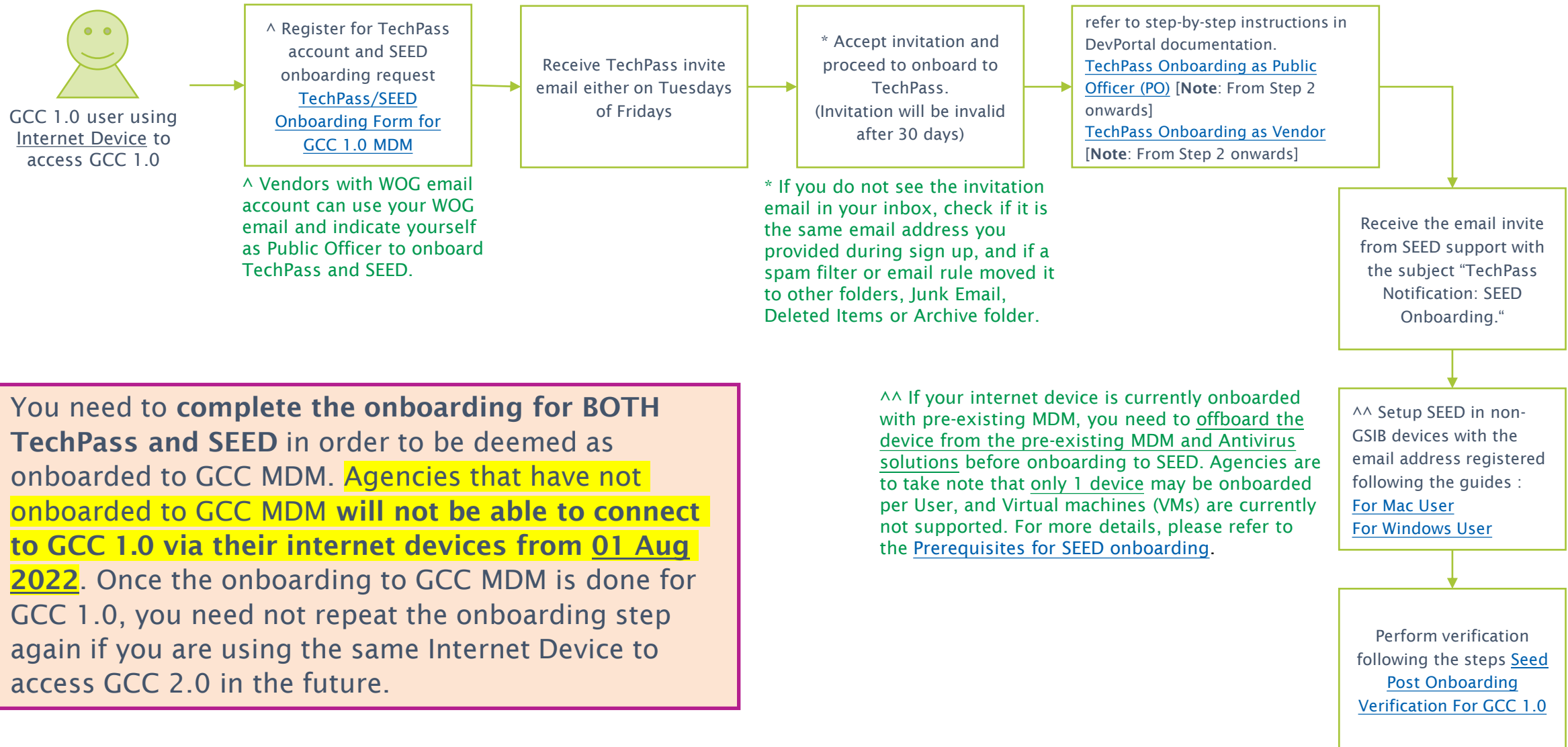
If you use GMD (internet device) to access GCC or some of the SGTS products, using SEED is **MANDATORY**

# Onboarding Flow





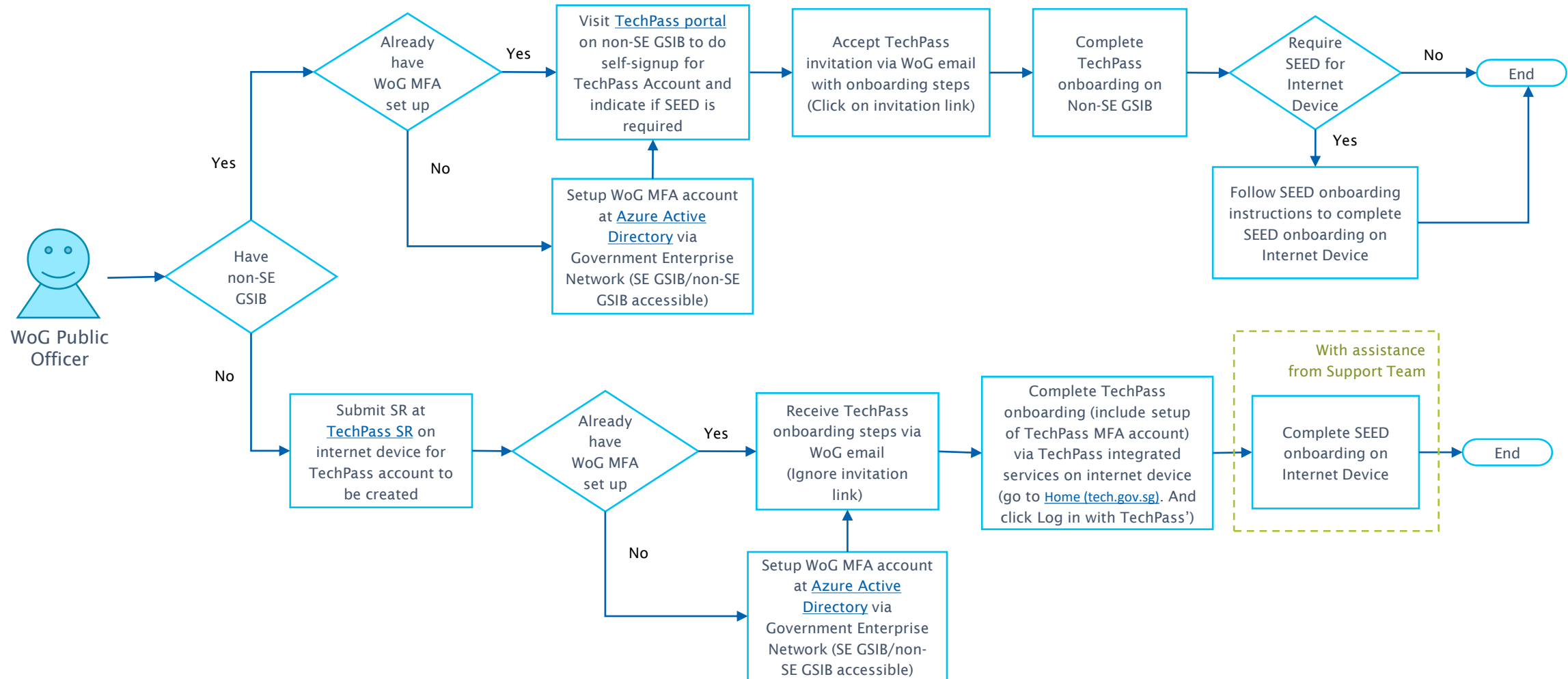
# GCC 1.0 MDM Onboarding Flow



**You need to complete the onboarding for BOTH TechPass and SEED in order to be deemed as onboarded to GCC MDM. Agencies that have not onboarded to GCC MDM will not be able to connect to GCC 1.0 via their internet devices from 01 Aug 2022.** Once the onboarding to GCC MDM is done for GCC 1.0, you need not repeat the onboarding step again if you are using the same Internet Device to access GCC 2.0 in the future.

^^ If your internet device is currently onboarded with pre-existing MDM, you need to offboard the device from the pre-existing MDM and Antivirus solutions before onboarding to SEED. Agencies are to take note that only 1 device may be onboarded per User, and Virtual machines (VMs) are currently not supported. For more details, please refer to the [Prerequisites for SEED onboarding](#).

# Typical Onboarding Flow < Public Officer >



# Onboarding to TechPass < Public Officer >

## Public Officers



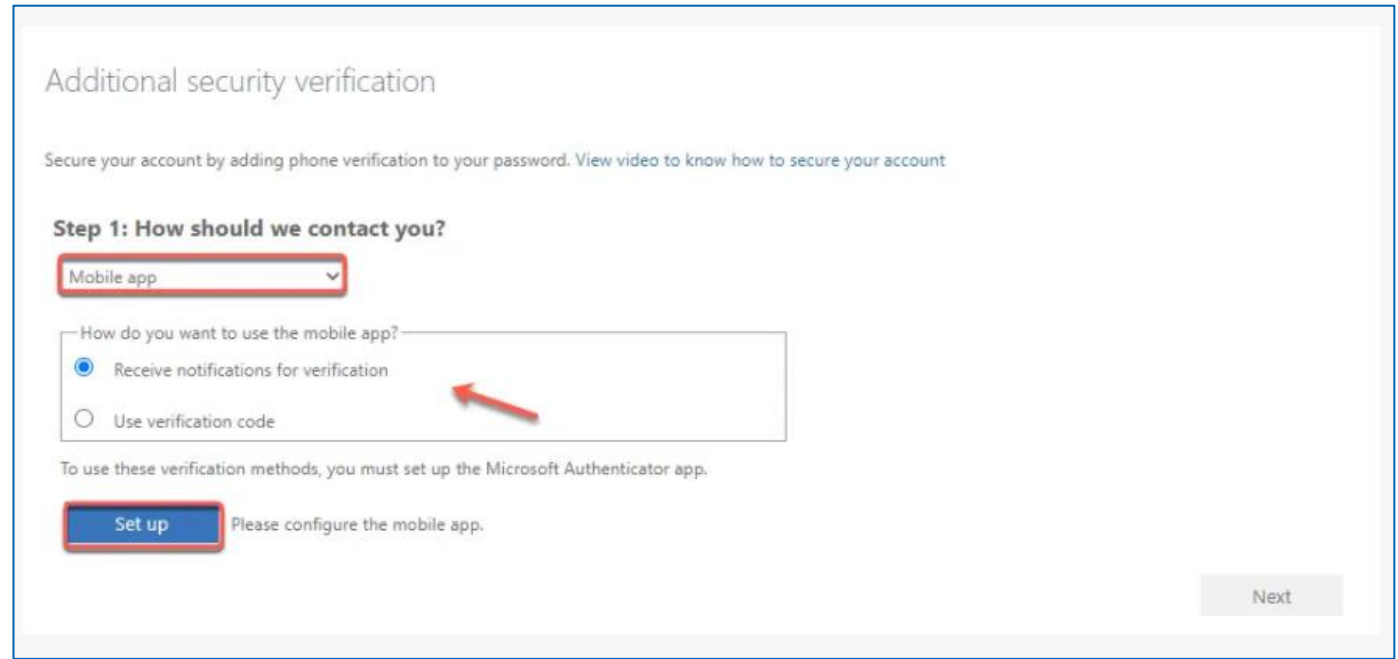
Who are considered  
Public Officers

Public Officer with WOG email account (ie. gov.sg)

Vendors with WOG email account (ie. gov.sg)

# 1a. Set up Security Verification for WOG Account <Public Officer>

- This step is mandatory for public officers who will be accessing SGTS services using their GMD and whose **SG Govt M365** profile is not displayed in their Microsoft Authenticator app. Others may skip this and proceed to [Step 2. Sign Up for a TechPass Account](#).
- Public officers need to set up security verification (multi-factor authentication) for their Whole-of-Government (WOG) account to access Singapore Government Technology Stack (SGTS) services and tools from their GMD device.
- To set up security verification for WOG account, go to [Azure Active Directory](#) in the non-SE GSIB device.
- If you are prompted to sign in, use your organisation email address and GSIB device password.
- Select **Mobile app** as the preferred authenticating method, and we strongly recommend you to choose **Receive notifications for verification**.
- Click **Set up**.



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** Please configure the mobile app.

Next


# 1 b. Set up Security Verification for WOG Account <Public Officer>

- Follow the on-screen instructions displayed on the **Configure mobile app** page.
- Once you scan the QR code displayed on your computer screen, your WOG account will be listed on the authenticator app and when you click **Next** your activation status is confirmed.
- In the **Additional security verification** page, click **Next**.
- To verify that you are reachable on your mobile device, a notification is sent to your mobile app. Approve sign-in on the **Authenticator** app.

**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.



Scan the QR code displayed on your computer

[Configure app without notifications](#)

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

Code:

URL:

Click to use other authenticators

If the app displays a six-digit code, choose "New" in the app.

**Next** **Cancel**

**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

Indicates that your Authenticator app is configured for notifications and verification codes

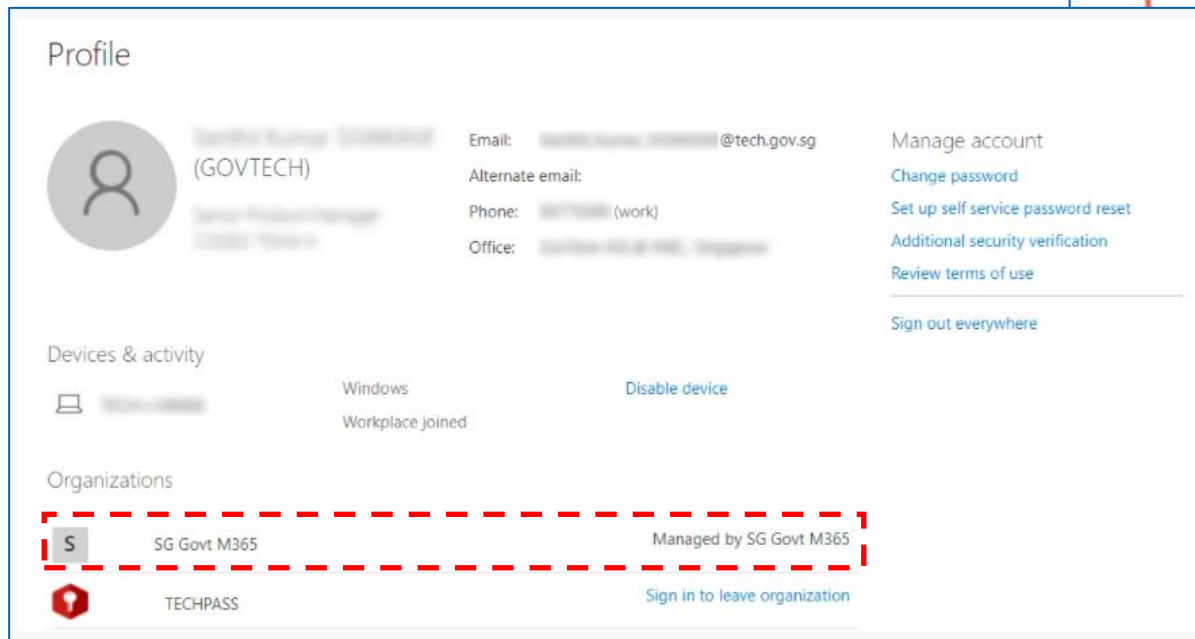
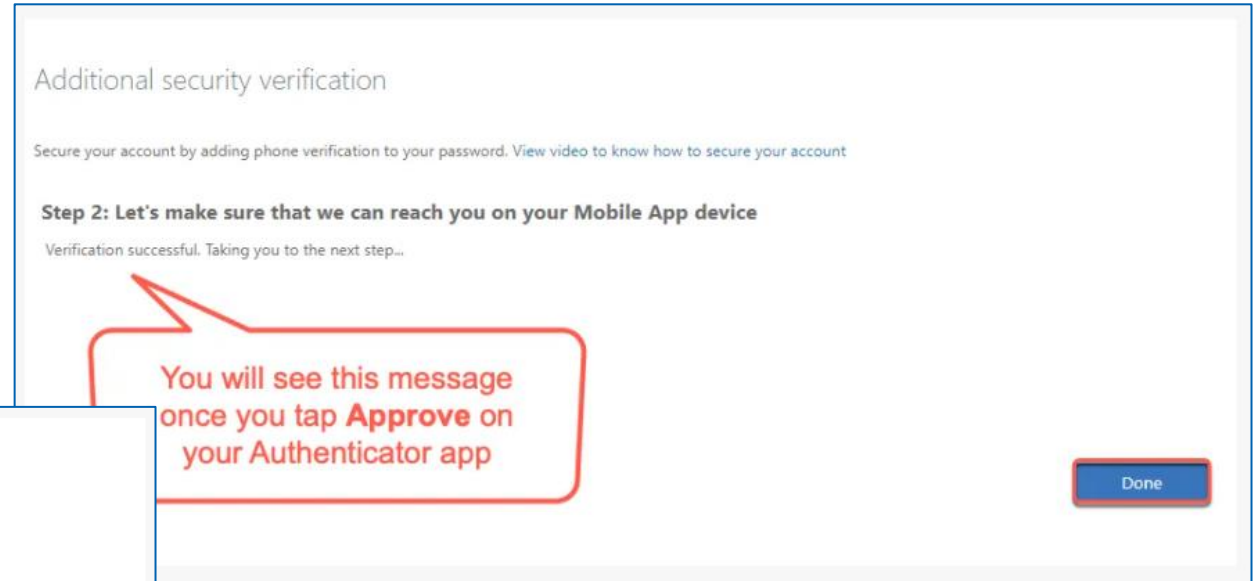
To use these verification methods, you must set up the Microsoft Authenticator app.

**Set up** Mobile app has been configured for notifications and verification codes.

**Next**

# 1c. Set up Security Verification for WOG Account <Public Officer>

- Click **Done**.
- Your **Profile** page is displayed.



## 2a. Sign Up for a TechPass Account < Public Officer >

### Public Officers Using Non SE Machines

Non SE Machines uses Bitlocker for encryption

1. Go to [TechPass portal](#) and click Sign Up.
2. Enter your organisational email address.  
(Format shall be your\_name@agency.gov.sg or your\_name@tech.gov.sg)
3. Indicate if you would require to onboard to SEED (only for non-GSIB device or Internet Device)
4. Select I'm not a robot.
5. Click Submit.
6. An invitation will be sent to this email address.  
Receive SEED onboarding instructions via WoG email for Internet Device if SEED is required.
7. Click on Invitation link.
8. Complete TechPass onboarding.
9. Complete SEED onboarding on Internet Device.

### Public Officers Using Secure Email GSIB Devices

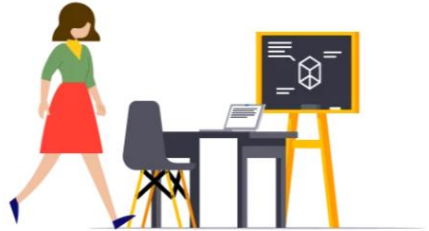
SE GSIB devices uses PSCard for encryption

1. Raise a [service request](#) to request for TechPass account on an Internet Device.
2. Select **Service Request** for ticket request type, **Create TechPass account for Secure Email GSIB users** and confirm that you are a SE GSIB user before submitting the ticket.
3. It takes 3 business days for to provision the TechPass Account.




## 2b. Sign Up for a TechPass Account < Public Officer >

### Public Officers Using Non SE Machines



**Ease of Integration**

Supports industry standard protocols (OAuth 2.0/OIDC & SAML 2.0)



### Sign Up for TechPass

Please take a moment to setup your account.  
Contact your Manager In Charge if you do not have a gov.sg email.


**Email Address**  
This is your official work email.

0/256 characters

**Is onboarding to SEED required?\***

☒ Yes ☐ No

- Please select "Yes" if you will be accessing services from a GMD that require SEED compliance (e.g GCC2.0, SHIP-HATS). Accessing services from GSIB does not require SEED.
- If you select "Yes", do not attempt to onboard your device if you haven't received the SEED onboarding email instructions (approximately 3 working days) because the licenses need to be assigned to you first. (Please check the junk email folder as well.)
- To learn more about SEED, head to the [SEED documentation](#).
- There are a few softwares which if already installed are to be removed before proceeding with SEED onboarding. See [prerequisites](#).

☐ I'm not a robot 

Submit

### Public Officers Using Secure Email GSIB Devices

#### 2. Ticket Request Type

Please select the type of support ticket you like to raise

- ☒ Service Request
- ☐ Incident Request

#### 3. Service Requests

Please select the issue that best describes the assistance you needed.

- ☐ Reset Multi Factor Authentication (MFA)
- ☒ Create TechPass account for Secure Email GSIB users

#### 4. Are you a Secured Email (SE) GSIB user?

SE GSIB user would be holding onto a SE card which is required to access your GSIB

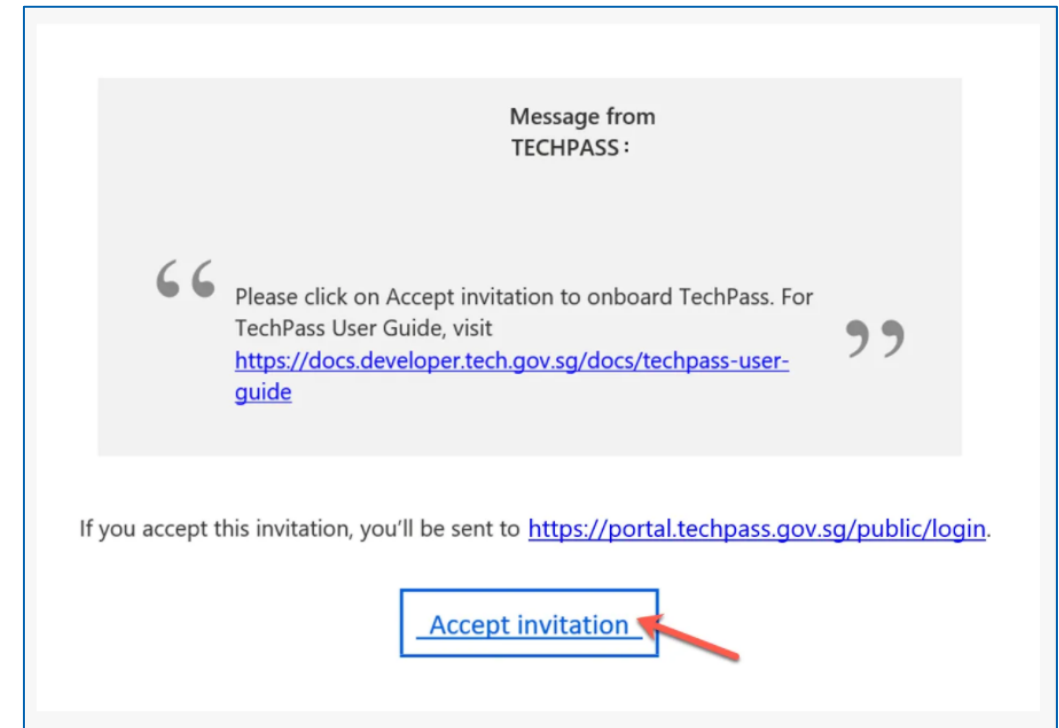
X NO

✓ YES



### 3. Accept Invitation < Public Officer >

- Search for the email with the invitation link in your inbox.
- If you do not see this email in your inbox, check if it is the same email address you provided during sign up, and if a spam filter or email rule moved it to other folders, Junk Email, Deleted Items or Archive folder.
- Click **Accept invitation** and proceed with Onboarding to TechPass.

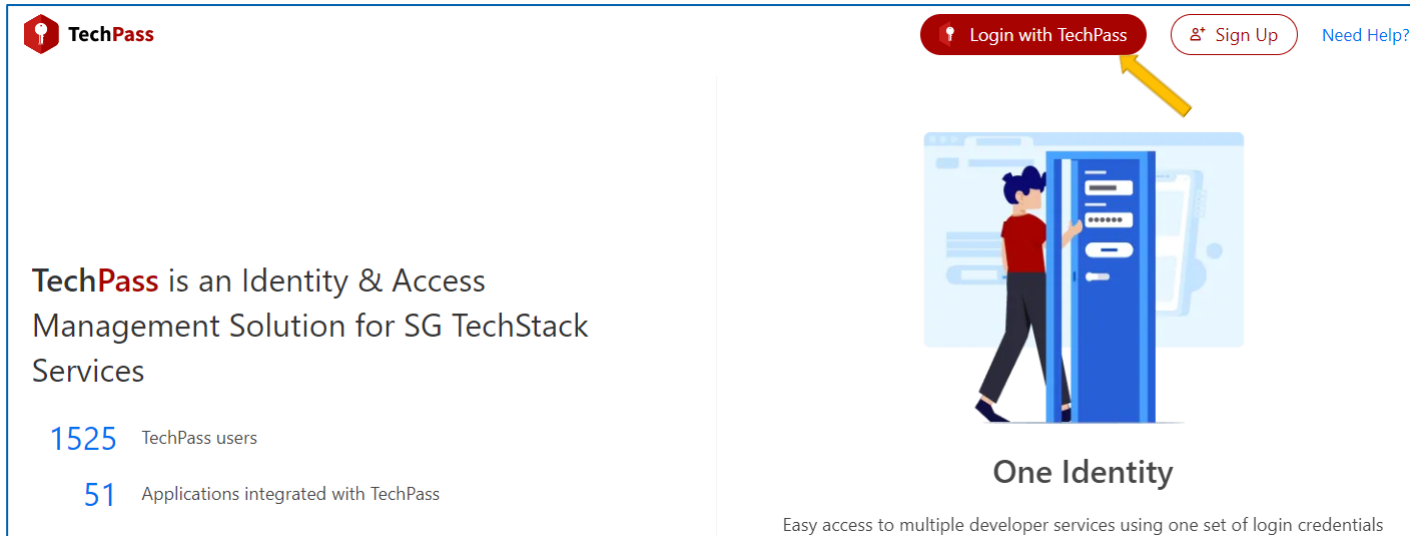


**Note :**

- Public officer has to accept this invitation within 30 days to onboard to TechPass. Invitation is not valid after 30 days and you need to sign up again for a TechPass account.
- Once you've started the TechPass onboarding process, it is important to complete it within the same session.

## 4a. Onboard TechPass < Public Officer >

- If you are already signed in to your WOG account, when you accept the TechPass invitation, you will be directed to **Review Permissions**. Click **Accept**.
- If you are not signed in to your WOG account while accepting the invitation, you will be prompted to sign in before proceeding further.
- Click **Log in with TechPass**.



**TechPass** is an Identity & Access Management Solution for SG TechStack Services

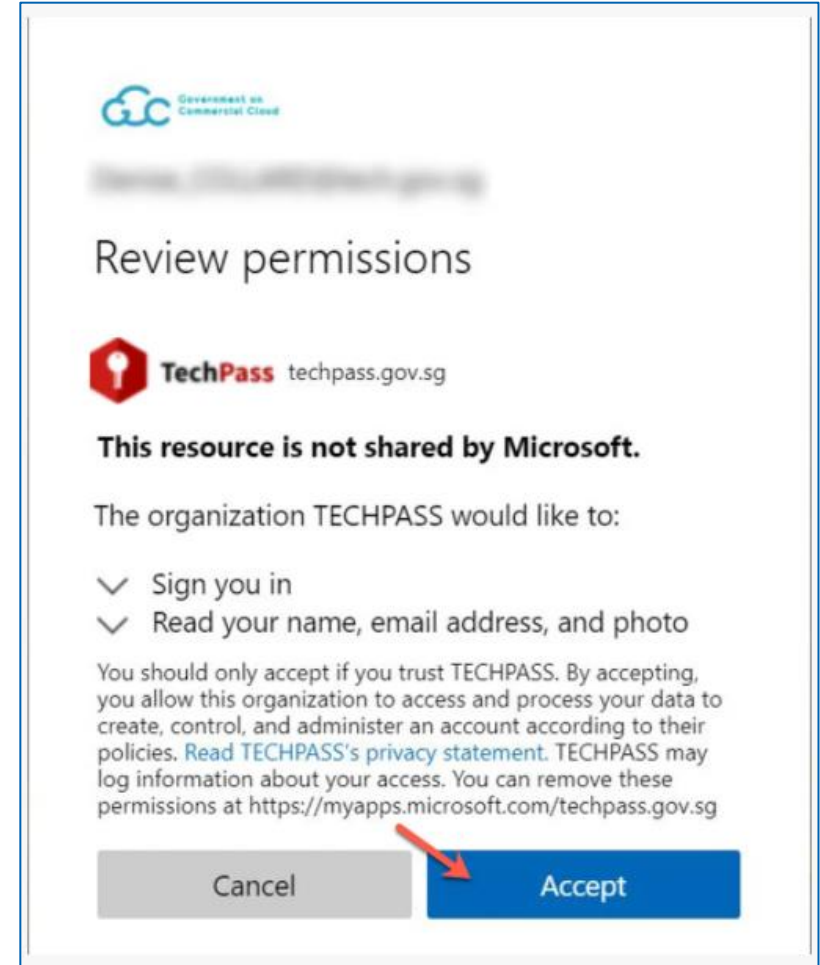
1525 TechPass users

51 Applications integrated with TechPass

**One Identity**

Easy access to multiple developer services using one set of login credentials

Login with TechPass Sign Up Need Help?



**Review permissions**

**TechPass** techpass.gov.sg

**This resource is not shared by Microsoft.**

The organization TECHPASS would like to:

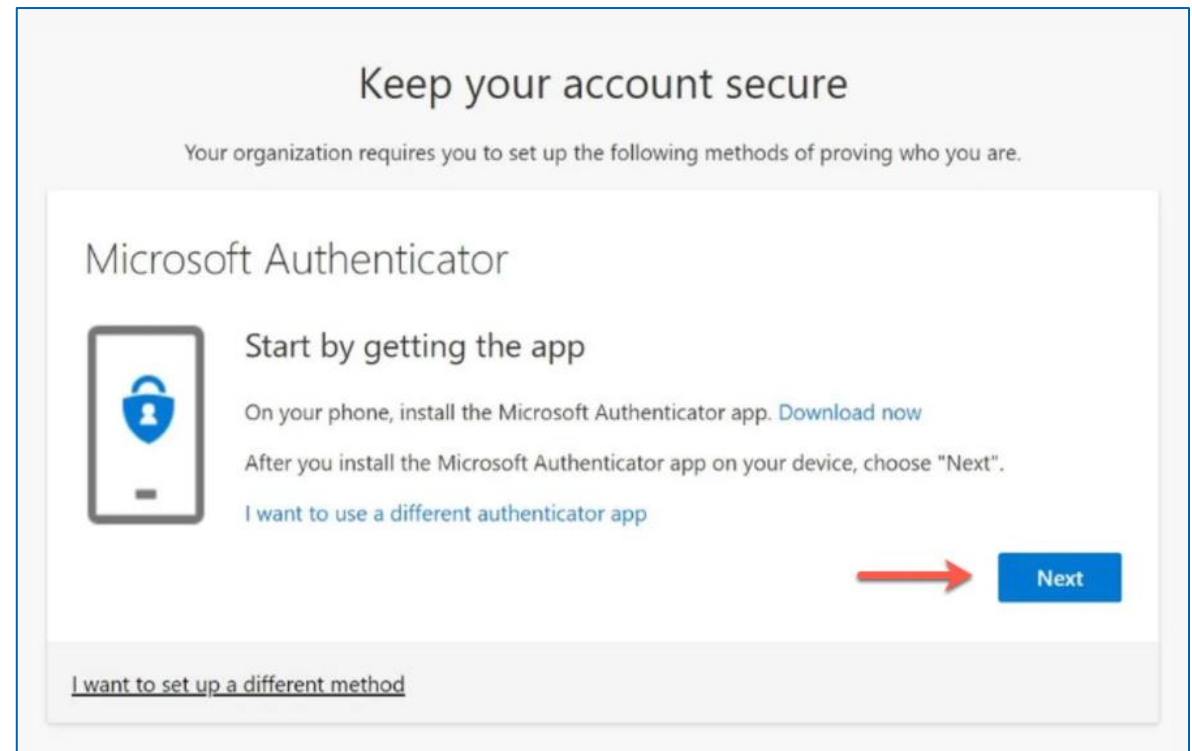
- ✓ Sign you in
- ✓ Read your name, email address, and photo

You should only accept if you trust TECHPASS. By accepting, you allow this organization to access and process your data to create, control, and administer an account according to their policies. [Read TECHPASS's privacy statement](#). TECHPASS may log information about your access. You can remove these permissions at <https://myapps.microsoft.com/techpass.gov.sg>

Cancel Accept

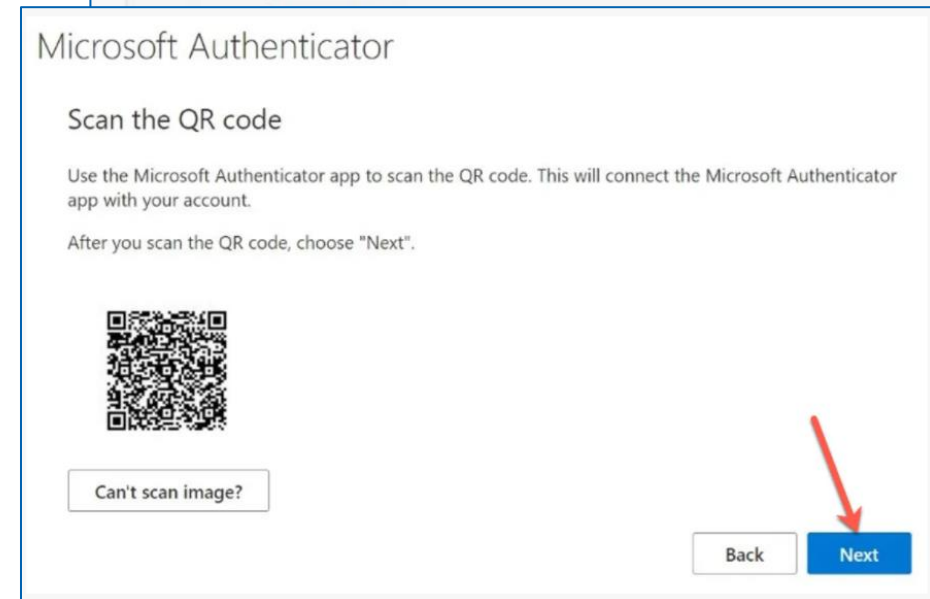
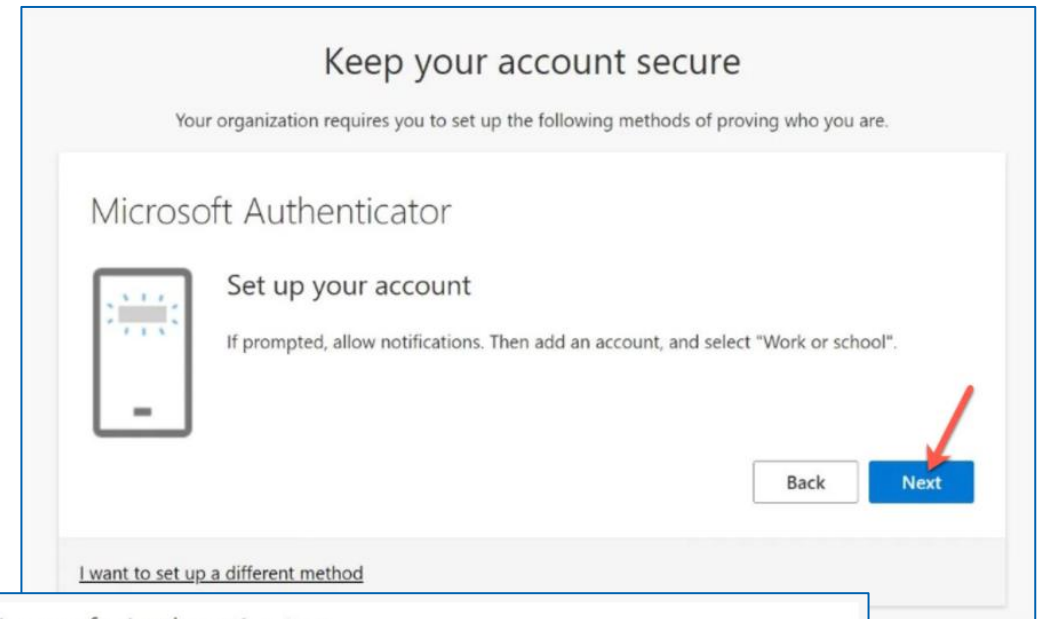
## 4a. Onboard TechPass < Public Officer >

- Click **Next**.
- Ensure that the email address which you used to sign up for TechPass account is displayed as username.
- Choose one of the following options and click **Next**.
  - If you do not have Microsoft Authenticator app(recommended) on your mobile phone, download and install it on your [Microsoft phone](#), [Android](#) or [iOS phone](#) and complete the wizard.
  - To use other authenticators, click **I want to use a different authenticator app**.
  - To use other methods, click **I want to setup a different method**.



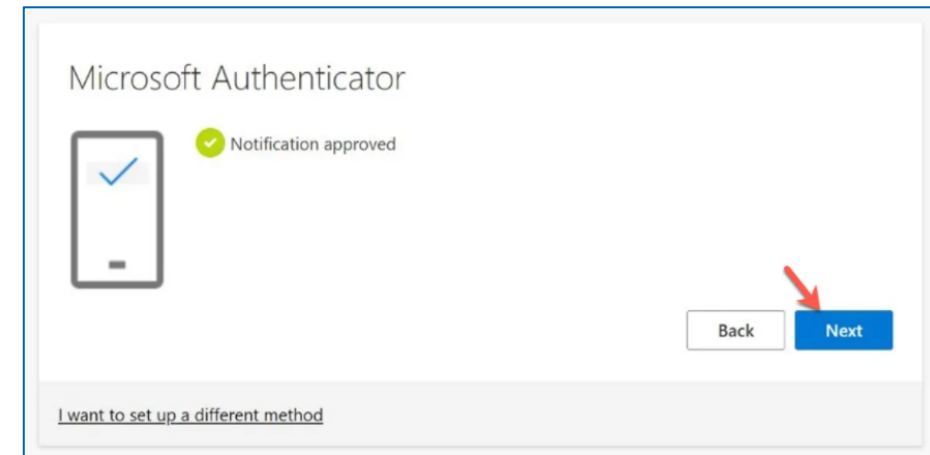
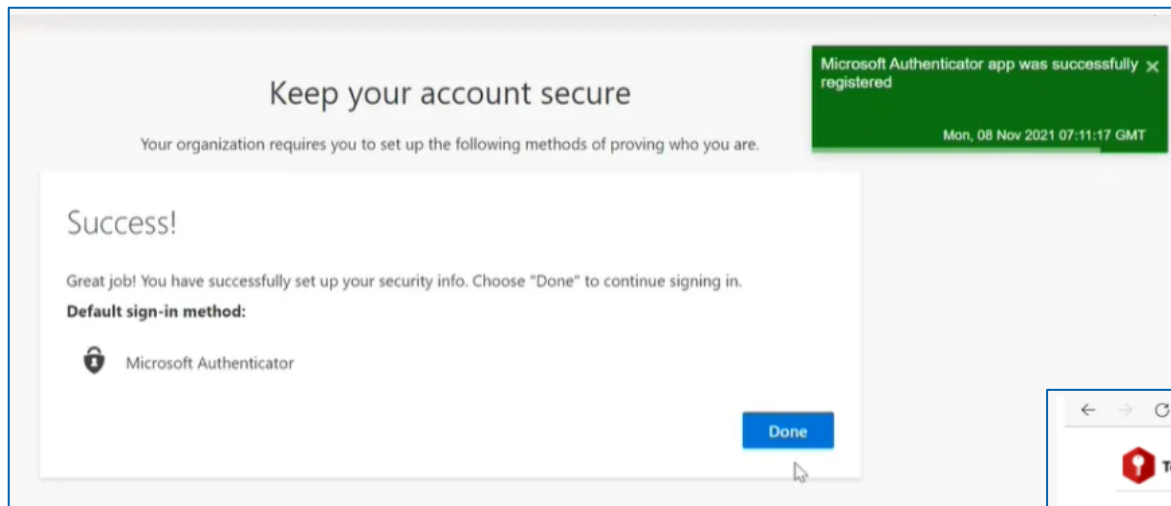
## 4b. Onboard TechPass < Public Officer >

- As we recommend Microsoft Authenticator, we will provide guidance for you to set up multi-factor authentication for your TechPass account using that. For other authenticators, refer to the respective help resources.
- In your mobile device, open Microsoft **Authenticator** and tap + **Add account** > **Work or School account**.
- Go back to your computer and click **Next**.
- Scan the QR code displayed on your computer screen and click **Next**. Your TechPass account gets activated and linked to the authenticator app.
- Authenticator will send a notification for you to approve and confirm if this verification was set up correctly.
- Tap **APPROVE** on your mobile device and on your computer, you will see that you have approved your sign-in.

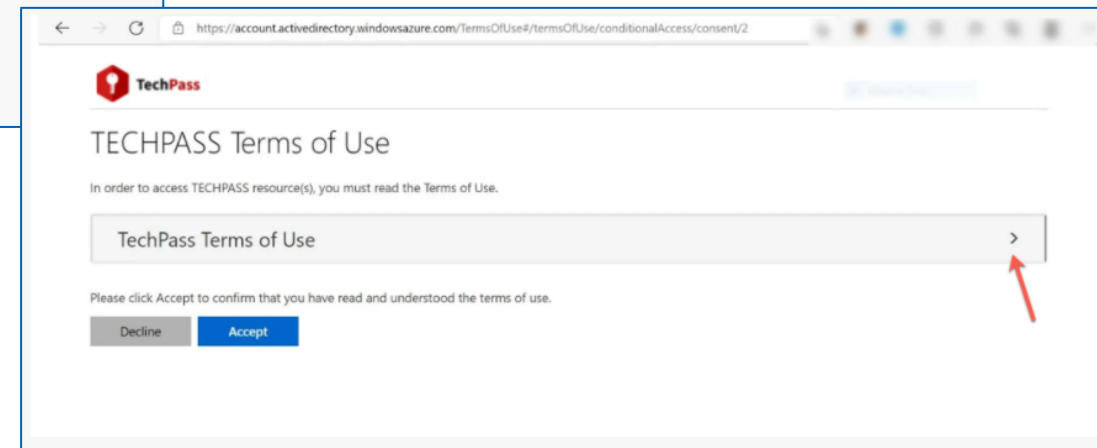


## 4c. Onboard TechPass < Public Officer >

- Click **Next**.
- When you see the success message, click **Done**. You will now be directed to the Terms of Use page.

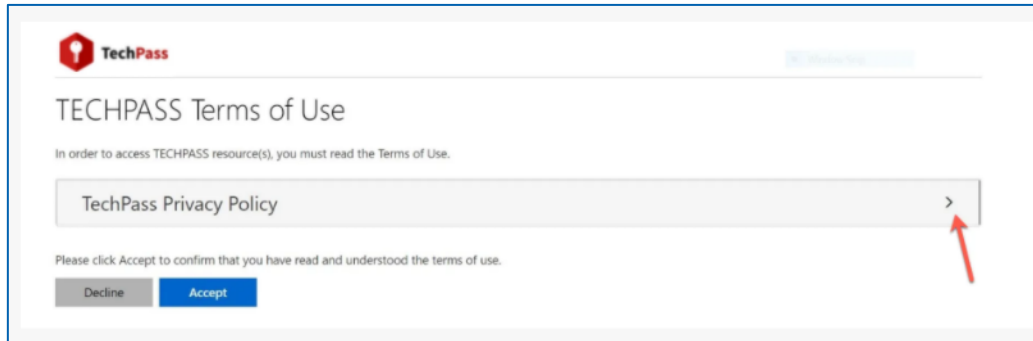


- Click the arrow to view the TechPass Terms of Use.

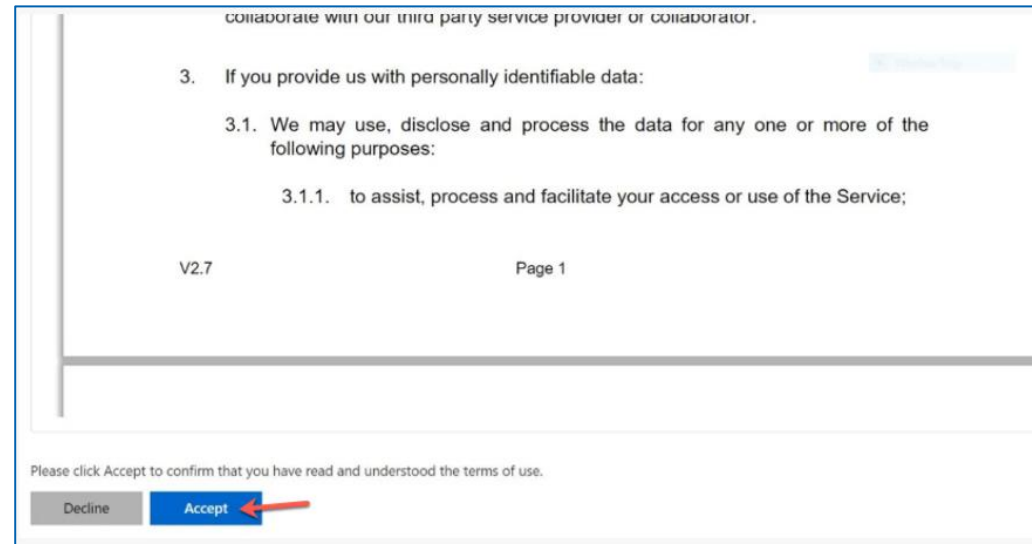
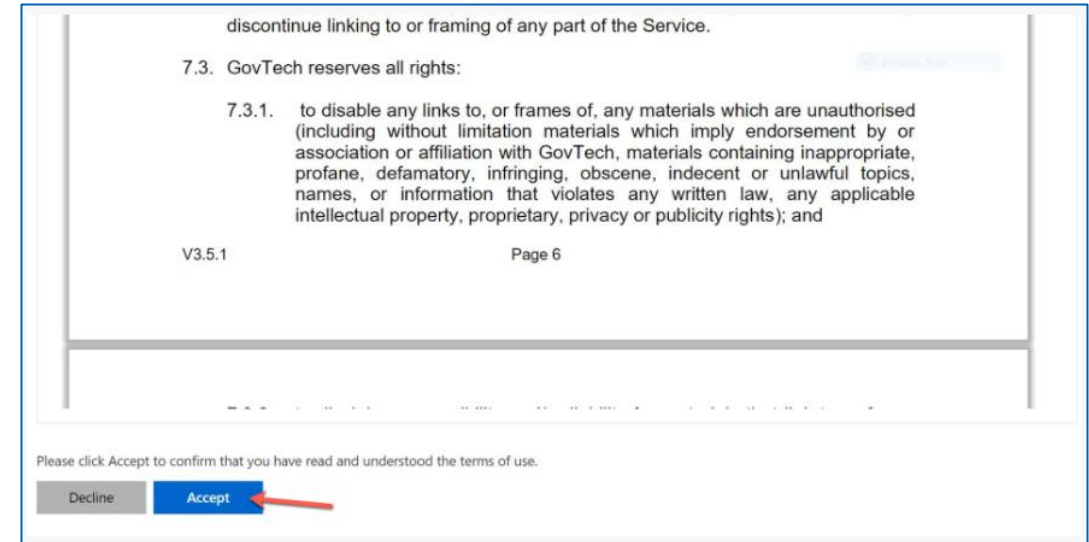


## 4d. Onboard TechPass < Public Officer >

- Read the TechPass **Terms of Use** and click **Accept**.
- Click the arrow to view the **TechPass Privacy Policy**.



- Read the TechPass **Privacy Policy** and click **Accept**.





## 4e. Onboard TechPass < Public Officer >

- Click the arrow to view the **TechPass MDM AUP Policy**.
- Read the policy details and click **Accept**.

**Organizational Protocol**

1. GovTech can and will establish audit trails, which will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to the network, and the resulting reports may be used for investigation of possible breaches and/or misuse. **The Agency and end user agree to and accepts that his or her access and/or connection to GovTech's networks may be monitored to record dates, times, duration of access, etc. in order to identify unusual usage patterns or other suspicious activity. The status of the device, including location, IP address, Serial Number, IMEI, may also be monitored.** This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties or users who are not complying with GovTech's policies.
2. The end user agrees to **immediately report** to his/her manager and GovTech **any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.**

**Policy Non-Compliance**

Failure to comply with the *Mobile Device Management (SEED) Acceptable Use Policy* may result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment or of the relevant vendor contract, by GovTech or the relevant Agency.

By selecting **"ACCEPT"** below it is deemed that you have read, understood and agree to all the provisions in this AUP. This AUP shall apply to you throughout the period that your device is provisioned with SEED and onboarded as a GMD. Any obligations herein that expressly or by their nature survive the cessation of your device as a GMD shall continue to survive.

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

**TechPass**

### TECHPASS Terms of Use

In order to access TECHPASS resource(s), you must read the Terms of Use.

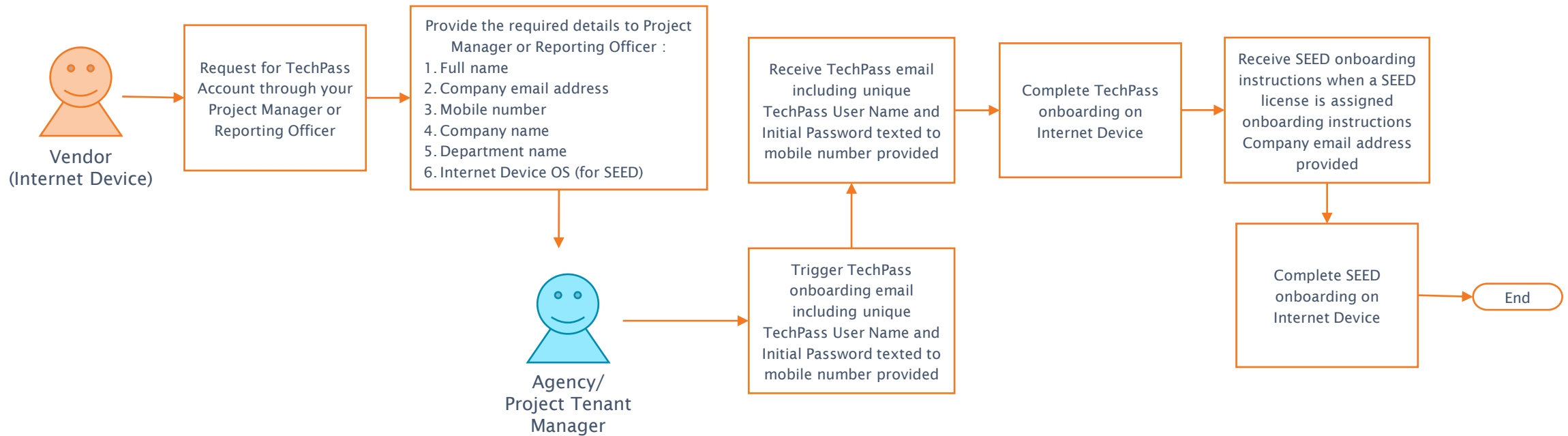
TechPass MDM AUP >

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

- You have now successfully onboarded to TechPass. You may now proceed to onboard your non-GSIB device to SEED.



# Typical Onboarding Flow < Vendor >





# Onboarding to TechPass < Vendor >

## Vendors



## Who are considered Vendors

Public Officer with non-WOG email account (eg. edu.sg, etc.)

Vendors with Vendor company email

# 1. Sign Up for a TechPass Account < Vendor >

## Vendors Using Non SE Machines

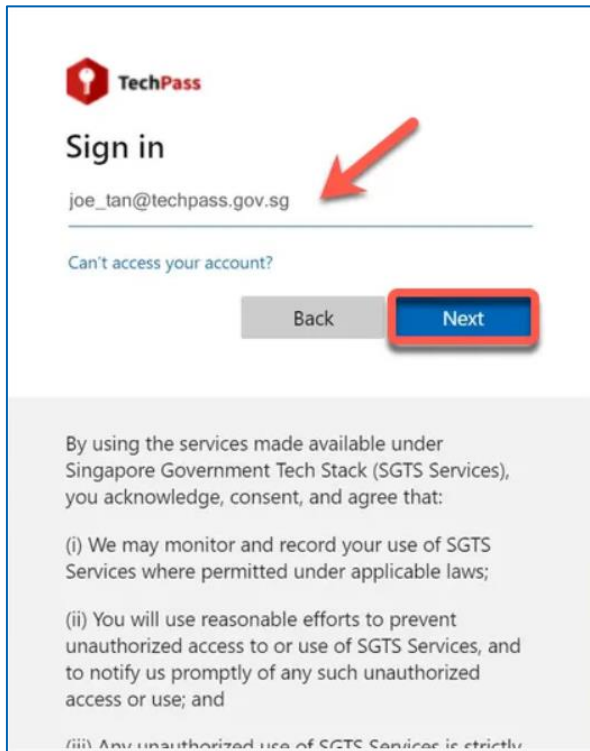
1. Go to [TechPass portal](#) and click Sign Up.
2. Enter your organisational email address.  
(Format shall be your\_name\_from.vendor@agency.gov.sg or your\_name\_from.vendor@tech.gov.sg)
3. Indicate if you would require to onboard to SEED (only for non-GSIB device or Internet Device)
4. Select I'm not a robot.
5. Click Submit.
6. An invitation will be sent to this email address. Receive SEED onboarding instructions via WoG email for Internet Device if SEED is required.
7. Click on Invitation link.
8. Complete TechPass onboarding.
9. Complete SEED onboarding on Internet Device.

## Vendors Using Internet Devices

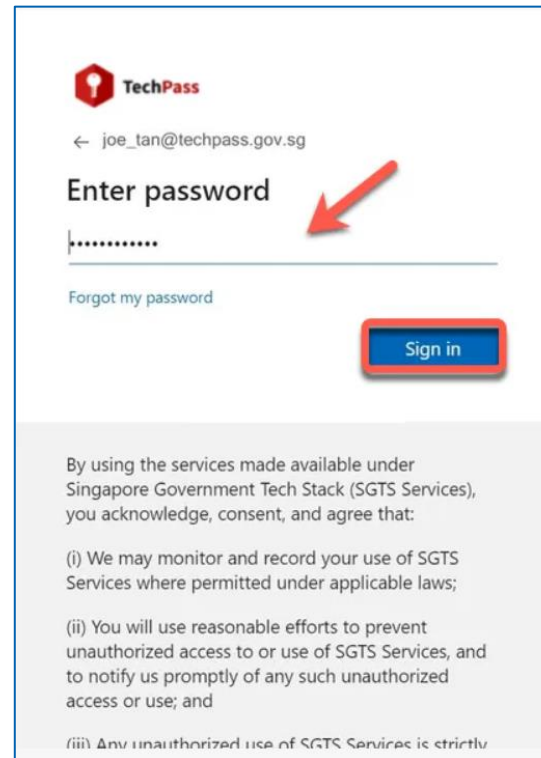
1. Request for TechPass Account and SEED license through your Project Manager or Reporting Officer.
2. Provide the required details to Project Manager or Reporting Officer :
  - Full name
  - Company email address
  - Mobile number
  - Company name
  - Department name
  - Internet Device OS (for SEED)
3. Receive TechPass email including unique TechPass User Name and Initial Password texted to mobile number provided.
4. Receive SEED onboarding instructions when a SEED licence is assigned onboarding instructions Company email address provided.
5. Complete SEED onboarding on Internet Device.

## 2. First-time Sign in Using Initial Password < Vendor >

- Go to the web address(url) provided by your project manager or reporting officer to sign in to SGTS service using your TechPass account.
- Enter your TechPass username and click **Next**.
- Enter the initial password and click **Sign in**. You will now be directed to configure MFA for your TechPass account.



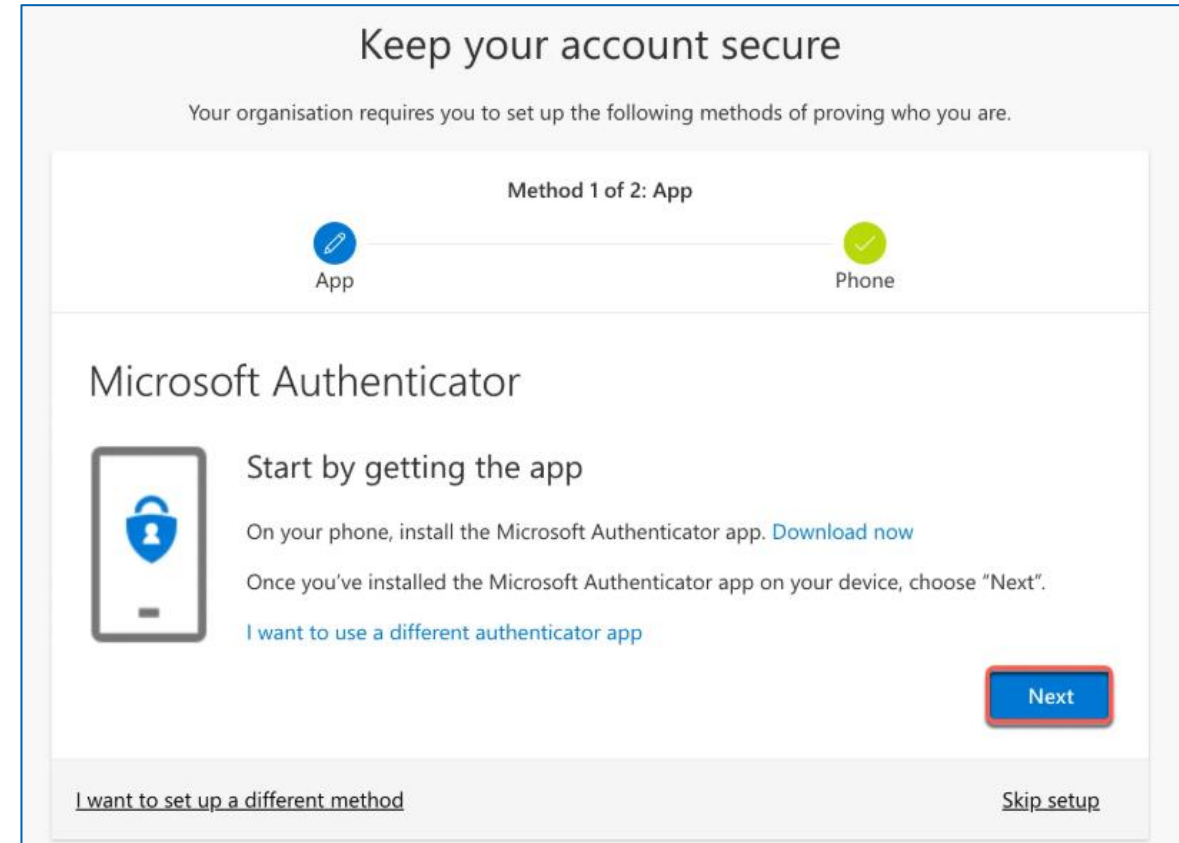
The screenshot shows the TechPass 'Sign in' page. At the top is the TechPass logo. Below it, the text 'Sign in' is displayed. A text input field contains the email 'joe\_tan@techpass.gov.sg', with a red arrow pointing to it. Below the input field is a link that says 'Can't access your account?'. At the bottom of the form area are two buttons: a grey 'Back' button and a blue 'Next' button with a red border. Below the form is a grey box containing a consent statement: 'By using the services made available under Singapore Government Tech Stack (SGTS Services), you acknowledge, consent, and agree that:'. This is followed by three bullet points: (i) We may monitor and record your use of SGTS Services where permitted under applicable laws; (ii) You will use reasonable efforts to prevent unauthorized access to or use of SGTS Services, and to notify us promptly of any such unauthorized access or use; and (iii) Any unauthorized use of SGTS Services is strictly prohibited.



The screenshot shows the TechPass 'Enter password' page. At the top is the TechPass logo. Below it, the text 'Enter password' is displayed. Above the password input field is the email 'joe\_tan@techpass.gov.sg' with a back arrow. The password field contains masked characters '.....', with a red arrow pointing to it. Below the input field is a link that says 'Forgot my password'. At the bottom of the form area is a blue 'Sign in' button with a red border. Below the form is a grey box containing a consent statement: 'By using the services made available under Singapore Government Tech Stack (SGTS Services), you acknowledge, consent, and agree that:'. This is followed by three bullet points: (i) We may monitor and record your use of SGTS Services where permitted under applicable laws; (ii) You will use reasonable efforts to prevent unauthorized access to or use of SGTS Services, and to notify us promptly of any such unauthorized access or use; and (iii) Any unauthorized use of SGTS Services is strictly prohibited.

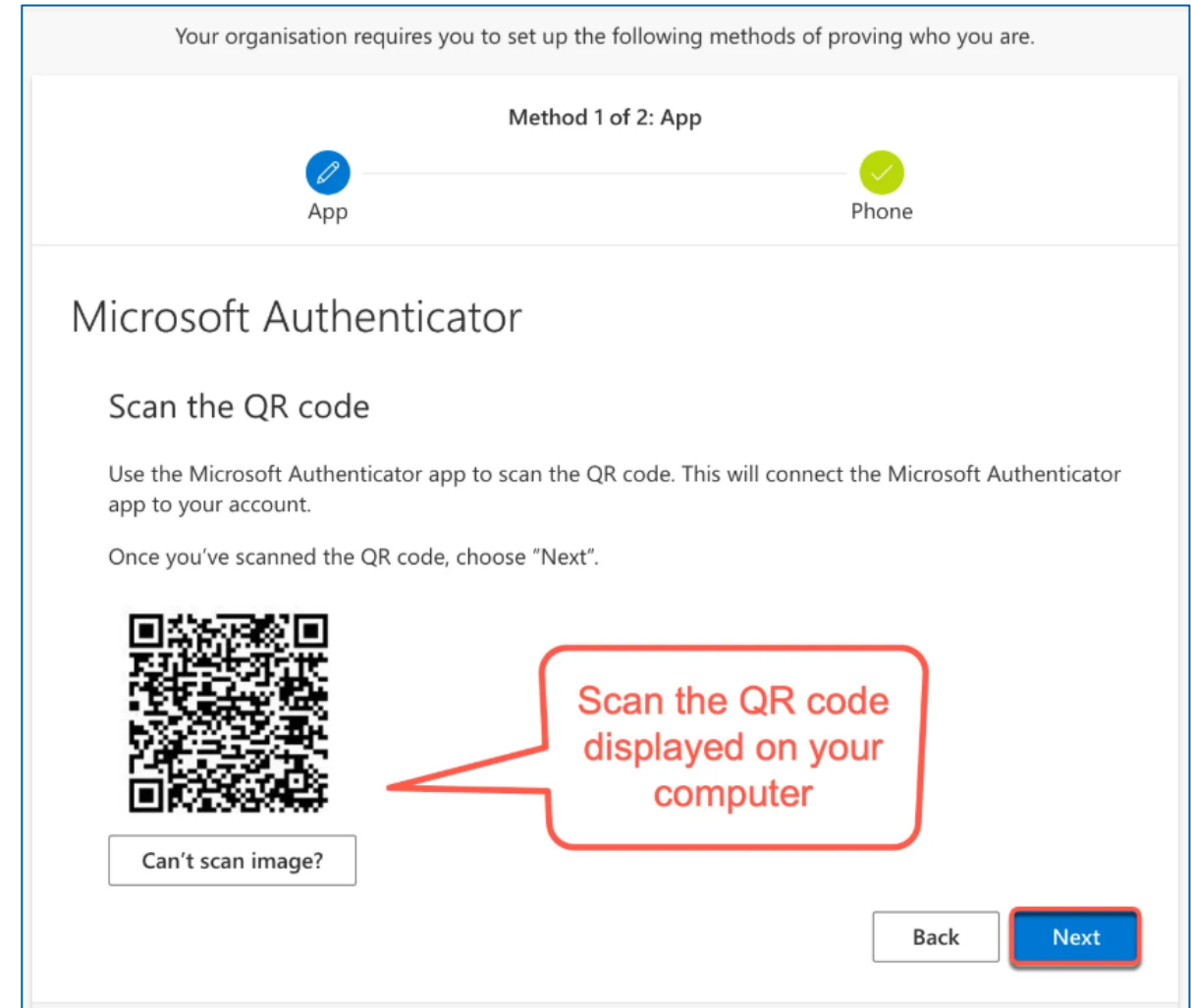
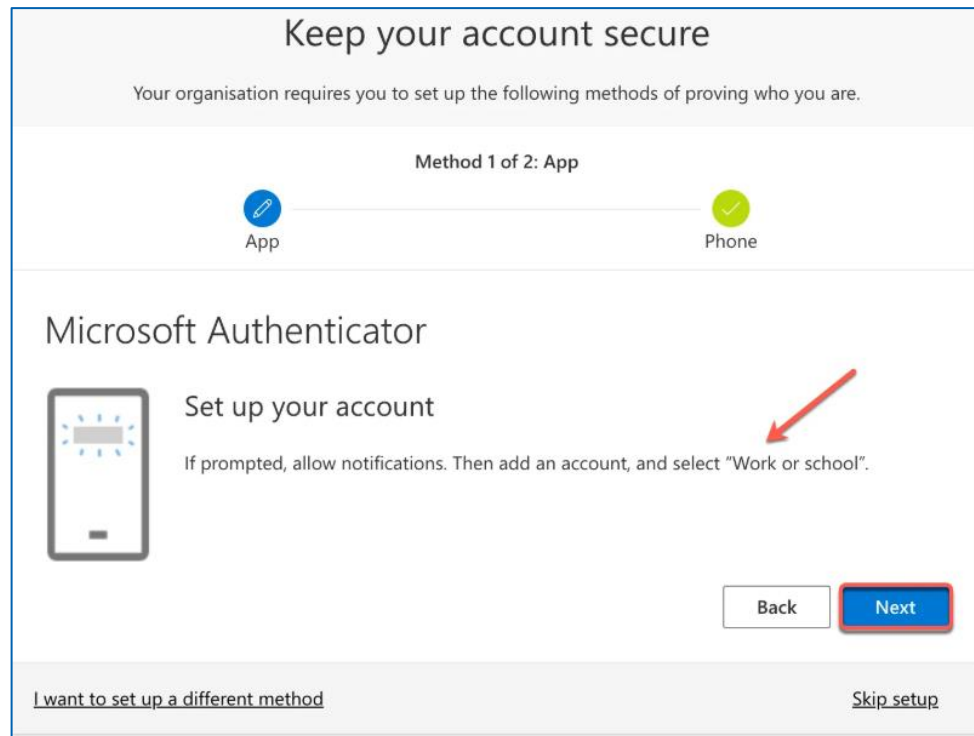
## 3a. Configure and Verify MFA for TechPass Account < Vendor >

- Install an authenticator on your mobile device. If you do not have Microsoft Authenticator app(recommended) on your mobile phone, download and install it on your Microsoft phone, Android or iOS phone and complete the wizard.
- As we recommend Microsoft Authenticator, we will provide guidance for you to set up multi-factor authentication for your TechPass account using that. For other authenticators, refer to the respective help resources.
- On your mobile device, open Microsoft **Authenticator** and tap + **Add account** > **Work or School account**.
- Tap Scan a **QR code**.



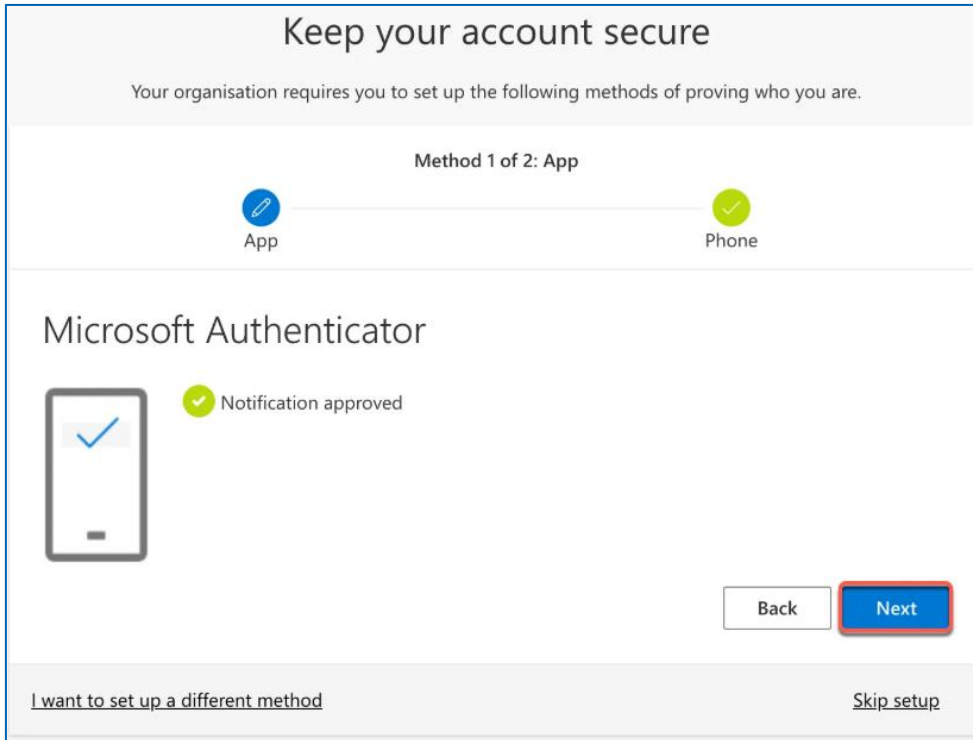
## 3b. Configure and Verify MFA for TechPass Account < Vendor >

- Go back to your computer and click **Next**.
- Scan the QR code displayed on your computer screen and click **Next**. Your TechPass account gets activated and linked to the authenticator app.



## 3c. Configure and Verify MFA for TechPass Account < Vendor >

- To confirm if this verification process was set up correctly, the Authenticator sends a notification to your mobile device.
- Tap **APPROVE** on your mobile device and on your computer, you will see that you have approved your sign-in.



Keep your account secure

Your organisation requires you to set up the following methods of proving who you are.

Method 1 of 2: App

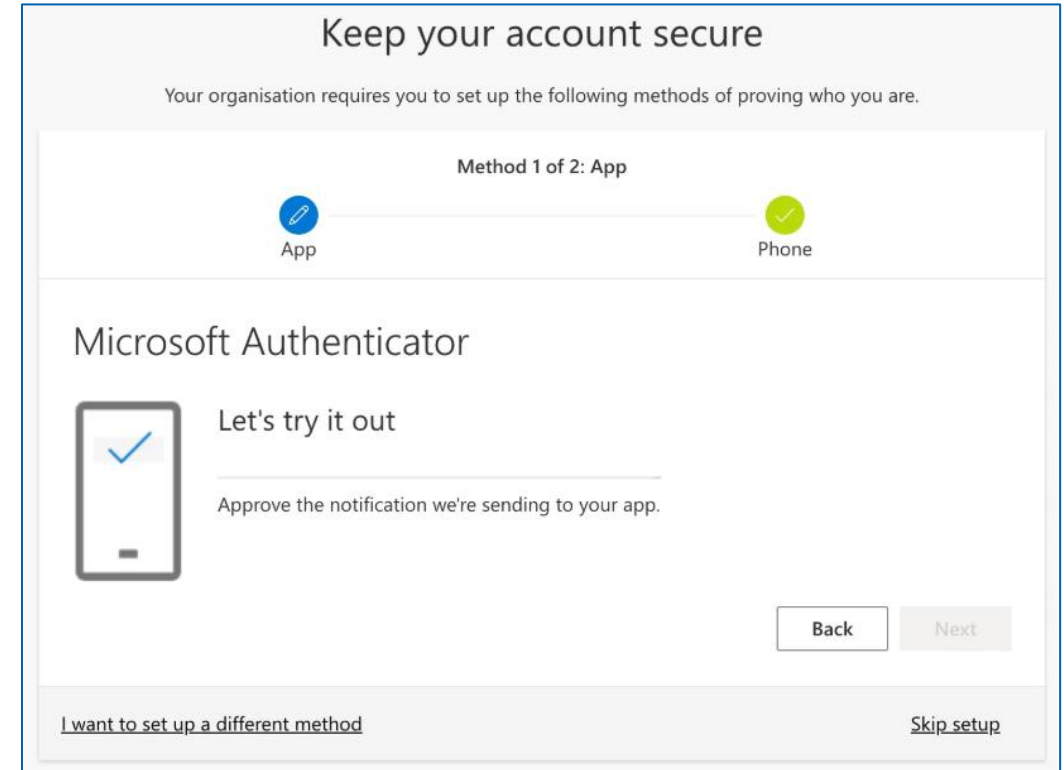
App Phone

Microsoft Authenticator

Notification approved

Back Next

[I want to set up a different method](#) [Skip setup](#)



Keep your account secure

Your organisation requires you to set up the following methods of proving who you are.

Method 1 of 2: App

App Phone

Microsoft Authenticator

Let's try it out

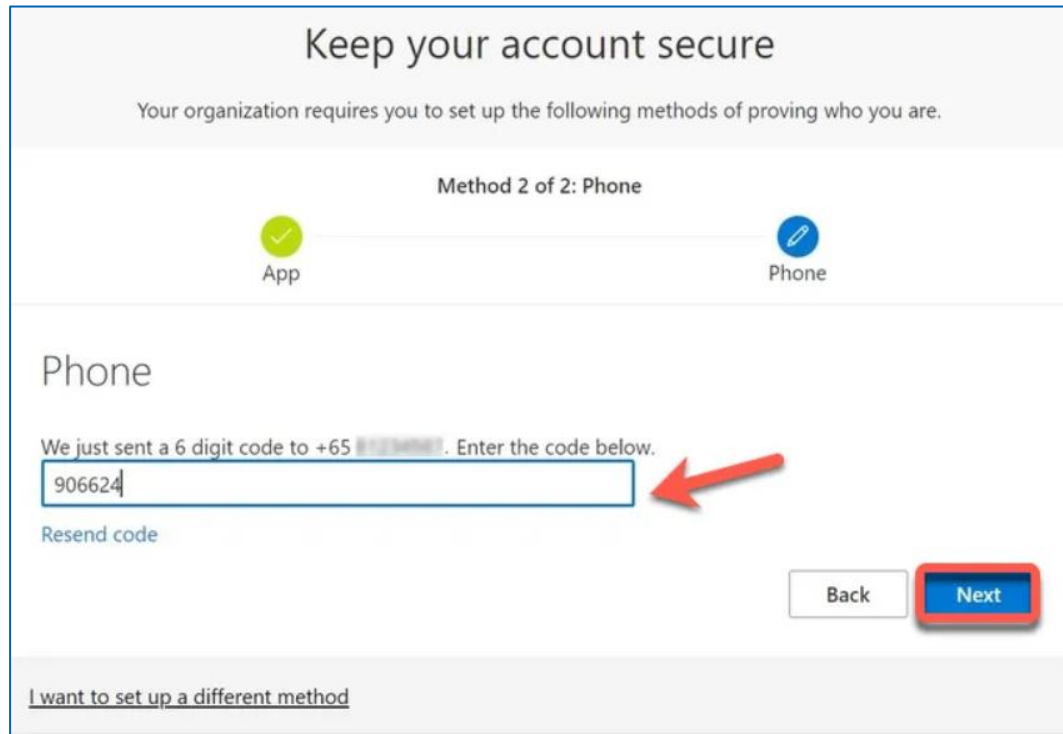
Approve the notification we're sending to your app.

Back Next

[I want to set up a different method](#) [Skip setup](#)

### 3d. Configure and Verify MFA for TechPass Account < Vendor >

- On your computer, click **Next**.
- Choose the country code and enter your handphone number.
- You will receive a six-digit code on this phone number. Enter the six-digit code and click **Next**.



Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 2 of 2: Phone

App Phone

Phone

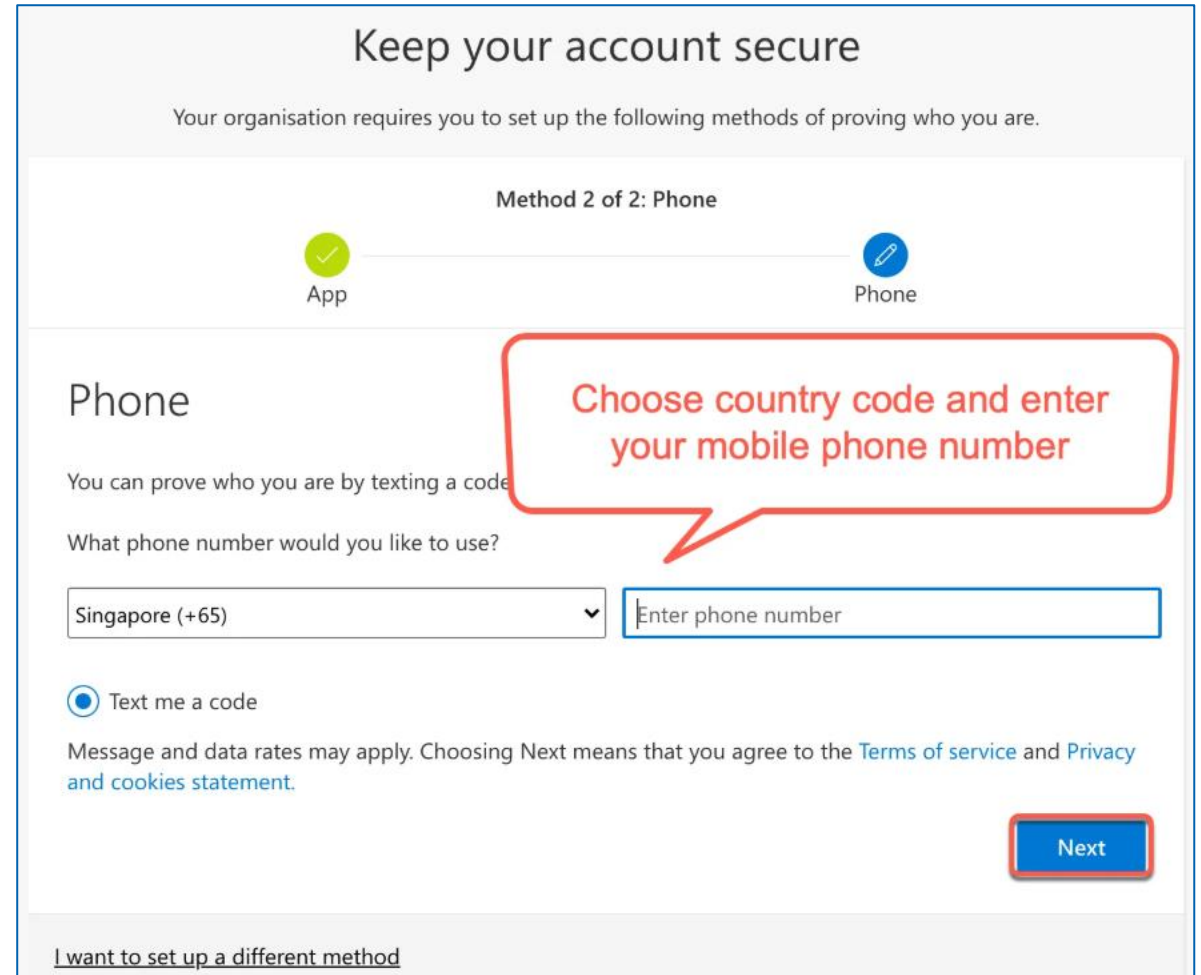
We just sent a 6 digit code to +65 [REDACTED]. Enter the code below.

906624

Resend code

Back Next

[I want to set up a different method](#)



Keep your account secure

Your organisation requires you to set up the following methods of proving who you are.

Method 2 of 2: Phone

App Phone

Phone

You can prove who you are by texting a code

What phone number would you like to use?

Singapore (+65) Enter phone number

☒ Text me a code

Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).

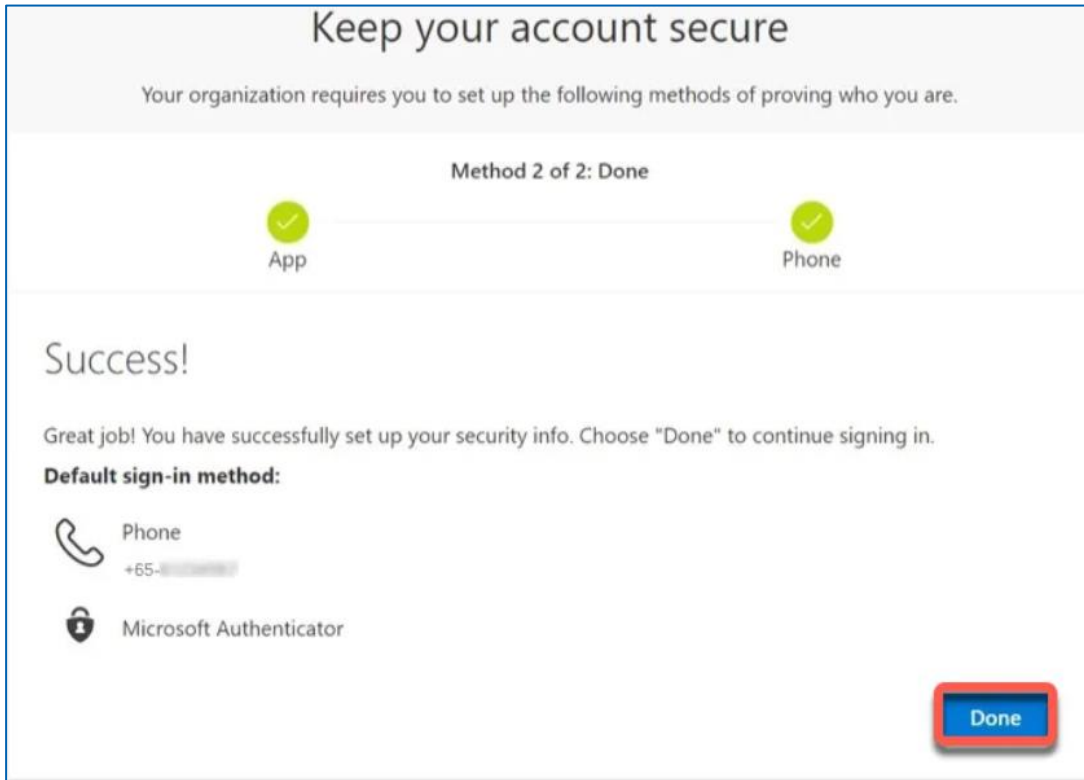
Next

[I want to set up a different method](#)



## 3e. Configure and verify MFA for TechPass account < Vendor >

- Click **Next**.
- When you see a success message, click **Done**.
- Now you will be prompted to reset your initial password.



**Keep your account secure**

Your organization requires you to set up the following methods of proving who you are.

Method 2 of 2: Done

App Phone

**Success!**

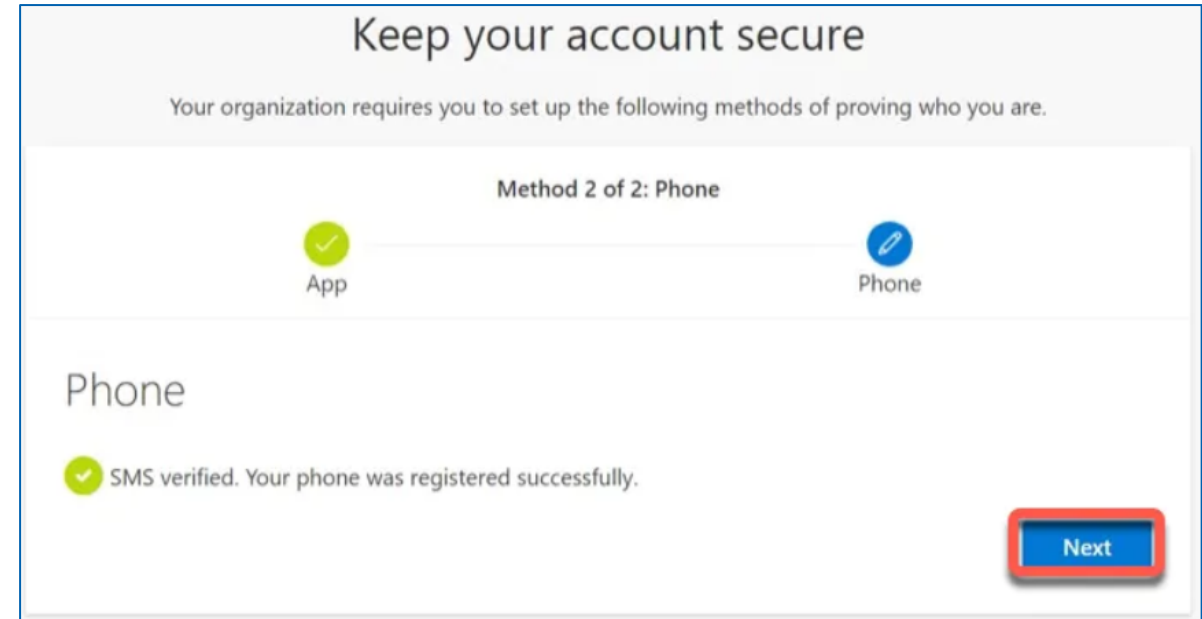
Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

**Default sign-in method:**

Phone  
+65-91234567

Microsoft Authenticator

**Done**



**Keep your account secure**

Your organization requires you to set up the following methods of proving who you are.

Method 2 of 2: Phone

App Phone

**Phone**

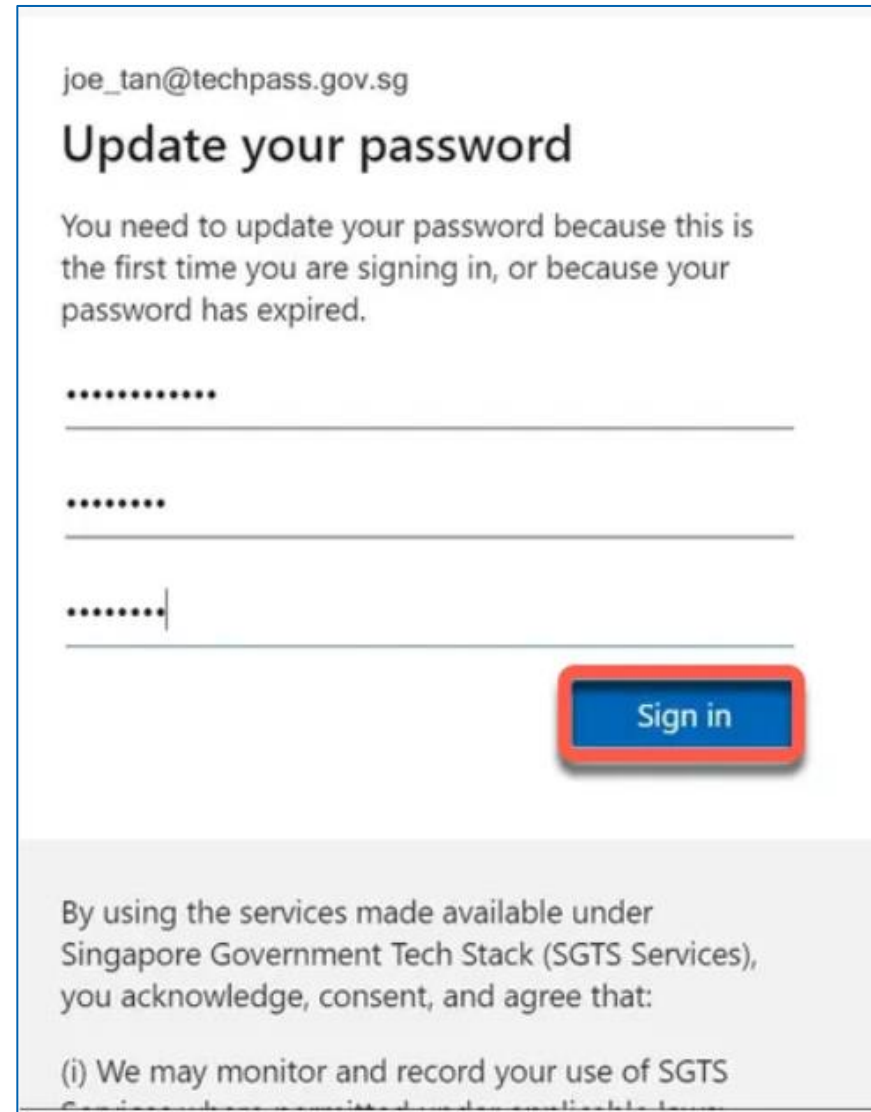
SMS verified. Your phone was registered successfully.

**Next**



## 4. Reset Your Initial Password < Vendor >

1. Enter your **initial password**, **new password** and retype the new password to confirm.
2. Click **Sign in** to proceed with Terms of Use.



joe\_tan@techpass.gov.sg

### Update your password

You need to update your password because this is the first time you are signing in, or because your password has expired.

.....

.....

.....|

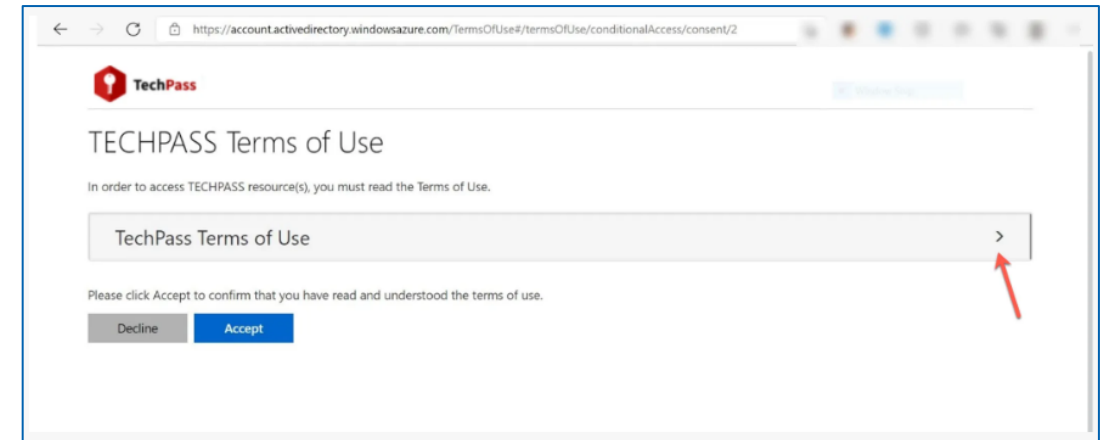
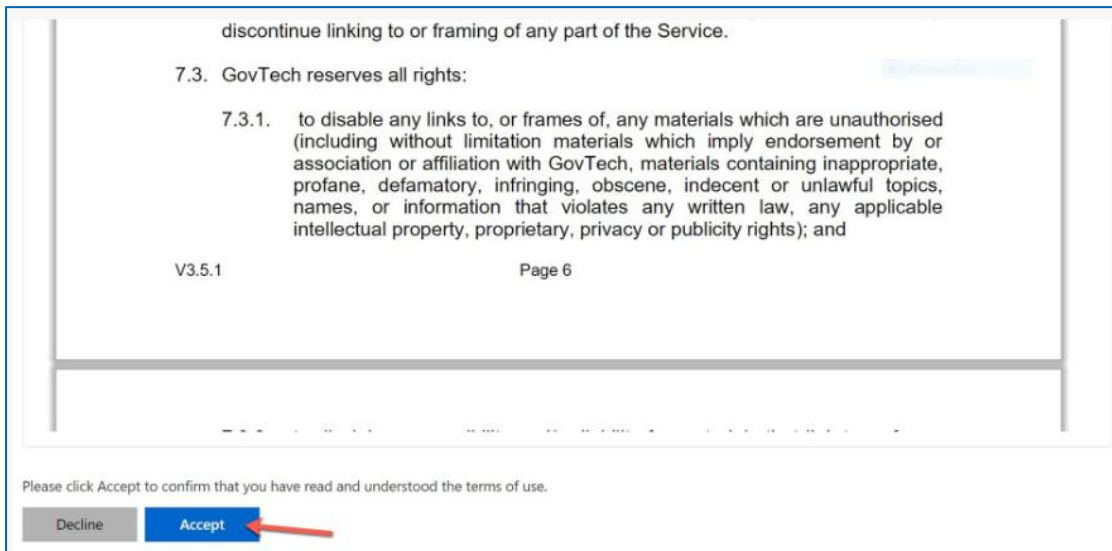
**Sign in**

By using the services made available under Singapore Government Tech Stack (SGTS Services), you acknowledge, consent, and agree that:

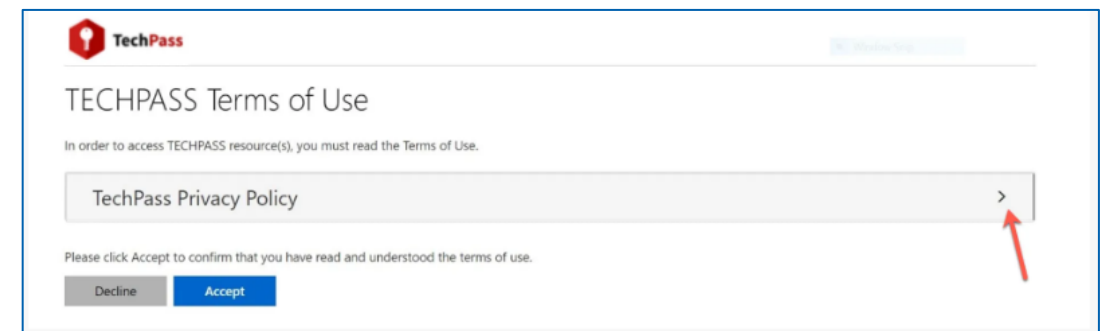
(i) We may monitor and record your use of SGTS

## 5a. Accept Terms of Use, Privacy Policy and Mobile Device Management-Acceptable Use Policy < Vendor >

- Click the arrow to view the **TechPass Terms of Use**.
- Read the TechPass **Terms of Use** and click **Accept**.

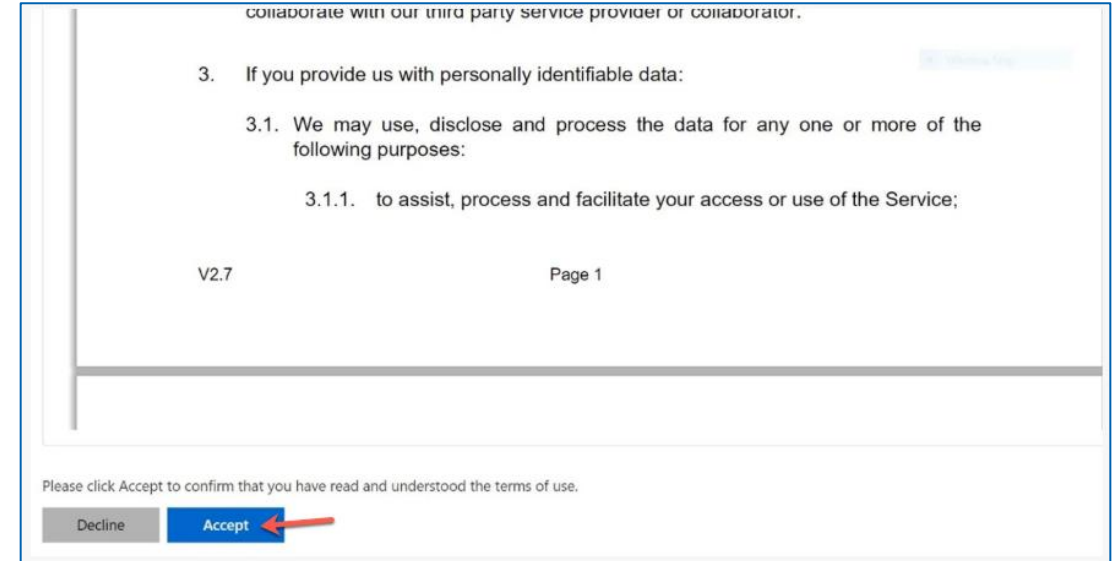
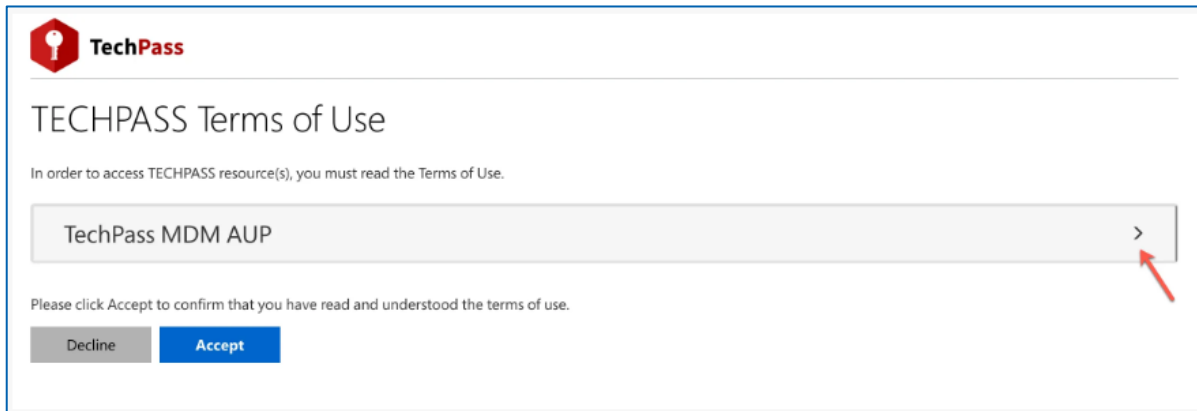


- Click the arrow to view the **TechPass Privacy Policy**.



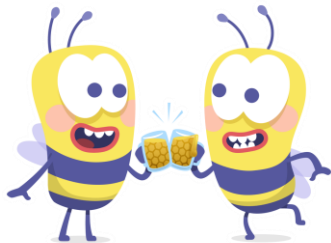
## 5b. Accept Terms of Use, Privacy Policy and Mobile Device Management- Acceptable Use Policy < Vendor >

- Read the TechPass **Privacy Policy** and click **Accept**. If SEED licence is assigned, you will be prompted to accept the TechPass Mobile Device Management(MDM) - Acceptable Use Policy(AUP).
- Click the arrow to view the **TechPass MDM AUP Policy**.



## 5c. Accept Terms of Use, Privacy Policy and Mobile Device Management Acceptable Use Policy < Vendor >

- Read the policy details and click **Accept**.
- You have now successfully onboarded TechPass. You may now proceed to onboard your non-GSIB device to SEED.



### Organizational Protocol

1. GovTech can and will establish audit trails, which will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to the network, and the resulting reports may be used for investigation of possible breaches and/or misuse. **The Agency and end user agree to and accepts that his or her access and/or connection to GovTech's networks may be monitored to record dates, times, duration of access, etc. in order to identify unusual usage patterns or other suspicious activity. The status of the device, including location, IP address, Serial Number, IMEI, may also be monitored.** This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties or users who are not complying with GovTech's policies.
2. The end user agrees to **immediately report** to his/her manager and GovTech **any incident or suspected incidents of unauthorized data access**, data loss, and/or disclosure of company resources, databases, networks, etc.

### Policy Non-Compliance

Failure to comply with the *Mobile Device Management (SEED) Acceptable Use Policy* may result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment or of the relevant vendor contract, by GovTech or the relevant Agency.

By selecting "**ACCEPT**" below it is deemed that you have read, understood and agree to all the provisions in this AUP. This AUP shall apply to you throughout the period that your device is provisioned with SEED and onboarded as a GMD. Any obligations herein that expressly or by their nature survive the cessation of your device as a GMD shall continue to survive.

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

Decline

Accept

# SEED - Prerequisites

Before you onboard your device to SEED, there are few things which you need to start the onboarding and few things to ensure a successful onboarding.

## You will need:

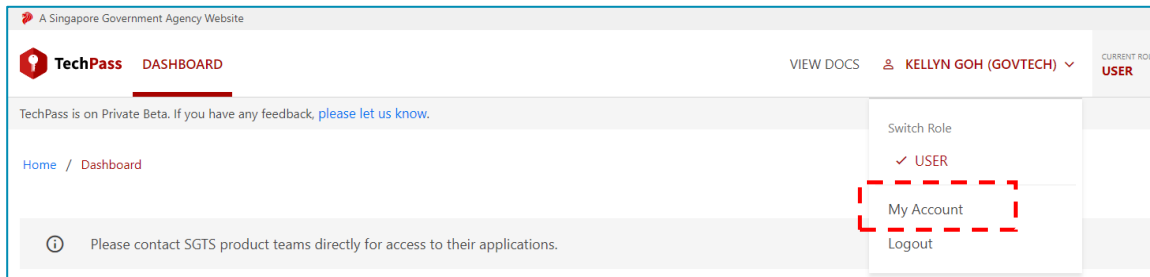
1. An active TechPass account.
2. SEED provisioning for you to onboard your device.
3. Device with supported operating systems and the required permissions.
  - A non-GSIB or a non-DWP device that runs on Windows 10 Pro/Enterprise versions or on macOS Big Sur 11 and later versions.
  - You must have Administrator rights on the device.

## To ensure a successful onboarding:

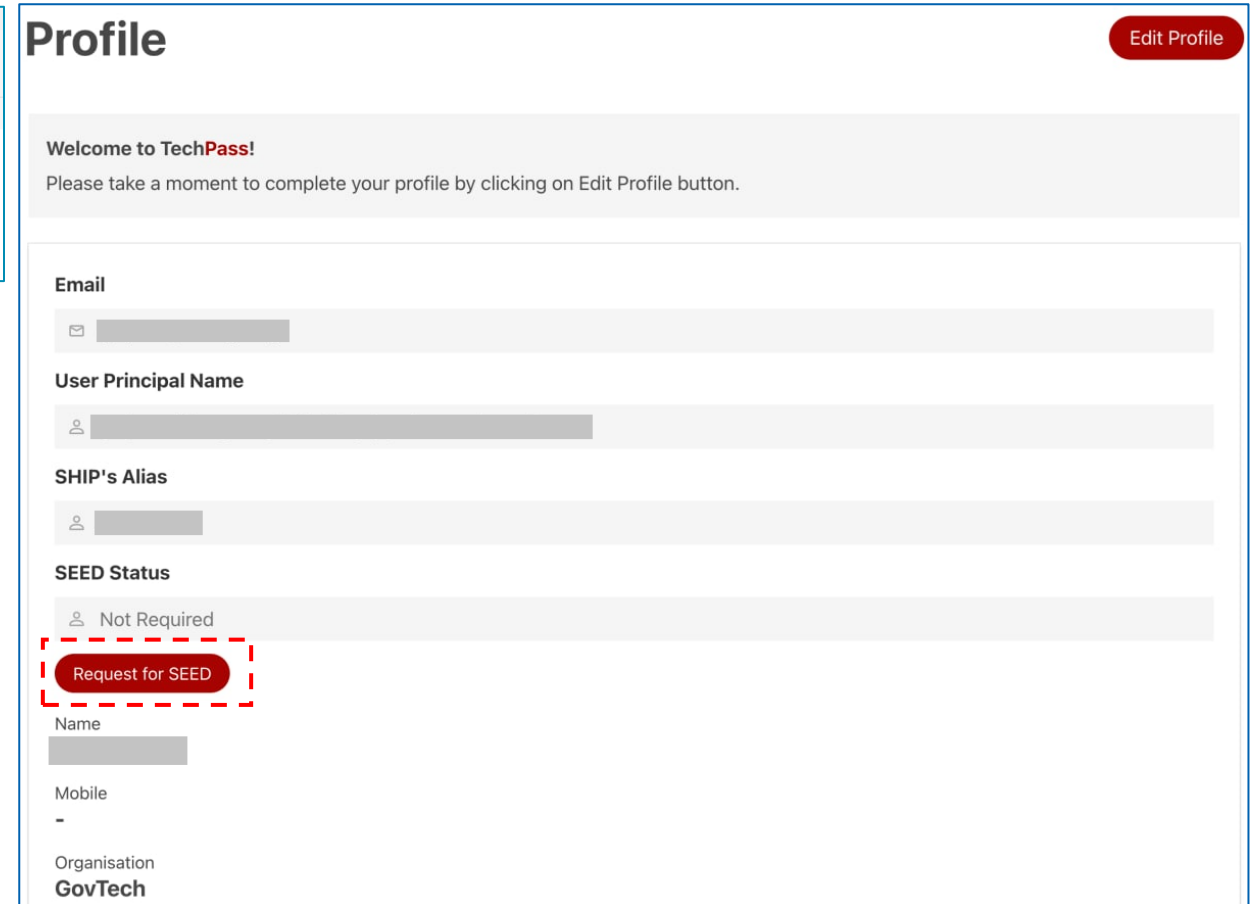
- a) Remove existing softwares on your device.  
**Note** : We will not be able to extend support for devices that have not offboarded from your company MDM and/or Antivirus solutions before onboarding to SEED.
- b) If you are onboarding a macOS device, verify if System Integrity Protection (SIP) is enabled.
- c) Encrypt your hard disk drive to protect your data at rest.
- d) Refer to [Best practices](#) to know about the supported browsers.

# SEED Licence Request < Public Officer >

- If you have already onboarded to TechPass and requires SEED onboarding, please log in to your TechPass account at <https://portal.techpass.gov.sg/> and select “Request for SEED”.

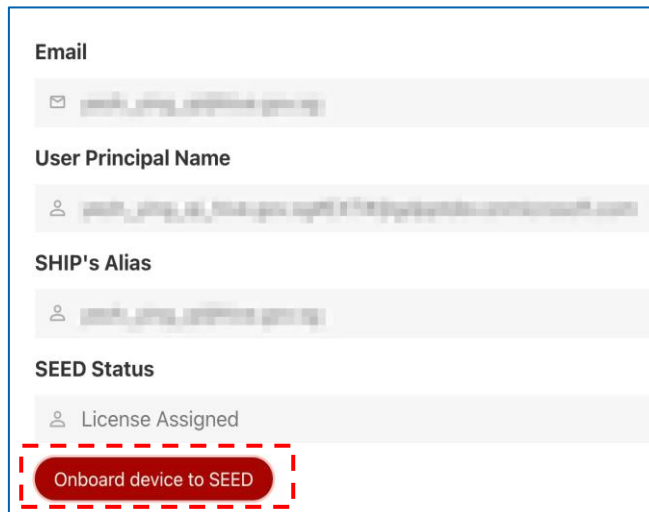


- Once you have submitted your Request for SEED, you will need to complete the onboarding following the instructions provided and register the Intune ID under your account on the TechPass Portal.
- The device will be enrolled within the next 30 minutes.



# SEED Licence Request < Public Officer >

- Note: If you have already been provisioned with SEED, instead of **Request for SEED**, the **Onboard device to SEED** button is displayed.
- The **SEED - Onboard Device** dialog is displayed. Follow the instructions on this dialog.
- Enter the Intune device ID (Refer to [slide 42](#) & [43](#)) in this dialog and click **Submit**. Ensure there are no spaces at the beginning and at the end of the Intune device ID.
- During this time, the device onboarding status is **Pending**. Once the device is updated with all the required softwares and configurations, the device onboarding status changes to **Onboarded** and you will receive a successfully onboarded email.



Email

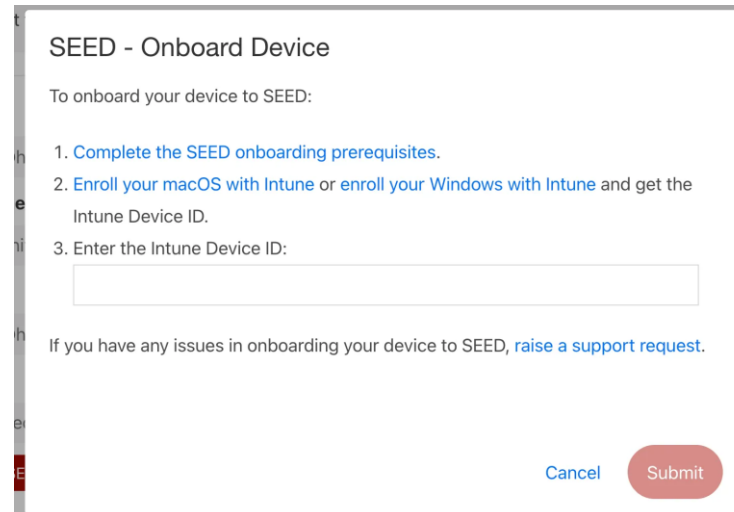
User Principal Name

SHIP's Alias

SEED Status

License Assigned

Onboard device to SEED



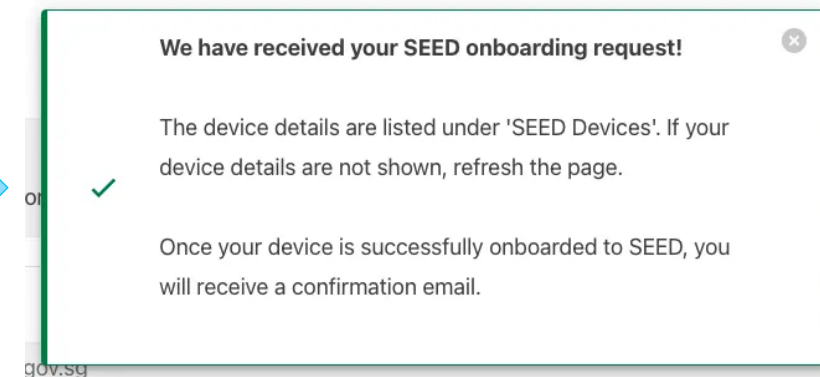
SEED - Onboard Device

To onboard your device to SEED:

1. [Complete the SEED onboarding prerequisites.](#)
2. [Enroll your macOS with Intune](#) or [enroll your Windows with Intune](#) and get the Intune Device ID.
3. Enter the Intune Device ID:

If you have any issues in onboarding your device to SEED, [raise a support request](#).

Cancel Submit



We have received your SEED onboarding request!

The device details are listed under 'SEED Devices'. If your device details are not shown, refresh the page.

Once your device is successfully onboarded to SEED, you will receive a confirmation email.



# To get the Intune device ID <Mac>

- This step is applicable only for public officers to get the required applications and device configurations on their device.
- If you are a public officer; your TechPass ID will be your official email address such as *your\_name@agency.gov.sg* or *your\_name@tech.gov.sg*. Ignore this step if your TechPass ID format is *your\_name@techpass.gov.sg*.

## 1. Open **Terminal** and run the following commands:

```
intune_id="$(security find-certificate -a /Library/Keychains/System.keychain | egrep -B 4 "\"issu\"<blob>=.+MICROSOFT INTUNE MDM DEVICE  
CA' | grep alis | cut -d '"' -f 4)"  
if [ -z "$intune_id" ]  
then  
    echo "\nIntune ID not found\n"  
else  
    echo "\n$intune_id\n"  
fi
```

## 2. Take note of the Intune device ID that will be displayed on the Terminal window.



# To get the Intune device ID <Windows>

- This step is applicable only for public officers to get the required applications and device configurations on their device.
- If you are a public officer; your TechPass ID will be your official email address such as *your\_name@agency.gov.sg* or *your\_name@tech.gov.sg*. Ignore this step if your TechPass ID format is *your\_name@techpass.gov.sg*.

## 1. Open **PowerShell** and run the following commands:

```
$rootKey = [Microsoft.Win32.RegistryKey]::OpenBaseKey(
    [Microsoft.Win32.RegistryHive]::LocalMachine,
    [Microsoft.Win32.RegistryView]::Registry64
)
$enrollmentsKey = $rootKey.OpenSubKey("Software\Microsoft\Enrollments")
$intune_id = "Intune ID not found"
foreach ($name in $enrollmentsKey.GetSubKeyNames()) {
    $enrollmentIdKey = $enrollmentsKey.OpenSubKey($name)
    if ($enrollmentIdKey.GetValue("ProviderID") -ieq "MS DM Server") {
        $intune_id = $enrollmentIdKey.OpenSubKey("DMClient\MS DM Server").GetValue("EntDMID", "Intune ID not found")
        break
    }
}
Write-Output $intune_id
```

## 2. Take note of the Intune device ID that will be displayed on the Powershell window.

# SEED Onboarding Guide for MacOS Users

## MacOS Users

- Based on your device settings, while onboarding, you may be prompted to **restart your device** a couple of times and **reset device password**.
- For a smooth onboarding journey, make sure to link your Apple ID to your device.
- Make sure to have your recovery keys ready in the event of you facing issues with resetting your password or logging in to your device.

### NOTE:

- If you do not receive the successfully onboarded email, [check if Microsoft Defender is configured correctly](#) and also check if Tanium and Cloudflare are installed. If Tanium or Cloudflare is not installed, [raise a support request](#).
- Shortly after this email, you will receive a desktop notification informing you that your device has been renamed and will automatically restart in the next five minutes. When you log in again, you will be prompted to reset your password. This is to enforce a strong password policy.
- If you had reset your password while onboarding, you will not be prompted to reset password when your device automatically restarts.
- Refer to [Best practices](#) to know about the supported browsers.

# SEED Onboarding for MacOS Users

## Onboarding your Mac device to SEED

- a. Set up Microsoft Intune to get the required applications and device configuration.
- b. If you are a **public officer**, submit the Microsoft Intune device ID for your macOS device.  
(refer to [slide 40](#))

If your onboarding is successful, you will receive a successfully onboarded email to your organisational email address within an hour.

## Post onboarding instructions

- i. Enable Full Disk Access(FDA) for the applications installed for SEED.
- ii. Enrol on Cloudflare using WARP client to connect to protected engineering resources.

# SEED Onboarding Guide for Windows Users

## Windows Users

- Based on your Windows settings, you may be prompted to restart or reset your password while onboarding.

### **NOTE:**

- If you do not receive the successfully onboarded email, [check if Microsoft Defender is configured correctly](#) and also check if Tanium and Cloudflare are installed. If Tanium or Cloudflare is not installed, [raise a support request](#).
- Shortly after this email, when you receive a desktop notification informing about the device name change and about the device being restarted, do the following:
  - Save your current work and restart your device.
  - If prompted to specify your password, enter it.
- Refer to [Best practices](#) to know about the supported browsers.

# SEED Onboarding for Windows Users

## Onboard your Windows device to SEED

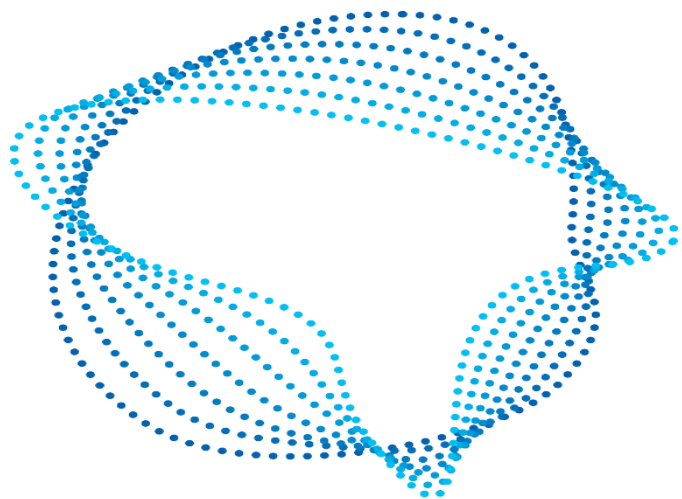
- a. Enrol your device in Microsoft Intune.
- b. If you are a public officer, submit the Microsoft Intune device ID for your Windows device.  
(refer to [slide 41](#))

If your onboarding is successful, you will receive a successfully onboarded email to your organisational email address within an hour.

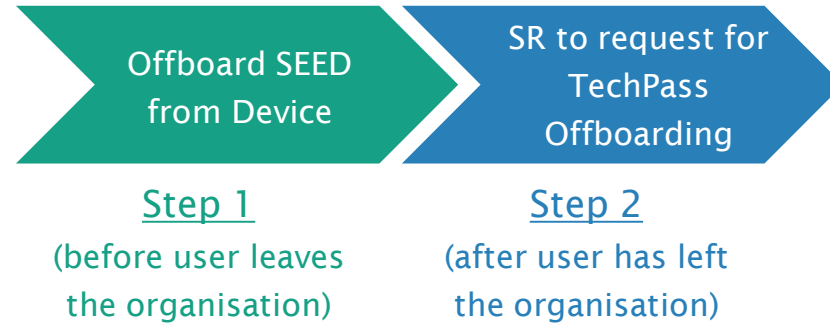
## Post onboarding instructions

- i. Enrol on Cloudflare using WARP client to connect to protected engineering resources

# Offboarding Process



# Offboarding Process



- Users should ensure that they offboard their devices from SEED before they leave the organization.
- You **should always** offboard device from SEED before requesting for TechPass account termination.

# 1. Offboarding Process - SEED

## Offboarding Your Device for SEED

- a. Remove your device from Microsoft Intune.
- b. Remove Tanium Client.
- c. Remove Cloudflare WARP client.
- d. Remove Microsoft Defender for Endpoint.



## 2. Offboarding Process - TechPass

- a. Raise a [service request](#) to request for TechPass account offboarding on an Internet Device.
- b. Select **Service Request** for ticket request type, **User has left the organization, I would like to terminate his account**, provide the necessary details (user email/TechPass ID) and submit the ticket.

### 2. Ticket Request Type

Please select the type of support ticket you like to raise

- ☒ Service Request
- ☐ Incident Request

### 3. Service Requests

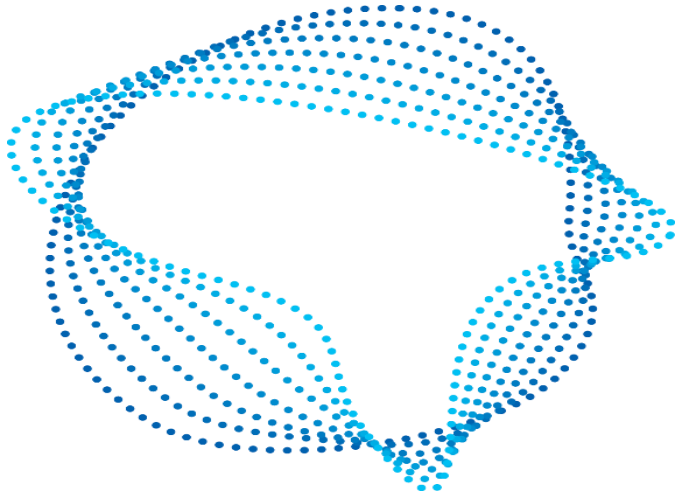
Please select the issue that best describes the assistance you needed.

- ☐ Reset Multi Factor Authentication (MFA)
- ☐ Create TechPass account for Secure Email GSIB users
- ☒ User has left the organisation, I would like to terminate his account

### 4. Details

Please describe the problem that you are facing. (Eg. Include the name of the tenant and/or application you are working on) or the reason you are contacting us.

# Incident Support



# Incident Support for TechPass

## Account management



For account-related issues such as password or MFA issues, refer to [Account Management FAQ](#) for more information.

## Signing in issues



For issues related to signing into SG TechStack applications using your TechPass account, refer to [Problems with Onboarding and Signing In](#).

## Need more help?



Submit a [service request](#). We will get back to you within three business days.

# Incident Support for SEED

Raise an incident support request with your respective [SGTS service or product](#) if you experience:

- Uninformed service interruption or degraded service.
- Issues with Cloudflare WARP, Tanium, Defender or Intune.
- Connectivity issues while accessing GCC 2.0 CMP or SGTS services.

## Support Channels

- [TechPass](#)
- [SHIP-HATS service desk](#)
- If you are a [GCC 1.0](#) user, raise an incident ticket from your Cloud Management Portal's service management.
- If you are a [GCC 2.0](#) user, raise an incident ticket via ITSM.

### Notes:

- To troubleshoot Cloudflare WARP, Tanium, Defender or Intune issues, attach diagnostics information for [Cloudflare Access](#) and [Cloudflare WARP](#) to the service request.
- To troubleshoot connectivity issues for GCC 2.0 CMP or SGTS services, [Generate HAR file](#) and attach it to the service request.

**1. Does SEED support mobile devices?**

No. Phones and Tablets (Android and IOS) as well as GoMAX devices are currently not supported.

**2. Will I need to onboard to MDM again to access GCC 2.0 in the future?**

No. Once this is done for GCC 1.0, you need not repeat the onboarding step again if you are using the same Internet Device to access GCC 2.0 in the future.

**3. I am using GSIB for remote administration of GCC 1.0, do I need to onboard?**

No. There is no need to onboard your GSIB to GCC MDM. Only Internet Devices used to access GCC 1.0 are required to onboard GCC MDM.

**4. Due to different project requirements (or possibly the need to support multiple Agencies), can my contractor onboard SEED using more than one account through different emails?**

Contractors are not encouraged to do that. It is strongly suggested that the contractor seek support and approval from the sponsor of the SEED account to support multiple projects or Agencies. Unless absolutely necessary, the contractor is not encouraged to create multiple accounts and onboard SEED multiple times using different identities on different internet devices.

**5. My laptop is already enrolled to my company's MDM and/or Antivirus solution. Can they onboard to SEED?**

Unfortunately, endpoints are not able to support 2 different MDMs or Antivirus solutions. Therefore, it is a requirement to offboard the company MDM or antivirus solution before onboarding to SEED. Note that we will not be able to extend support for devices that have not offboarded from your company MDM and/or Antivirus solutions before onboarding to SEED.

**6. Will onboarding to SEED cause my internet device to slow down?**

Common things that may cause your internet device to slow down;

- You have installed more than one antivirus solution;
- HDD space of your internet device is reaching capacity;
- Your internet device has an outdated OS.

**7. Can overseas vendors onboard to SEED?**

Agencies can onboard overseas vendors to SEED subjected to Agencies' risk assessment. However, there will be minimum/no support provided.

## 8. Does TechPass support LiteMail?

LiteMail are not supported and we require users to upgrade to standard mailbox before applying for TechPass accounts.

## 9. Will vendor's device be managed and controlled by GovTech after onboarding to SEED?

Vendors' devices that have onboarded to SEED are not joined to WOG AD, and the asset will not be managed and controlled by GovTech.

## 10. Do I still have admin access once device has been onboarded to SEED?

You will still have admin access to the GMD and can install any required developer tools.

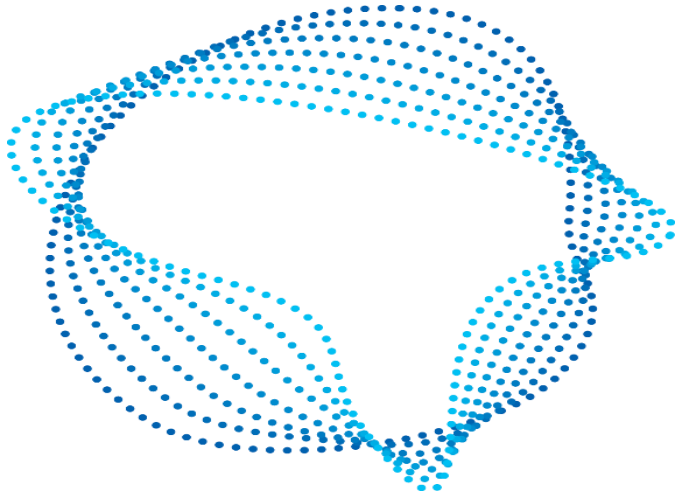
## 11. How do I receive notifications about maintenance or status updates for downtime?

Subscribe to the SEED broadcast channel to receive notifications on maintenance and status updates  
[https://t.me/+m\\_lkrOEUMpViN2RI](https://t.me/+m_lkrOEUMpViN2RI)

For any other technical Frequently Asked Questions when enrolling your Internet Device with Microsoft Endpoint Manager, you may refer to this [FAQ link](#).



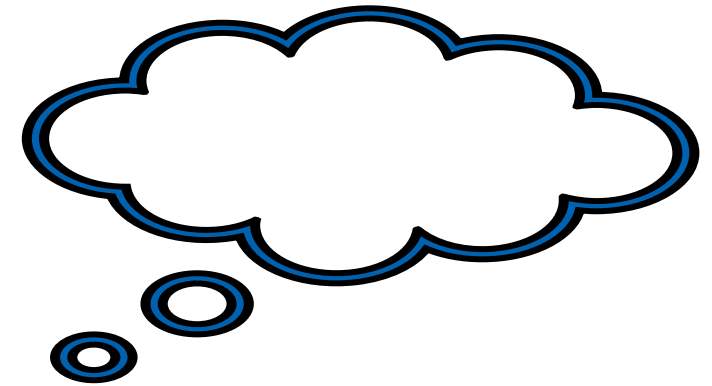
# TIPS on How to have a smooth onboarding journey to SEED + DEMO



# SEED (Security Suite for Engineering Endpoint Devices)

## TIPS on How to have a smooth onboarding journey to SEED

- Please take time to read the onboarding guide  
<https://docs.developer.tech.gov.sg/docs/security-suite-for-engineering-endpoint-devices/#/>
- Make sure the device meets all the prerequisites
- Have your appleID linked to your device if it's MAC, also recovery key ready (just in case)
- Dedicate some time to be spent on the onboarding
- Be patient



# SEED (Security Suite for Engineering Endpoint Devices)

Summary of onboarding steps : credit to Ying Qi from TechPass team

- [https://govtechgds.sharepoint.com/:v:/s/DEN/ETZvAA3\\_mMtAo8XZhJp2H54B2n-CB7UeWNI5jNUhRMtdAw?e=vskVyN](https://govtechgds.sharepoint.com/:v:/s/DEN/ETZvAA3_mMtAo8XZhJp2H54B2n-CB7UeWNI5jNUhRMtdAw?e=vskVyN)
- 9 mins- What happens when you close the status menu?
- 12 Mins – profile propagating
- 12.15 Mins – CF client deployed (observe the icon appearing on the top right corner)
- 15.20 Mins – Defender client deployed
- 17.15 Mins – Defender completed
- <https://govtechgds.sharepoint.com/:v:/s/DEN/ET00hptow3VBh6ffFDdjpwEBw8iW2KwAlSL5jxbufzJ3xA?e=sTcAm2>

# SEED (Security Suite for Engineering Endpoint Devices)

## Full Onboarding to WOG - MAC

- <https://govtechgds.sharepoint.com/:v:/s/DEN/EZfHYFQeKXZJksgGYOnIOyoBB5fsWjyD-y6jkioXMVbp1w?e=x6WOCZ>

# SEED (Security Suite for Engineering Endpoint Devices)

←

→

↺

portal.techpass.gov.sg/secure/account/profile

🔗

☆

⚙️

🗖️

👤

⋮

🌐 ONESpace 🌐 Apps Dev Mapping... 🌐 Instruction Manuals...

Profile

Edit Profile

👤 [Redacted] #EXT#@gdstechpassprod.onmicrosoft.com

SHIP's Alias

👤 [Redacted]

SEED Status

👤 License Assigned

Onboard device to SEED

Name

[Redacted]

Mobile

[Redacted]

Organisation

**Govtech**

Department

**ENP**

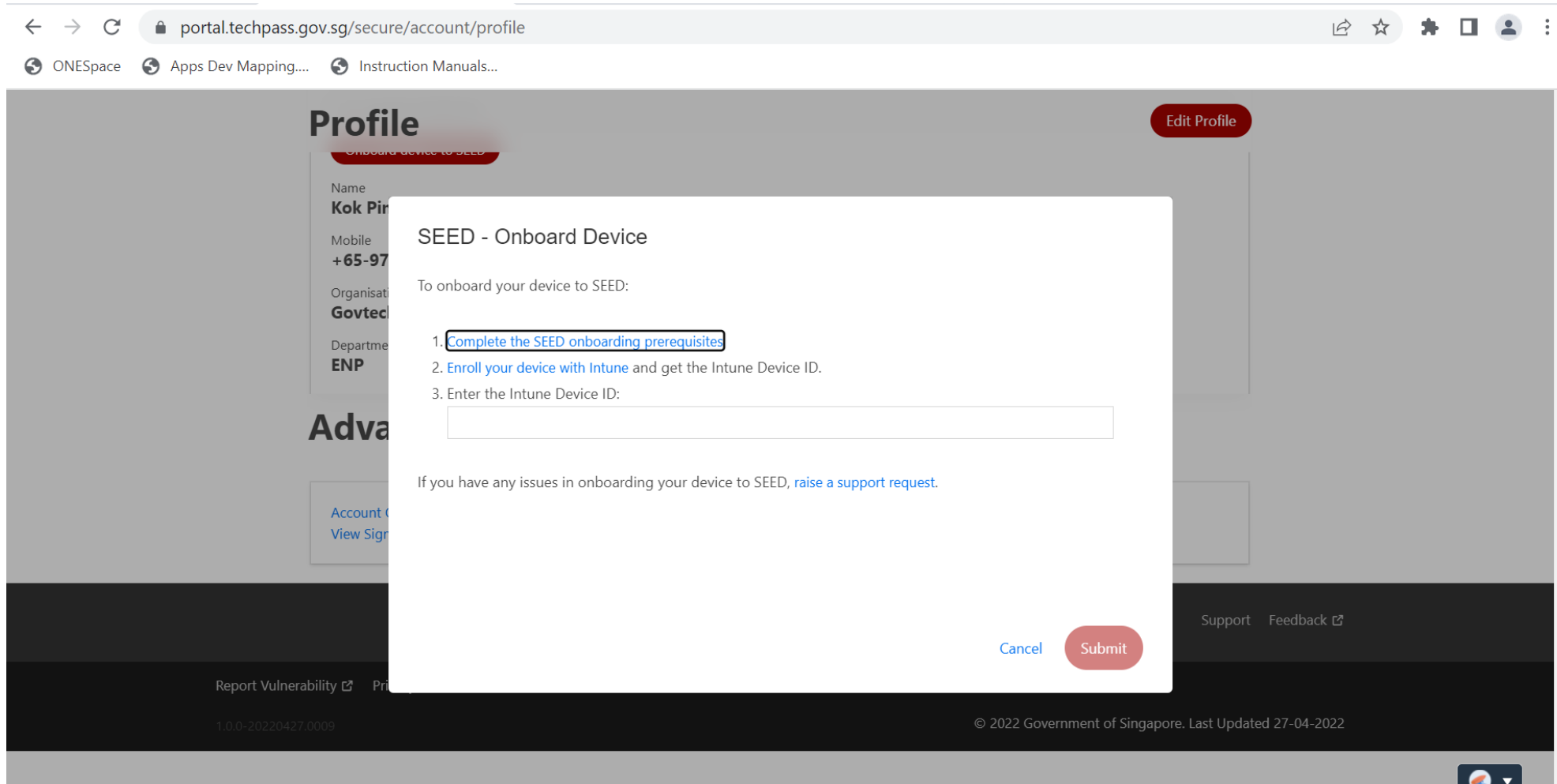
Advanced Settings

Account Overview

View Sign-In Activities

🇸🇬 ▼

# SEED (Security Suite for Engineering Endpoint Devices)



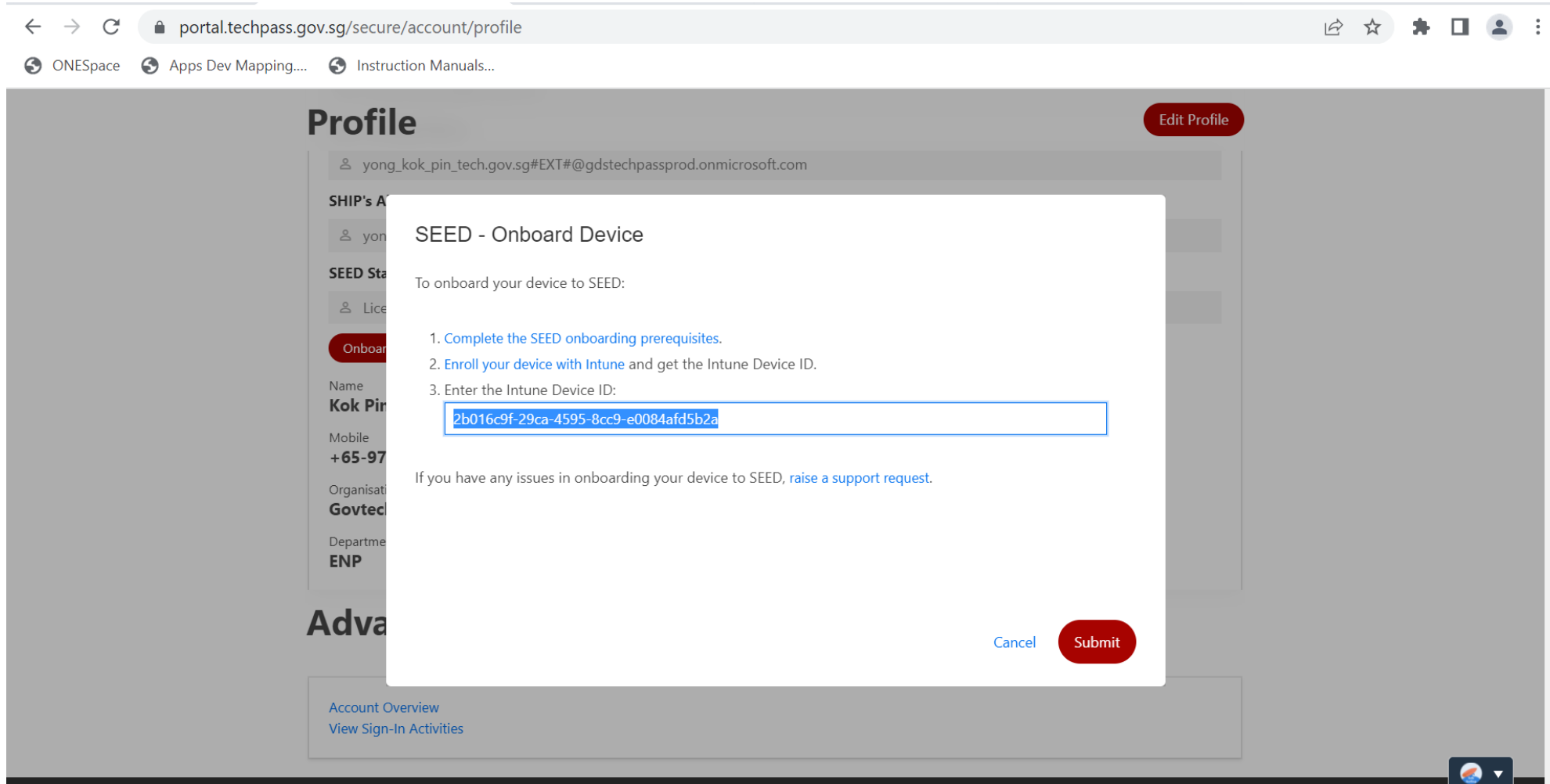
The screenshot shows a web browser window with the address bar displaying `portal.techpass.gov.sg/secure/account/profile`. The page title is "Profile". A modal titled "SEED - Onboard Device" is open in the center. The modal contains the following text:

To onboard your device to SEED:

1. [Complete the SEED onboarding prerequisites](#)
2. [Enroll your device with Intune](#) and get the Intune Device ID.
3. Enter the Intune Device ID:

Below the list is a text input field. At the bottom of the modal, there are "Cancel" and "Submit" buttons. Below the modal, the text "If you have any issues in onboarding your device to SEED, [raise a support request](#)." is visible. The background page shows a profile section with fields for Name (Kok Pir), Mobile (+65-97), Organisation (Govtech), and Department (ENP). There is also an "Edit Profile" button in the top right corner of the profile section.

# SEED (Security Suite for Engineering Endpoint Devices)



The screenshot shows a web browser window with the address bar displaying `portal.techpass.gov.sg/secure/account/profile`. The browser's address bar includes navigation icons (back, forward, refresh) and a search icon. Below the address bar, there are three tabs: "ONESpace", "Apps Dev Mapping...", and "Instruction Manuals...".

The main content area is titled "Profile" and features a red "Edit Profile" button in the top right corner. The profile information includes the email address `yong_kok_pin_tech.gov.sg#EXT#@gdstechpassprod.onmicrosoft.com`. Below this, there is a section for "SHIP's A" and a "SEED Sta" section. The "SEED Sta" section contains a list of items, including "yong\_kok\_pin\_tech.gov.sg#EXT#@gdstechpassprod.onmicrosoft.com" and "Licen".

A modal dialog titled "SEED - Onboard Device" is open in the center of the screen. The modal contains the following text:

To onboard your device to SEED:

1. [Complete the SEED onboarding prerequisites.](#)
2. [Enroll your device with Intune](#) and get the Intune Device ID.
3. Enter the Intune Device ID:

The Intune Device ID input field contains the text `2b016c9f-29ca-4595-8cc9-e0084afd5b2a`.

Below the input field, there is a link: "If you have any issues in onboarding your device to SEED, [raise a support request.](#)"

The modal has two buttons at the bottom: "Cancel" and "Submit".



# SEED (Security Suite for Engineering Endpoint Devices)

[←](#)
[→](#)
[↺](#)

portal.techpass.gov.sg/secure/account/profile

[🔗](#)
[★](#)
[⚙️](#)
[🖱️](#)
[👤](#)
[⋮](#)

[🌐 ONESpace](#)
[🌐 Apps Dev Mapping...](#)
[🌐 Instruction Manuals...](#)

## Profile

SHIP's Alias

yong\_kok\_pin

SEED Status

Onboarding In Progress

Onboard device to SEED

SEED Devices

Name	OS Type	Serial No.	Intune Device ID	Status
...	macos	...	2b016c9f-29ca-4595-8cc9-e0084afd5b2a	pending

Edit Profile

We have received your SEED onboarding request!

✓

The device details are listed under 'SEED Devices'. If your device details are not shown, refresh the page.

Once your device is successfully onboarded to SEED, you will receive a confirmation email.

Advanced Settings

# SEED (Security Suite for Engineering Endpoint Devices)

**From:** DEEP Team <no-reply@deep.techpass.gov.sg>  
**Sent:** Thursday, 28 April 2022 4:46 pm  
**Subject:** [DEEP] Attn: Your device has been successfully onboarded

Your macOS device with serial number [REDACTED] has been successfully onboarded to DEEP (Developers' Environment Endpoint Posture). Please visit the [DEEP Dashboard](#) for more information. Additionally, please take note of the following:

1. In order to access protected engineering resources, you will need to configure and connect your Cloudflare WARP client to the Cloudflare network. Please follow the instructions provided in the onboarding email to complete this step if you have not already done so.
2. In a while, you may receive a desktop notification that your device has been renamed according to convention, and that a timed restart will occur in 10 minutes. This is completely expected, and you should save any existing work to prevent data loss. Instead of waiting for the timer, you can also opt to manually restart your device to speed up the process. As the naming convention is required for administrative purposes, please refrain from renaming your device thereafter.

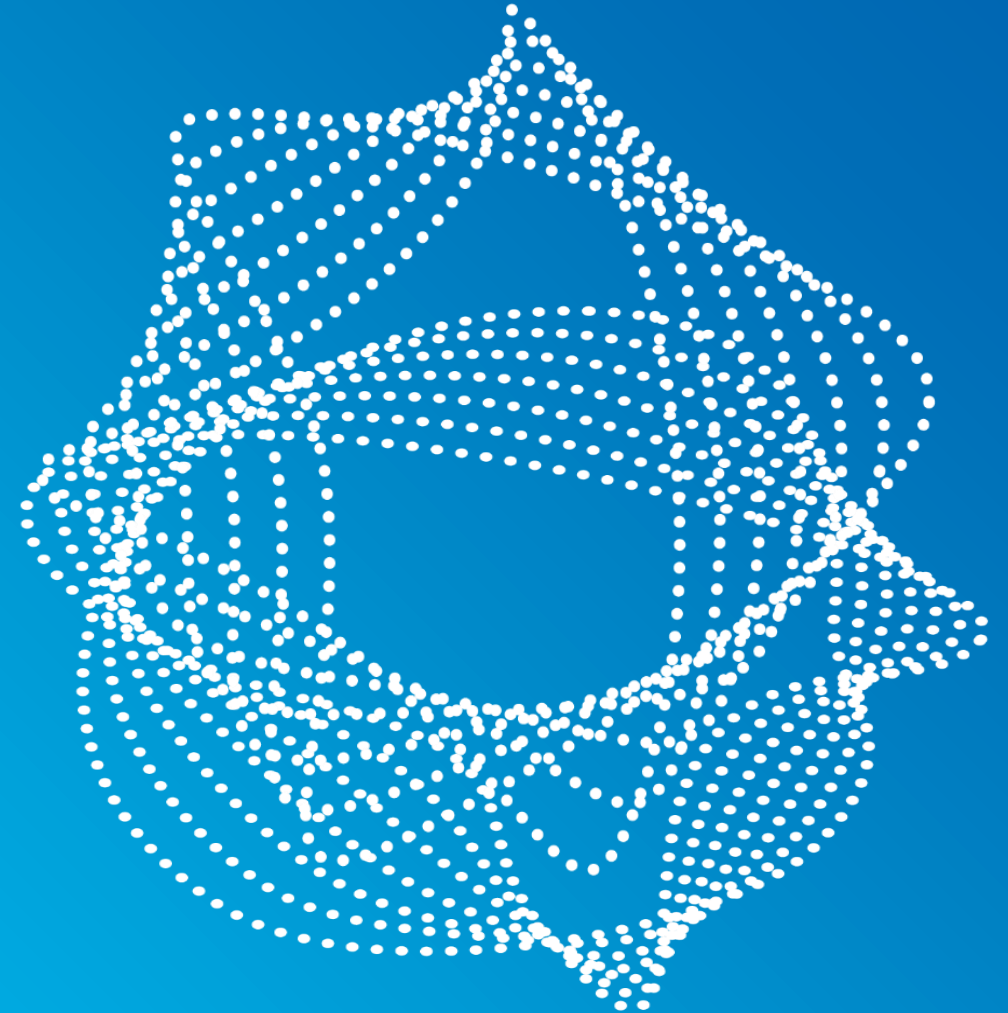
# SEED (Security Suite for Engineering Endpoint Devices)

## Onboarding to SEED - Windows

- <https://govtechgds.sharepoint.com/:v:/s/DEN/ERNPGcHn5OtOnLtF6thKT7IBQM2eoLJmEj9y5MSE256giQ?e=ExuZVw>

THANK YOU

Questions and Answers



# We Want to Hear Your Feedback!



<https://form.gov.sg/625cbd578a621f0012fa9bac>

- Let us know what went well and how we can improve.
- We want to ensure that we are bringing the right contents to you so as to help Agencies.
- If you have any questions, please reach out to us at [Ask\\_CODEX@tech.gov.sg](mailto:Ask_CODEX@tech.gov.sg)